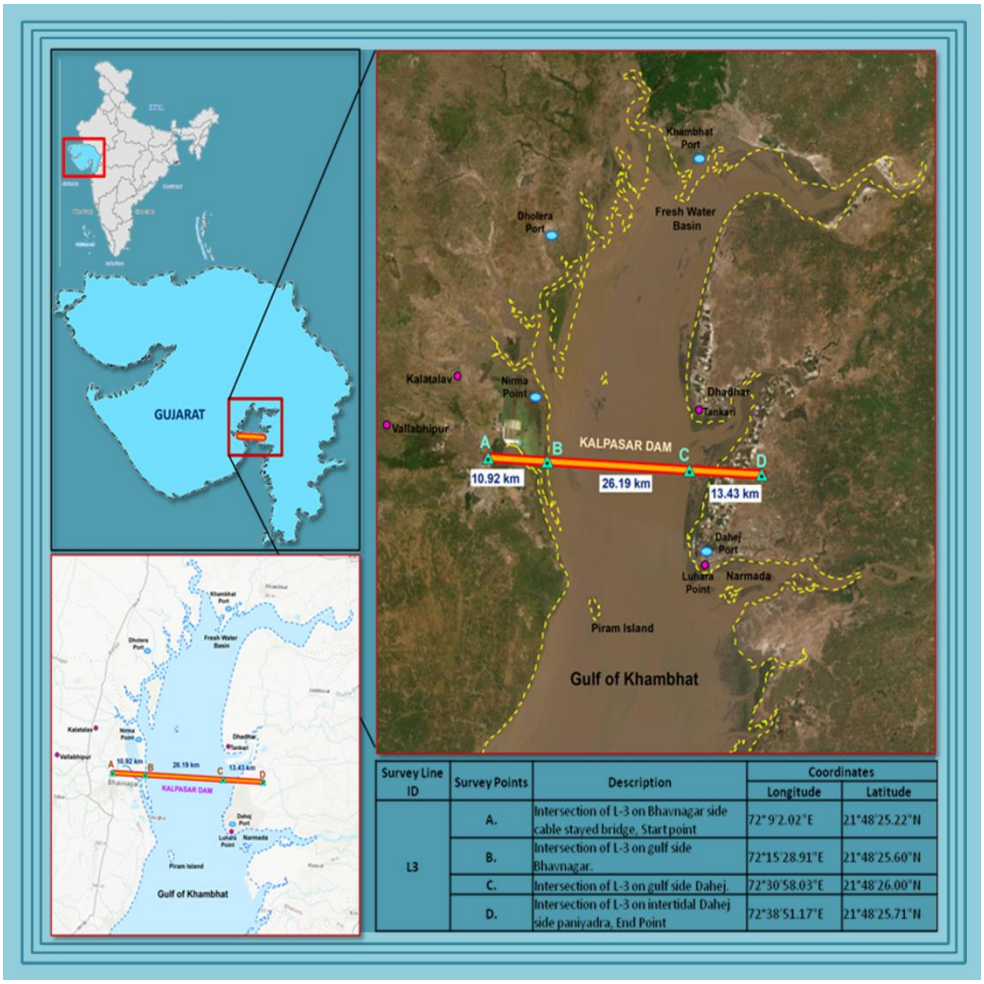


Survey Line ID	Survey Points	Description	Coordinates	
			Longitude	Latitude
L3	A.	Intersection of L-3 on Bhavnagar side cable stayed bridge, Start point	72°9'2.02"E	21°48'25.22"N
	B.	Intersection of L-3 on gulf side Bhavnagar.	72°15'28.91"E	21°48'25.60"N
	C.	Intersection of L-3 on gulf side Dahej.	72°30'58.03"E	21°48'26.00"N
	D.	Intersection of L-3 on intertidal Dahej side paniyadra, End Point	72°38'51.17"E	21°48'25.71"N

DETAILED PROJECT REPORT (DPR)SECURITY ASSESSMENT OF KALPASAR DYKE

CONFIDENTIAL

Project Study Team:

Commodore Shiv Tewari (Retd)	-	Project Director
Ms. Sunandini Arun	-	Project Coordinator
Commander Samir Mittal (Retd)	-	Sr Security Consultant
Commander Mukul Rathi (Retd)	-	Sr Security Analyst
Ms. Karen Yadav Tewari	-	Study Coordinator and Analyst

Contents

List of Figures

List of Tables

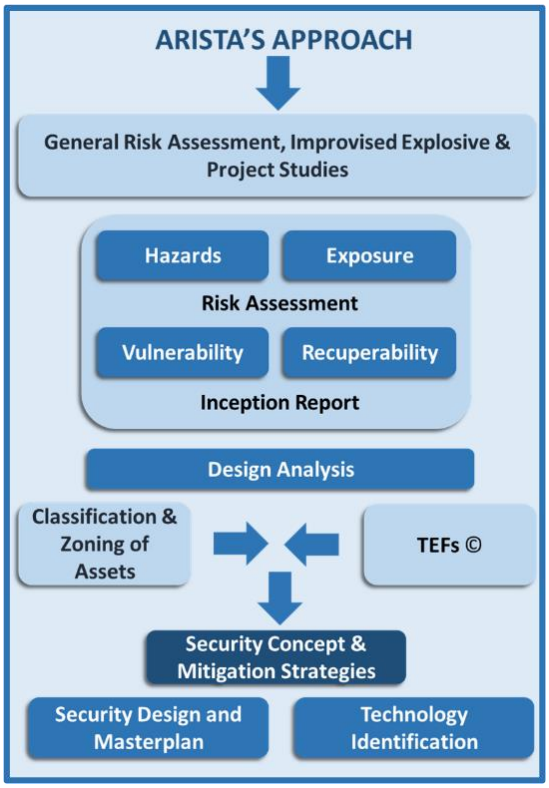
1 Introduction

1.1 Executive Summary

1.1.1 Background

The Ministry of Earth Sciences (MoES), Government of India, is in the process of preparation of a Detailed Project Report (DPR) for the Kalpasar Dyke Project through its attached office, the National Centre for Coastal Research (NCCR). A project of national importance at the scale envisaged requires a detailed study related to Security Aspects which will impact this critical infrastructure. Accordingly, NCCR has appointed Rashtriya Raksha University (RRU), together with its execution partner Arista Risk and Corporate Solutions LLP, to undertake a comprehensive Risk Assessment of the Project.

Arista has a clearly defined methodology, the core principles of which allow reaching conclusions specific to each project and client requirement. The approach defined and adopted based on suitability to this project is mentioned below:



1.1.2 Understanding the Environment

The development of a security design master plan for the Kalpasar Dyke requires deeper understanding of the related environment and this was undertaken by the study group by way of examining the project related environment, site visits, discussions and

interaction with stakeholders and other study groups. Apart from analysing national level security aspects, the local security situation was established by approaching a variety of security stakeholders from the armed forces to paramilitary forces in the region. The NIAS social impact study team provided credible field inputs to support the development of the overall hazard picture. The design team involved with traffic study, flood regulator design, engineers at the Kalpasar site were all integrated into the analysis to seek inputs before undertaking a comprehensive Risk Assessment.

Traditionally a Dyke is a secure site where public in general has restricted access. The uniqueness of the Kalpasar Dyke project lies in the fact that apart from being a freshwater reservoir for the Saurashtra region, it has also been designed to provide a transportation corridor to reduce the envisaged travel distance between Saurashtra and South Gujarat from approximately 350 kilometres around the Gulf to 50 kilometres across the Gulf providing access to a large volume of people and vehicles. From the security perspective this is a tremendous challenge and thus a detailed study translating into a comprehensive tailor-made security design including its subsequent implementation is the way forward.

The global indices and events that have occurred in relation to incidents at similar sites along with the capabilities that exist with various inimical groups in our neighbourhood as well as internally, point to the fact that the likelihood of such attempts at Kalpasar site in future is possible. Further, targeting of water related infrastructure in the recent months in India, details of which have been captured in the study, further highlight the intent of perpetrators and the effect of such incidents. Political dynamics, terrorism, crime and unrest including study of inimical groups and their capabilities have been factored to arrive at conclusions.

The geographical location of Kalpasar dyke in the vicinity of our western neighbour makes it a strategic target and thus vulnerable both during peace and wartime. Wartime targeting of the asset and impact of military grade ordnance will be designed by the adversary for degradation of the asset and would be difficult to quantify, however to understand the impact and damage potential of improvised explosive devices delivered by various means during peacetime have been studied by qualified Explosive Ordnance Disposal (EOD)experts in Arista's team.

1.1.3 Risk Assessment

Since resources are always at a premium, a need exists to categorize assets so that those more critical to the organisation are given greater focus than those which are less critical. Exposure is invariably to those assets that are essential for supporting the operational role of the organisation.

The assets associated with the dyke have been identified through the use of the CARVER Matrix developed by the U.S. Special Forces. The CARVER Matrix is a decision-making tool used for rating the relative desirability of potential targets and for properly allocating attack resources. The CARVER assessment factors of Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognisability assist in selecting the best targets to attack. As the factors are analysed and values assigned, a decision matrix is formed, indicating the highest value target to be attacked within the limits of the capability.

A list of 25 key assets related to the dyke has been identified and shortlisted for development of the Risk Assessment.

Assessing Risk is an important part of the security designing process as it provides the basis for defining the hazards, exposure, vulnerabilities, ability to recover, scale, areas, type of controls required and provides the `***Why'*** behind the exercise. Risk categorisation further assists in quantifying subjectivity to enable translating the Security Concept and Principles into the design. The risk scores achieved for further analysis are placed at Table 26 for reference.

A Risk Assessment based criteria both analytical and field observed, indicates that the Flood regulator, Machinery Spaces, Trained Operations and Maintenance Personnel and Control Room are assets exposed to the highest risk. Other assets which are at high risk include Project Site Administrative Infrastructure, Storage and Stacking Yard, Administrative and Machinery Spaces, Power Transmission and Distribution Network and Controls.

A detailed analysis of each critical asset based on designs and plans obtained has been further undertaken to improve understanding of the security risks and provide tools, guidelines, information, best practices, and resources to facilitate a more effective concept, design and security plan development.

1.1.4 TEFs©, Risk Evaluation & Observations

(a) Tactically Exploitable Features

Breaching security systems and technology requires detailed planning, information, technical knowhow, physical capability and at times insider support amongst many other factors that contribute to success. Based on Arista's real-world experience, these have been identified and derived as TEFs© Tactically Exploitable Features which translate to vulnerabilities and form the core part of our methodology.

Every perpetrator when planning a malicious act against a facility, carefully studies the facility before creating their plan of action. Their surveillance may include an onsite reconnaissance, insider information, blueprints etc. through which they would attempt to identify these TEFs© or vulnerabilities. It is therefore these TEFs© that need to be identified by an `Experts Eye' with an intruder's perspective and attended to during the security designing process. Twelve project-specific TEFs© have been identified and have assisted in further development of the security plan to minimise risk.

(b) Evaluation and Observations

Keeping in mind hazards, exposure and TEFs© the overall evaluation and observations of key critical assets are highlighted in the succeeding paragraphs.

(1) **Evaluation & Observation - Dyke Structure, Abutments, Irrigation Structure, Solar/ Wind Farm, Power Transmission and Distribution Network** - The inherent strength of the dyke structure, including abutments, in design and materials used ensures that the structures will remain stable unless specifically targeted in a warlike situation using military grade ordnance. During peace using improvised explosive devices the risks are limited, however, sabotage and surveillance especially using drones to gain information for future targeting cannot be ruled out. Similarly, irrigation structures, solar and wind farm as well as power transmission and distribution network are all more

susceptible during wartime, while sabotage and cyber-attacks during peace time pose greater risk;

(2) **Evaluation & Observation –Flood Gates, Control Rooms, Machinery Spaces, Maintenance Corridor**- Flood regulator gates, control rooms, machinery spaces and maintenance corridor remain the most vulnerable critical assets of the project with a variety of very high risks. The seaward side hazards are more during wartime by traditional marine forces. From the reservoir side, boats and surface crafts are more likely to succeed in reaching the flood regulator because of greater depths in the reservoir and considerably less flow rate of the water being discharged into the gulf. The vulnerable part will most likely be the mechanism which physically hoists and lowers the gates. Guides and concrete piles may be near impenetrable but the steel wire ropes which lift and lower the gates will be vulnerable to attacks from shaped/cutting explosive charges, mechanical cutters and gas cutters. If an adversary with intent to disrupt the dyke does get access to the reels and motors, they can, as well, be jammed and damaged by various means. Both the control room, machinery space and maintenance corridor of the dyke are the hub of operational activity with highly sensitive equipment which if disrupted can have catastrophic effect on the overall functioning of the dyke. If specifically targeted, in cohesion when water levels are high due natural/ seasonal conditions they can be highly vulnerable to attacks with the aim of crippling the operations of the dyke. Sabotage and cyber-attack in peacetime pose greater risks, while their susceptibility to improvised explosives is moderate to low;

(3) **Evaluation & Observation - Road and Rail Transportation Corridor** - The road and rail transportation corridors are a unique feature of this project and not many dykes exist where public at large is permitted to access the feature for regular use. This poses tremendous challenges in the design of security to ensure functionality without disruption of activities as well as robust security to various elements of the dyke. Examination of the traffic study undertaken and the designs prepared, show that a large number of security related issues have clearly been taken care of in the design. The corridors are designed to pass over the crest of the dyke on a strengthened concrete structure with a rock base. The road corridor is on the reservoir side thus preventing general public from being able to approach close to high-risk areas such as the flood regulator, maintenance corridors and machinery spaces. The three-meter setback between the road and rail corridor prevents crossover of vehicles to target dyke features/ operations as well as the railway corridor itself. The railway corridor which is to the seaward side offers a buffer zone to people and vehicles to undertake any targeting. While there are inherent hazards of sabotaging the tracks to create an incident during peacetime, the impact on the structure will be limited. To carry out an incident of value using IEDs to damage either of these structures is limited. Any such attempt would be to temporarily disrupt operations to gain limelight or media attention. Both the corridors are therefore less susceptible to risks during peace time; however, they present a very strategic target for adversaries during wartime using military grade ordnance;

(4) **Evaluation & Observation - Trained Operation and Maintenance Personnel** - The softest underbelly of any facility is the human resource without which any activity or operation is not feasible. Further, targeting the workforce causes huge impact on the morale and further functionality. The ability to recover from loss of trained manpower who have built expertise in management and operation of a complex critical asset like the Kalpasar Dyke is very tough and time consuming. The trained operations and maintenance manpower thus remains most vulnerable both during peacetime and wartime as they are easy to target and offer high gains to the adversary. They are susceptible to all forms of

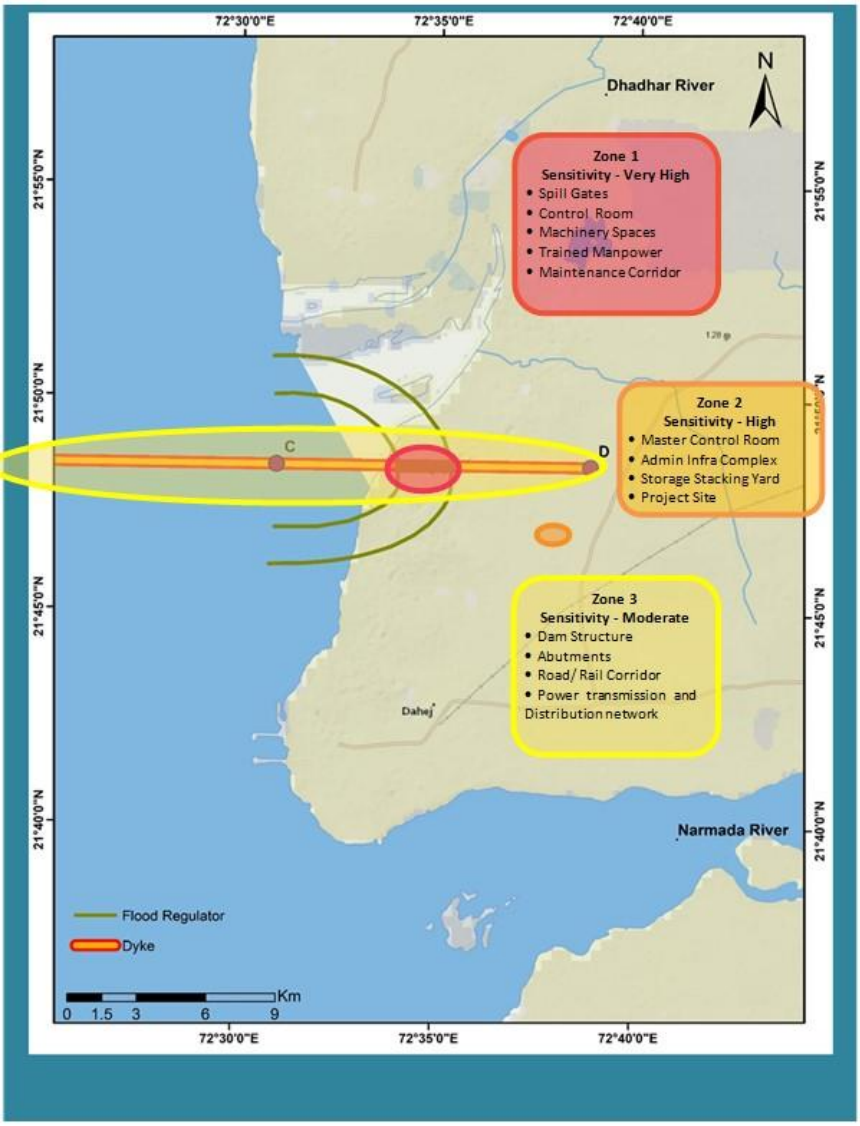
improvised explosive devises, active shooters, and wartime collateral loss of life and most other forms of hazards; and

(5) **Evaluation & Observation - Administrative Infra / Complex, Storage/ Stacking Yard, Project Site Admin Infra** - The administrative infra/ complex, storage/ stacking yard, project site administrative infrastructure are all vital functional areas of the project. Their construction will be of regular material with limited hardening. The flow of activity, movement of a variety personnel, including vendors, contactors, labour other than the project staff itself, presents a soft target to adversaries with limited capabilities but with high intent to create an incident. These assets therefore remain at high risk to a variety of hazards both during peace and wartime.

1.1.5 Sensitivity Based Zoning, Security Design Concept, Mitigation Strategies

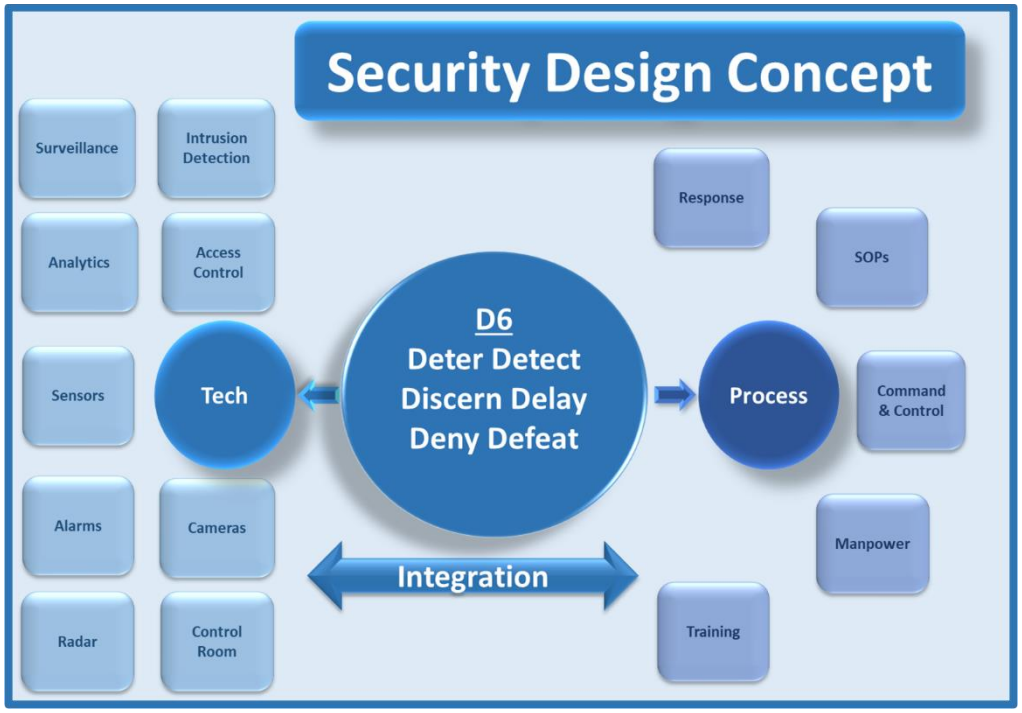
(a) Zoning

Based on the assessed risk and TEFs©, assets have been classified into four broad categories of Sensitivity based Zones, to enable provision of the requisite security features and control measures corresponding to the Risk they are exposed to. This method of classification further helps in identifying assets of similar risk sensitivity and while planning infrastructure, if feasible, consolidating them in areas/zones for the provision of defensive layers and defence in depth to the more sensitive areas. Based on analysis and Sensitivity the project has three Zones and are represented at figure below:



(b) D6 Security Design Concept

Based on study of the documents, drawings, understanding of the local conditions through a site review and the defined security design principles above, the D6 concept of security along with a layered defence concept has been evolved for the Kalpasar dyke project.



(c) Mitigation Strategies

Prior defining the Project Security Defence Plan mitigation strategy options that are available based on a detailed analysis of risks, TEFs© and its evaluation undertaken in the preceding sections of the study have been defined.

(1) **Mitigation of Risks - Dyke Structure Including Abutments, Irrigation Structure, Solar/ Wind Farm, Power Transmission and Distribution Network -** The core mitigation strategy for the dyke structure and abutments needs to be aimed at achieving deterrence and early detection by way of robust surveillance and monitoring along with preventing hazards from gaining proximity to the structure by denial. These can be achieved by institutionalising procedures complimented with technology. Exclusion Zones, prohibited/restricted areas, both marine and land coupled with barrier systems, smart fences, alarms together can achieve the above. The irrigation structures, solar/wind farms, power transmission and distribution network which are likely to be geographically spread would need independent sensor based early warning systems with the capability of quick response in the event of an incident;

(2) **Mitigation of Risks - Flood Gates, Control Rooms, Machinery Spaces, Maintenance Corridor -**The critical assets grouped in this section are at highest risk, thus mitigation strategy should aim to first discern between friend and foe and then delay and deny, as far as possible, access to the flood regulator and the flood regulator mechanism. This can be achieved by use of multiple measures deployed together such as manned watchtowers, patrolling by boats, monitoring of the reservoir and seaward side by hi-definition CCTV cameras strategically placed on either side of the carriageway and overlooking the reservoir and the gulf, placement of radars and use of drones etc. Exclusion zones of 1-2 nautical miles on seaward side and post construction as appropriate on reservoir side should ideally be established. Security patrols on top of the flood regulator can also augment monitoring efforts. Jetties on the reservoir as well as the gulf side to embark/disembark manpower for conduct of patrols and ensure quick response to defeat hazards will need to be provided for the marine force. Berthing and maintenance facilities also need to be factored to ensure operational functionality of the mitigation strategy. Peacetime airborne drone hazards need to be mitigated with a robust CUAV solutions appropriately designed to function in an integrated manner with the larger air defence plan.

Today's unmanned technology in the underwater space needs to be mitigated with underwater diver/AUV detection systems on the reservoir side around the flood regulator area. Control Centres and vital machinery can be protected by providing a spatial separation from the traffic flow. It is unlikely that explosives in large quantities will be deployed, both due to difficulty in sourcing as well as the likelihood of detection. In smaller quantities, the hazard to personnel will be far lesser while infrastructure would largely be impervious to any effect. Effect will be more for media coverage;

(3) **Mitigation of Risks -Road and Rail Transportation Corridor -** The two corridors are meant to reduce the travel distance between Saurashtra and South Gujarat and service a large population. The mitigation strategy needs to be based on the expected Hazard Level on a particular day and the availability of design features and technology available to implement the control. Although the vehicles, by themselves, will not pose a hazard to the infrastructure, however, if laden with explosive material and operated by people inimical to national security, they can cause disruptions in the dyke activity. Similarly, freight traffic will need to be monitored for content. This cannot be done on a daily basis, however whenever intelligence indicates a credible specific hazard and has been communicated to the operator, all elements of the D6 concept need to be applied as per design;

(4) **Mitigation of Risks - Trained Operation and Maintenance Personnel**- Trained operation and maintenance manpower remains the softest and weakest area and thus all elements of the D6 security design concept are applicable to create a robust mitigation strategy. The placement of smart technology, including cameras, sensors, alarms, access control devices together itself create sufficient deterrence value for perpetrators to stay away and discard targeting plans. Well-designed SOPs that lay down methodologies to discern between authorised and unauthorised entries, along with zoning and physical barricades will delay and deny access to inimical elements posing a hazard. Safe rooms can be catered for shelter in case of major incidents;

(5) **Mitigation of Risks** - *Master Control Room, Administrative Infra / Complex, Storage/ Stacking Yard, Project Site Admin Infra* - Control Centres and vital machinery can be protected by providing a spatial separation from the traffic flow. Although data has been worked out for large quantities, it is unlikely that explosives in such large quantities will be deployed, both due to difficulty in sourcing as well as the likelihood of detection. In smaller quantities, the hazard to personnel will be far lesser while infrastructure would largely be impervious to any effect. The effect will be more of 'Optics' and uneven media coverage; and

(6) **Security Manning Strategy** - A well established and trained Quick Response Team (QRT) comprising security forces involved with management of security at the facility, who can intervene to defeat hazards in real-time is mandatory. Both marine and landward QRTs need to be suitably trained and equipped with protective gear, ballistic shielded vehicles/ boats, secure communications and robust command and control structures to be effective. Manpower requirements to cater for the security of the facility need to be worked out in detail once the detail designs have been made and the project is in the pre contract stage. Correct manning in commensuration with the technology/ hardware deployed is mandatory to ensure that systems are optimally exploited and do not remain unused for want of sufficient manpower qualified to technically exploit modern systems. The manning strategy needs to be established basis designation of roles, with uniformed security forces; private contracted security and technical support staff to man and maintain OEM equipment.

1.1.6 Budget

The project cost for security would emerge based on quantification of numbers of each equipment at the final design stage at the time plans are frozen prior implementation. For the purpose of budgeting approximate costs have been arrived at based on fair assessment of the cost of listed security equipment vis a vis the project cost as enumerate in the succeeding paragraphs.

(a) Capital Expenditure

(1) **Physical Measures (Infrastructure) and Surveillance -** A large part of infrastructure and equipment in this category would be performing dual functions like road safety monitoring, traffic management etc. Additionally, the numbers required and the technology to be used cannot be frozen at the moment. Therefore, for the purpose of budgeting, an approximate cost of 1.5% (One and a half percent) of the project cost may be budgeted for the security infrastructure and surveillance equipment;

(2) **Special Equipment -**Special equipment listed above are unique to this project and the quantities can be estimated reasonably. Going by the estimated quantities and the approximate costs a total of INR 200 crore may be budgeted for these equipment;

(3) **Allied Equipment -** These form part of the project infrastructure and hence may not be catered for separately in the security infrastructure;

(4) **Security Manpower -** For the provision of security during the construction phase, the responsibility of security is normally with that of the individual contractors. For the purpose of budgeting expenditure by contractors over a five-year period on security manpower, an approximate cost of 1.0 % (one percent) of the contracted amount is estimated based on current manpower costs; and

(5) **Additional Equipment/ Systems -** Any additional equipment/ systems, required by the Army, Indian Navy, Indian Air Force, Indian Coast Guard or CAPF as envisaged by them as per their operational plans for defence of a national level strategic asset would need to be projected and catered for by these organisations as per their budget plans.

(b) Revenue Expenditure

(1) **AMC and Maintenance -** Revenue expenditure of 10% of the equipment cost may be budgeted per year for operational maintenance of the installed equipment; and

(2) **Security Manpower -**The security manpower would ideally be provided through state forces and revenue expenditure on these would therefore be borne by the state.

1.1.7 Summary

Keeping in mind the outcomes of the study, Zone wise Security Design concept has been evolved and along with the plan represented diagrammatically in **Chapter 4**; technologies that are relevant to the project have been identified and placed at the end of the said chapter.

Kalpasar dyke is a national level strategic asset with large benefits to the nation and its population. Keeping it secure becomes the collective mandate of all stakeholders and towards that first identifying the core principles, concept and design of security becomes imperative. This study has systematically approached developing a security master plan based on brief shared by NCCR, and using proven methodologies, for future implementation of security based on the current information available at the time of the study. As the environment is dynamic, this will remain an ongoing process and at every stage of the project implementation a review would be essential.

As brought out, Armed Forces, Coast Guard, various Paramilitary and Police forces in the region were corresponded with and preliminary interactions were carried out apprising them of the project. During interactions it was suggested that additional assets, resources that may be required for the defence of the Kalpasar Dyke during peace and war time as may be envisaged by them as per their operational role may be catered for by them. It would also be advisable that the National Committee overseeing the preparation of the DPR may separately correspond with these authorities and officially intimate them regarding planning and catering for their envisaged project related security requirements in the coming years. Cyber hazards which form an independent aspect of another study need to be separately addressed to ensure mitigation of project security risks from such hazards.

The value of the study lies in its correct implementation on ground in letter and spirit during subsequent phases of the project and is recommended that a similar approach of involving domain expertise be continued for the subsequent phases of the project to ensure overall national security objectives of such a critical asset as the Kalpasar Dyke.

1.2 Overview

The Ministry of Earth Sciences (MoES), Government of India, is in the process of preparation of a Detailed Project Report (DPR) for the Kalpasar Dyke Project through its attached office, the National Centre for Coastal Research (NCCR). A project of national importance at the scale envisaged requires a detailed study related to Security Aspects which will impact this critical infrastructure. Accordingly, NCCR has appointed Rashtriya Raksha University (RRU), together with its execution partner Arista Risk and Corporate Solutions LLP, to undertake a comprehensive Risk Assessment of the Project. This would include defining the operational requirements and commensurate security concept, identifying tactical gap areas, and proposing a basic security design and appropriate technology.

This report contains a comprehensive Risk Assessment of the project, using fourteen criteria, both field and analytical, based on the expert consultant's proven methodology. The report also aims to identify critical assets within the project and the risk exposure of each asset against the identified hazards prior to formulating a security concept for the overall security of the project. Based on the security concept, technological and procedural solutions have been recommended for mitigation of the identified risks.

1.2.1 Background

The Saurashtra region of Gujarat has been experiencing severe droughts for few decades due to reduction in the groundwater table and scarcity of freshwater. To meet the freshwater demand for drinking and irrigation, the Government of Gujarat (GoG) proposes an ambitious project, called Kalpasar Dyke Project, which involves constructing a ~30 km long dyke across the Gulf of Khambhat and create a freshwater reservoir by storing the run-off of 8,000 million cubic meter of water from east-flowing rivers, namely Sabamati, Mahi, Dhadhar and Narmada rivers on the upstream of the dyke.

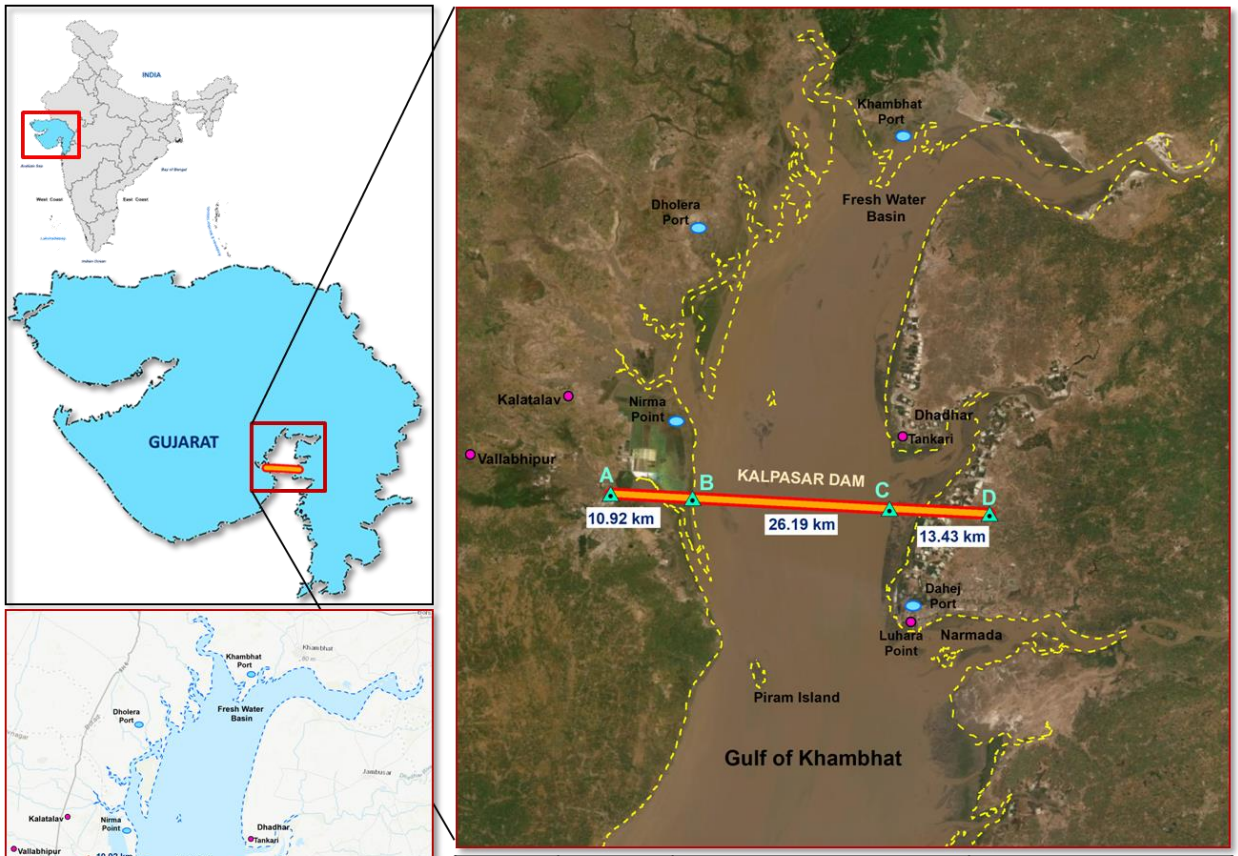
The project location is influenced by a higher tidal range (~9m) and currents (velocities ~3 m/s) at the head of the Gulf. It involves constructing a ~30 km earth dyke across the Gulf of Khambhat to create a massive freshwater coastal reservoir for irrigation, drinking and industrial purposes, with about 2 km concrete flood regulator for emptying

saltwater or flood water. A 16-lane road along with 2-lane permanent way for rail transport was planned to be built over the dyke; it is envisaged this will reduce the travel distance approximately from 350 km around the Gulf to 50 km across the Gulf. Also, the project involves flood protection in the upstream area, supply of freshwater to the Saurashtra region, and renewable energy for the lift irrigation system. The project site is located in the Moderate Seismic Zone and about 700 km to the west of the Gulf from the Makran fault.

Over the years, the Kalpasar Department of the *Government of Gujarat* conducted several studies from *Engineering Investigations* to *Design of the Dyke* with the engagement of various international, national organisations and consultants. The *Government of Gujarat* has requested the *Ministry of Earth Sciences (MoES), Government of India,* to prepare the Detailed Project Report (DPR) for the Kalpasar Dyke Project considering the expertise available with the *MoES*. This DPR will enable the Government of Gujarat to identify a suitable firm for the implementation of the project through a possible financial model, as it forms one of the important components of the Blue Economy. The MoES has conveyed its willingness to take-up the project through its attached office, namely the National Centre for Coastal Research (NCCR).

Towards the preparation of the DPR, the urgent tasks are to:
(1) Compile the reports of the completed studies;
(2) Identify the gap areas; and
(3) Prepare a Detailed Project Report (DPR) for obtaining the necessary clearances and statutory approvals for the construction of the Dyke.

It is proposed to undertake the work of preparation of the DPR with the assistance of consultants for each domain. Works are identified for each consultant. This document deals with the components of Kalpasar Project. The alignment for dyke is shown in Figure 1.



Survey Line ID	Survey Points	Description	Coordinates	
			Longitude	Latitude
L3	A.	Intersection of L-3 on Bhavnagar side cable stayed bridge, Start point	72° 9'2.02"E	21°48'25.22"N
	B.	Intersection of L-3 on gulf side Bhavnagar.	72°15'28.91"E	21°48'25.60"N
	C.	Intersection of L-3 on gulf side Dahej.	72°30'58.03"E	21°48'26.00"N
	D.	Intersection of L-3 on intertidal Dahej side paniyadra, End Point	72°38'51.17"E	21°48'25.71"N

Figure 1: Alignment of Kalpasar Dyke

1.2.2 Components of Kalpasar Dyke

(a) Dyke

The total length of the dyke including the embankments is 51.3 KM. the total length of dyke is divided into three zones based on the bathymetry and soil profile in the project area. The three zones are (i) Intertidal zone at Bhavnagar, (ii) Gulf region and (iii) Intertidal zone at Dahej. The length of the intertidal zone at Bhavnagar is 12.5 Km. the sea bed level in this zone is about +4.0 m. The water level depth during the high tide varies from 0.3 to 0.9m. The gulf region is between inter tidal zones of Bhavnagar and Dahej. The length of this region is 25 km and consists of Sand. The sea bed in this region ranges from -25.0 m MSL to -5.0 m MSL. The water level during the high tide is +6.0 m MSL. The water depth in this region during the high tide ranging from 11 m to 31 m corresponding to seabed profile. The length of Intertidal zone at Dahej is 13.85 Km. The sea bed level in this region +4.0 m MSL. The intertidal zones in Bhavnagar and Dahej mainly consist of clayey soil.

The protection structure to the main dyke of Kalpasar project is proposed from either side of the bank, which extending up to - 25 m depth contour w. r. t MSL. The rubble mound protection breakwater was designed using the Hudson Formula. The breakwater consists of primary/armour layer, secondary/filter layer, toe berm and core as shown in Figure 2. The armour layer of rubble mound breakwater are made with either concrete armour units to protect the structure from wave attack on sea side. The secondary/under layer consists of stones. This will act as filter layer between the core and primary layer. The thickness of the armour and secondary layer is determined based on the stone size. The core under the primary and secondary layer will consist of stones 10 to 500 Kg quarry stones up to the sea bed. The toe berm will be provided on the sea side, which will provide the support to the armour units and act as scour protection.

The embankment under the transport corridor is filled with sand. The rock toe protection is given on reservoir side to protect the sand fill embankment. The Typical cross section of the breakwater is given Figure 2. The crest level of the breakwater is designed based on the allowable overtopping rate for safety and structural design as per the Specification given in EurOtop manual. The breakwater is designed based on the wave overtopping criteria of 50-200 lit/s/m for accropode to estimate the crest level of the breakwater. The crest level for the bed levels from – 5.0 m to – 25.0 m and 0.0 m to -5.0 m is calculated as +19.0m MSL. The crest levels in the shallow regions of the bed level from 0 m to +2.0 m, +2.0 m to +5.0 m and +5.0 m is calculated as +16.5 m, +15.0 m and +12.0 m respectively.

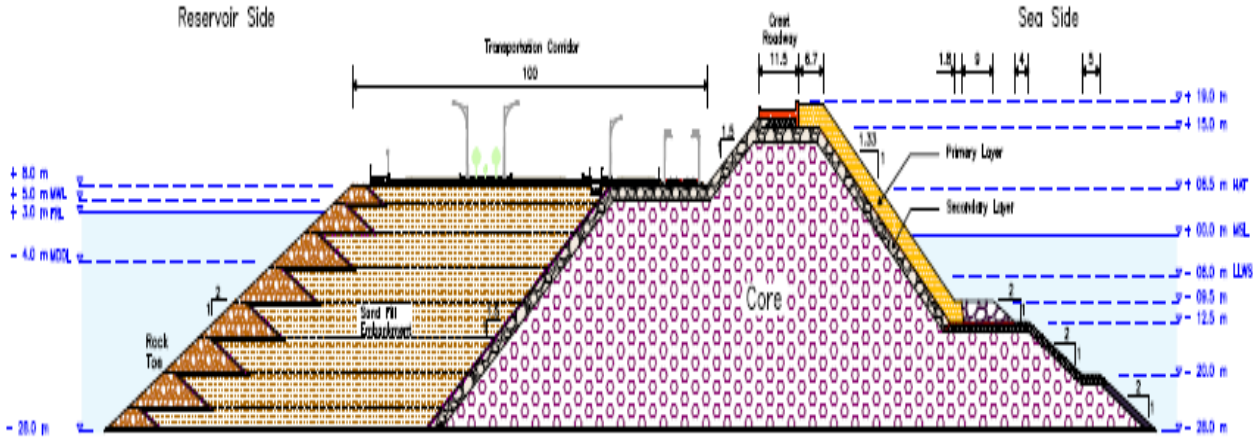


Figure 2: Cross Section of the Breakwater

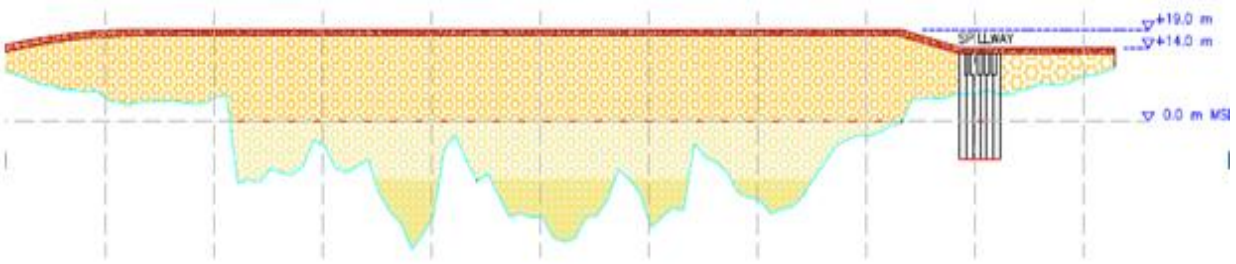


Figure 3: Longitudinal Section of Kalpasar Dyke

(b) Flood regulator

Flood regulator is major component, which regulates and controls the outflow from the reservoir. It prevents outflow from a reservoir below a fixed level and allows the flow when the water surface in the reservoir rises above the level. In most of the cases, the control section consists of a weir, which may be sharp crested, ogee, or broad crested. Gates may also be provided on the crest of the control structure to regulate the flow of water from the reservoir. A typical cross section of Flood regulator is shown in the figure 4. For the Kalpasar reservoir Ogee profile is proposed. The shape of the crest or the upper curve of the ogee profile of this flood regulator is made to conform closely to the profile of the lower surface of the nappe (or lower nappe).

The capacity of flood regulator is 1,20,000 Cumecs, gross width is 2284 meters and net width is 1872 meters having 104 spans of 18 meters width and 103 no. of 4 m thick piers is proposed. The levels of structural elements such as downstream apron level is -10.0 m MSL, upstream apron level is -7.1 m MSL, level of ogee crest -3.5 m MSL and water level during HFL is +5.00. The Ogee profile is sloped on upstream side with ratio of 1H: 1V and the profile on the downstream side formed by an equation X^1.85 = 15.21Y. The crest gates will be vertical lift type, of the size 18m wide x 7.5m high and will be provided with double seals to resist water levels from both sides. Baffle blocks will be constructed on the downstream side for energy dissipation.

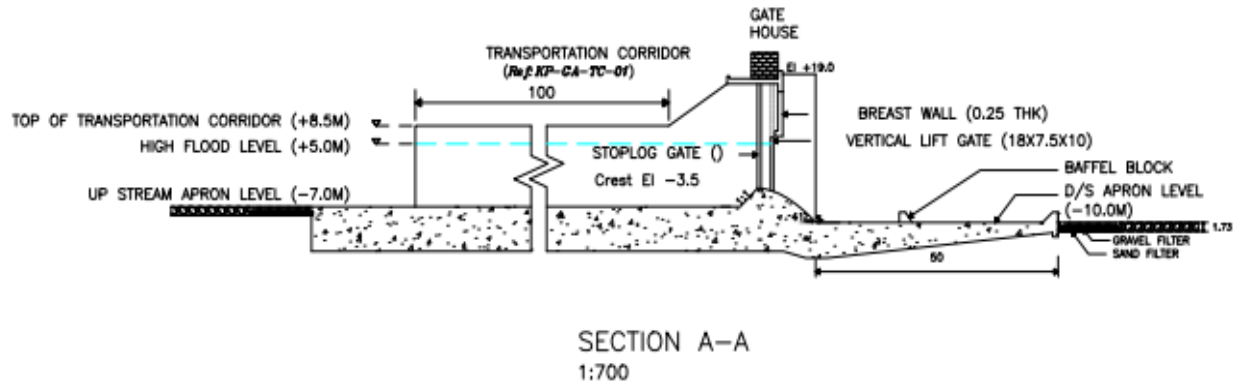


Figure 4: Layout of Proposed Flood Regulator

(c) Road and Rail Network

The storm surge and seiches study IIT Delhi indicate an increase water level of 2.5m in the reservoir for hypothetical cyclone track. So, the transport corridor is located on the crest of sand fill embankment of Kalpasar Dyke on the reservoir side at an elevation of +8.0m MSL elevation (3m above MWL). A sixteen-lane carriageway for vehicles, and a two-lane railway line is proposed as part of transportation system.

(d) Roadways

The four-lane roadway is provided on both the directions. The roadway connects the Bhavnagar in Saurasthra region and Bharuch in south side of Gujarat as shown in Figure 5. The width of the four-lane road is 14m each on both directions. The width of each lane is 3.5 m. The paved and unpaved shoulders of width 1.5m and 5 m respectively, are provided on both sides of the corridor. The total width of the roadway is 57 m which includes the median between the lanes in both directions. The median is of width 14m.The width of the median

is provided as same as four lane roadway in view of future extensions. A walkway of 5m is provided on the reservoir side of the carriageway. A Setback of 5m is also provides on the reservoir side to avoid any water splashing under extreme events.

A two-lane roadway is provided towards sea side for the transportation of heavy vehicles mainly for IRC Class 70R loading. The width of this two-lane roadway is 16.5 m, which includes median of 3 m and a paved and unpaved shoulder of 1.5 m each. Two extra lanes will be provided for every 2 km interval to accommodate the repaired vehicles/parking of vehicles. The road drainage system is provided along the roadway to control the surface water away from the road surface. A 2 m diameter pipe lines crosses underneath the roadway to remove the saline water from reservoir side to sea side. At these pipe locations culverts will be constructed. The 2.4 km long bridge will be provided at flood regulator location, where the road and railway lines will pass over the Flood regulator Bridge. A 10 m width access road is constructed on crest of breakwater on sea side for accessing the flood regulator for operation and maintenance.

Trees and shrubs are planted on the median to reduce the headlight glare during the night drive. The electric poles are installed on the roadway to provide the adequate lighting along the road and it enables the road users to see more accurately and easily the carriageway and its surrounding areas at night. Toll plaza booths will be set on the roadway for toll collection.

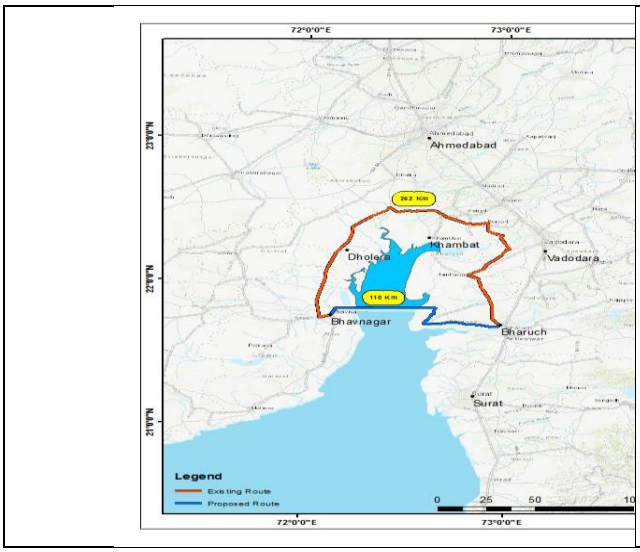


Figure 5 (a): Existing and proposed roadway connecting Bharuch and Bhavnagar

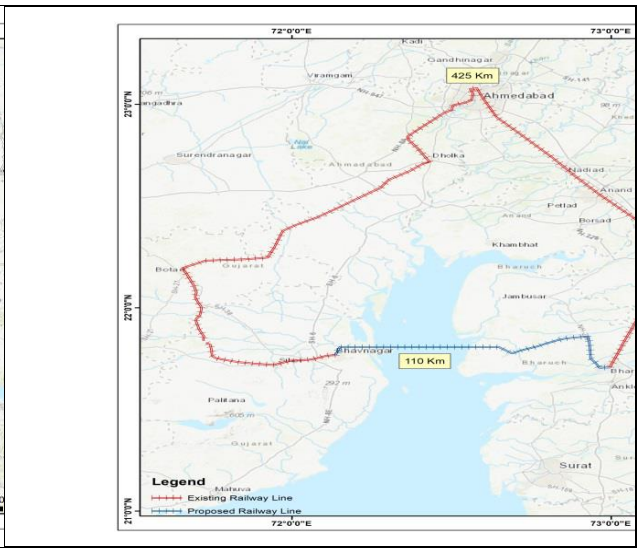


Fig 5 (b): Existing and Proposed Rail track connecting the Bhavnagar and Bharuch

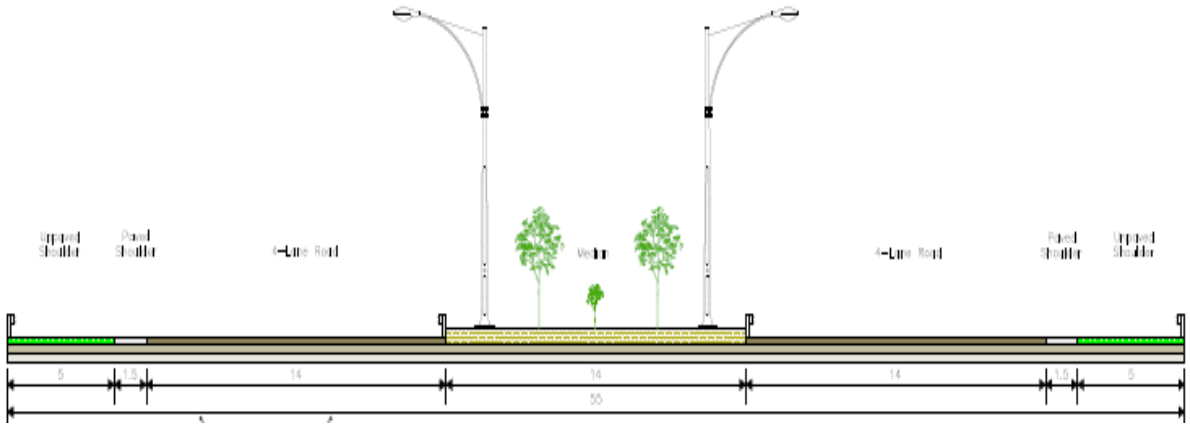


Figure 6: Proposed Eight Lane Roadway

(e) Railway

A width of 30 m is being proposed to accommodate two lane railways on the crest of the sand fill embankment. Railway foundation comprises of blanket, prepared subgrade and embankment fills. Depending upon availability of soil and economic considerations, we are adopting a two-layer construction. Below the sleeper and ballast, two-layer formation consists of blanket, sub grade and embankment fills.

Two-layer formation and broad-gauge railway line is considered. The width of the railway line is 13.2 m. The centre-to-centre distance between rails tracks are 1.67m. The length of each sleeper is 2.75m. The proposed railway line on the dyke connects the Bhavanagar and Dahej railway stations. The electrically powered trains are used for the transport of passengers as well as cargo. For this, the railway tracks will be electrified. So, the electrification 51.3 route kilometre (RKM) of broad gauge will be done on the dyke and nearest railway stations.

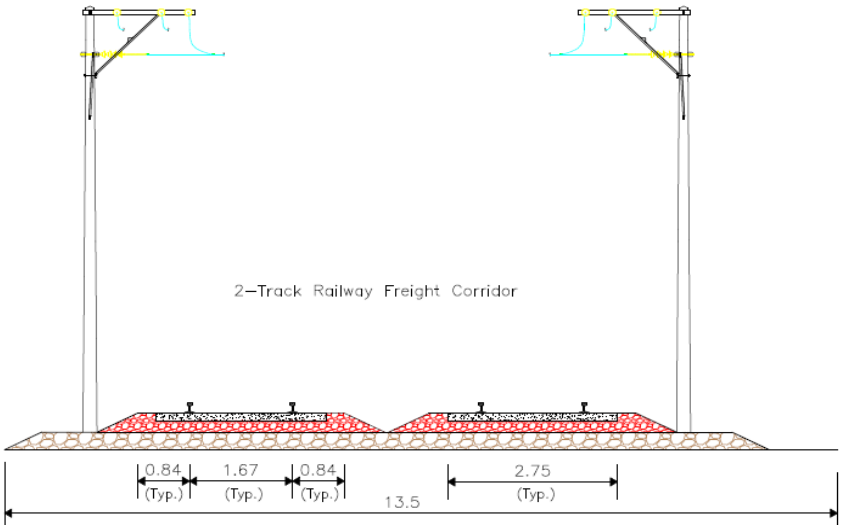


Figure 7: Proposed Railway Track

(f) Fresh Water Reservoir

The proposed reservoir will have water spread area of be 2,000 sq. km. The reservoir storage capacity is determined by area-capacity and water available for storage. Within the perimeter of the reservoir, the maintenance of the reservoir water levels, namely Full Reservoir Level (FRL), Maximum Water Level (MWL), Maximum Drawdown Level (MDDL), provides the leverage for the management of the reservoir in a desired way. An area-capacity table for the reservoir has been prepared on the basis of the NIOT bathymetry as shown in Table 1 and live storage with respect to the dead storage is given in the Table 2.

Table 1: Area Capacity Table for the Reservoir

Level with MSL	Area in (Sq.m)	Volume in (Mm3)
-5	6.633E+08	4181
-4	7.438E+08	4886
-3	8.475E+08	5681
-2	9.694E+08	6589
-1	1.107E+09	7626
0	1.228E+09	1228
1	1.335E+09	10090
2	1.430E+09	11470
3	1.522E+09	12950
4	1.645E+09	14530
5	1.796E+09	16250
6	12.287E+09	18230
7	2.296E+09	20950

Table 2: Live Storage with respect to the Dead Storage

Level with MSL	Area in (Sq.m)	Volume in (Mm3)
-4	0	0
-3	1.04E+08	795
-2	2.26E+08	1703
-1	3.63E+09	2740
0	4.85E+09	3914
1	5.91E+09	5200
2	6.86E+09	6585
3	7.78E+09	8063
4	9.01E+09	9645
5	1.05E+09	11360

The proposed fresh water reservoir has potential of 7807 $Mm^3$from upstream rivers and diversion of Narmada waters at 50% dependability. Based on the Area-Capacity tables, different water levels in the reservoir are fixed. The MDDL determines how long the tank will last in terms of dead storage capacity and sedimentation. In accordance with the area-capacity Table 13.1, the available volume at -4.0 m MSL is 4886 Mm^3. The rate of

sedimentation in the Gulf of Khambat area is 14 Mm3/year. With this sediment deposit rate, it will take 400 years to fill up the volume of 4886 Mm3. Consequently, the MDDL of the reservoir is set to -4.0 m MSL. The volume available between the level - 4.0 m MSL and + 3.0 m MSL, as derived from the area-capacity Table13.2, is 8063Mm^3, which is just as required to store the available fresh water quantity (7807Mm3). As per this requirement of live storage, the FRL is fixed at +3.0 m MSL.

The tidal range in project area is about 5.4 m. If MWL is fixed more than 5.4 m, it will create inundation in reservoir area. The infrastructure development proposed for Dholera Special Investment Region (DSIR) was planned above 5.5m contour in the gulf region. Moreover, flood routing study has indicated that Kalpasar reservoir would have substantial capacity of absorption of floods between the normal operating level +3.0 m MSL and +5.0 m MSL. By taking all these aspects into consideration the MWL of Kalpasar reservoir is fixed at +5.0 m MSL. This MWL will govern the requirement of flood regulator discharge, length and configuration.

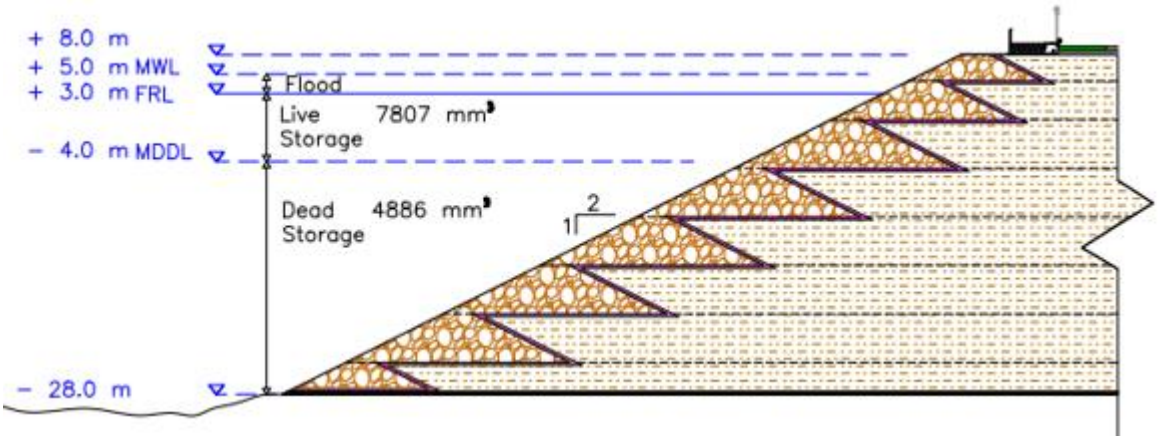


Figure 8: Various Water Levels on Reservoir Side

(g) Renewable Energy

The power required for pumping of 6500 Mm^{3}of water from the Kalpasar reservoir to Saurastra region, which is at higher elevation is about 2500 million units/year. To supply power for the lift irrigation system about1470 MW capacity wind turbine generators are proposed in three locations as shown in figure 13.9. The proposed wind farms will generate2523 million units annually. A total of 700 wind turbine generators (WTG's) of 2.1MW capacity will be placed in these locations. Out of 700 wind turbine generators, 341 WTG's will be placed in Wind Farm 1 (Vadgam I), 186 WTG's will be placed in Wind Farm 2 (Vadgam II) and 173 WTG's will be placed in Wind Farm 3(Jambusar Nada). The proposed wind farm requires about 4500 ha land for wind park out of which 3000 ha land area (without shadow effect) can be available for solar power development. Solar isolation in this area is 5.8 KWh/m^2/day and this can yield about 174 million units and a capacity of about 1000 MW.

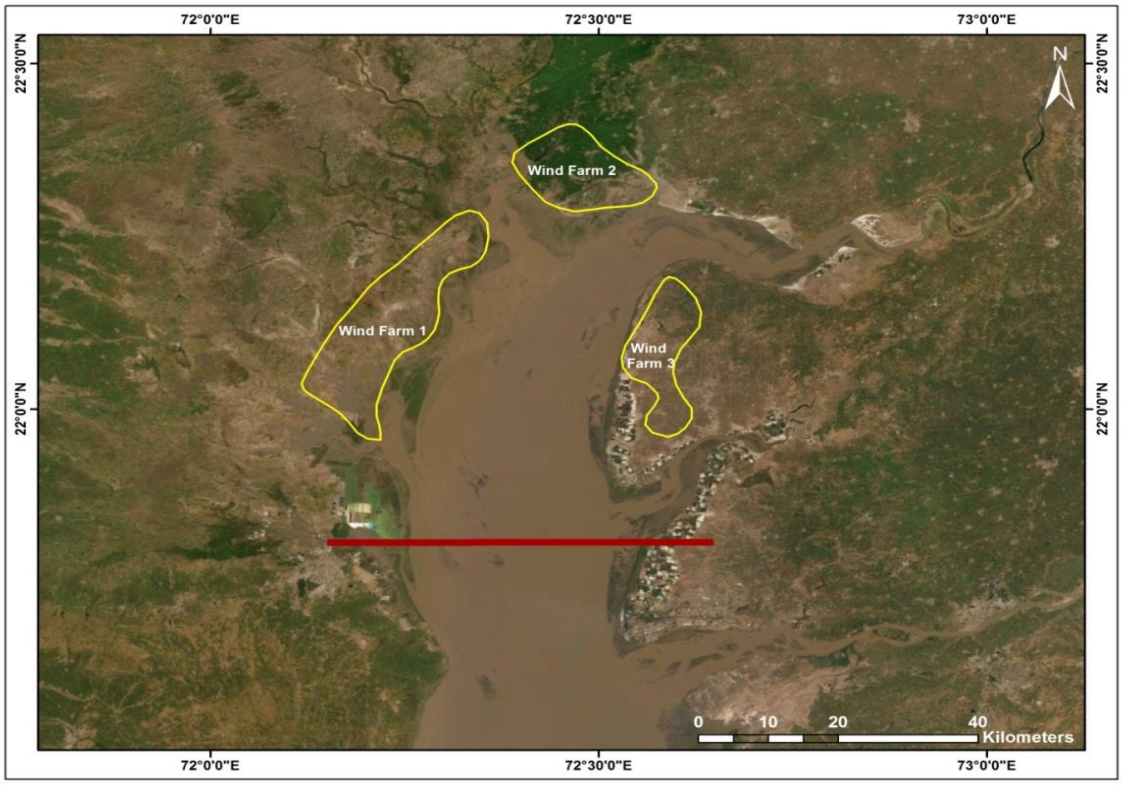


Figure 9: Layout of the Wind Farm Locations

1.2.3 Approach

Arista has a clearly defined methodology, the core principles of which allow reaching conclusions specific to each project and client requirement. The approach defined and adopted based on suitability to this project is mentioned below:

(1) Examining the brief shared by NCCR, project related environment, site visits, discussions and interaction with other stake holders and study groups;
(2) Identification of Hazards, Exposure, Vulnerabilities and an assessment the overall risk;
(3) Inception Report and Client's acceptance;
(4) Classification and Zoning of Assets as per Risk, keeping in mind geographical contiguity and administrative control;
(5) Establishing a tactical overlay on the design by incorporating Tactically Exploitable Features TEFs© towards integration of tactics with technology;
(6) Evolving a Security Concept applicable to the project; and
(7) Developing Mitigation Strategies, Security Master Plan, and identification of commensurate technology to meet requirements of Security Measures to be put in place.

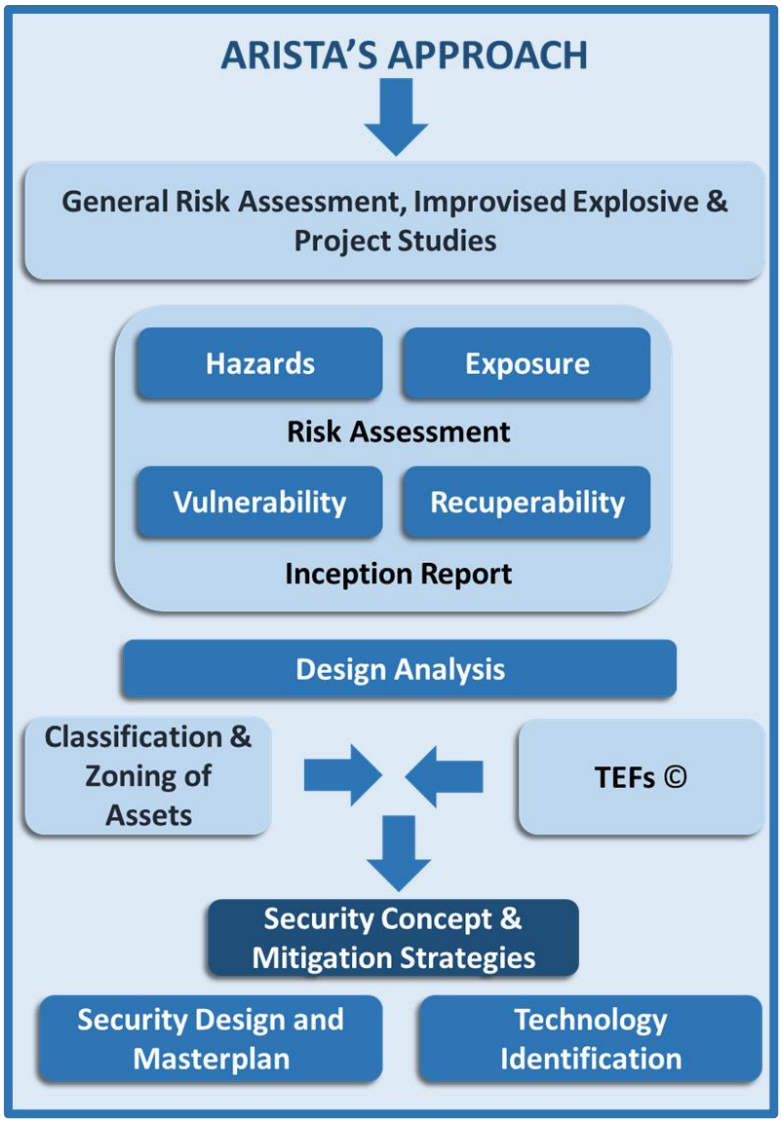


Figure 10: Arista's Approach

2
Components of Risk

2.1 Security Assessment

2.1.1 Country Level Assessment

India has seen many armed conflicts and external security challenges since independence with frequent hazards emerging based on a variety of factors and developments in its neighbourhood. The postures of our neighbours, their military capability and intent revealed with past incidents all together point to the fact that in times of aggression, our critical infrastructure especially in proximity and range of adversaries will be strategic targets.

India has also inherited a host of internal security issues since the country's independence with communalism posing a tremendous hazard to the social fabric of the nation. Over the years, India's internal security problems have multiplied due to linguistic riots, inter-state disputes and caste and ethnic tensions. Other hazards include the rise of religious extremism, militancy in Jammu Kashmir, North-East insurgency, and left-wing extremism. Transnational organized criminals/mafias have given further impetus by international terrorism to operate in India by forging linkages between organized crime and radicalism. Cyber is one of the newest and most critical challenges faced by India. Cyber-attacks on critical infrastructures, ransom ware attacks, propaganda and information warfare are some of the new tactics utilized by adversaries.

Both external and internal hazards put together present a serious challenge to security planners and the security forces mandated with its mitigation. While hazards during armed conflict are serious, their mitigation is beyond the scope of this study as the Armed Forces have their existing mechanisms to cater for the same. The detailed discussions in this study are therefore restricted to internal security and hazards thereof. At the same time in analysing Risk, the type of attacks during armed conflict and their impact on the dyke structure have been scored to ensure the adequacy of the design.

(a) Political Dynamics and the Security Environment

India is a multiparty democracy, with the government being elected every five years through elections being held for state and national parliaments. Also, India is a secular country wherein it gives no preference to any of the myriad religious, social and communal groups. The political system in India tends to engender coalition governments that lack the ability to push through economic reforms. Politically influenced polarization based on religion, caste, region etc. has always been a prominent security hazard to the nation. Some examples of this can be seen in the politically fuelled protests of the recent past such as the political opposition and nationwide protests against the Citizenship Amendment Act in late 2019, the Farmers' Protest starting in August 2020 which went on till December 2021, and

most recently, the protests against the Agnipath Scheme, these are all cases in point to politically driven hazards to infrastructure and security.

(1) **Political Unrest** - Political unrest manifests in India in varied ways. Not only opposition political parties but various pressure groups like students' unions, farmers unions, trade and labour unions etc. continuously disrupt the smooth functioning of the administration. Reservation movements like the 2016 Patidar reservation agitation in Gujarat; 2016, Jat reservation agitation, which spread into Uttar Pradesh, Rajasthan and NCR from Haryana, had witnessed huge losses to public infrastructure;
(2) **Youth Unemployment -**Due to lack of employment youth are the easiest to instigate during times of unrest and protest, either through politically appealing to their dissatisfaction or paying for their agitation. Youth protests and agitations are usually disorganized although they can turn violent if unchecked, trending towards vandalism and destruction of public and private property. In Bihar, in January, 2022, students allegedly stopped trains and set fire to coaches. The recent destruction of infrastructure during the protests against the Agnipath scheme is yet another case in point to youth led mob violence and destruction; and
(3) **Communalism**: Communal riots pose great difficulty to the administration along with loss of property and lives. India has seen some of the most violent communal riots since independence. Further, religious leaders and religion-oriented groups also try taking advantage of communal sentiments and inadvertently fuel further communal tensions leading to a simmering potential for further disharmony and violence.

(b) Terrorism

Recent times have seen a volatile mix of insurgent attacks punctuated by incidents of terrorism in the Indian Union Territory of Jammu and Kashmir. India faced more terror attacks on its soil in the first year of the Covid-19 pandemic, 2020, than in 2019; with 37% of these incidents being reported from Jammu and Kashmir, according to data compiled by the US State Department[1]. Overall, 679 terrorism-related incidents were reported in India in 2020, in which 567 people were killed (2% of global fatalities in terror attacks in 2020). In 2019, 655 terror attacks were recorded in the country, according to the US data. India was in the top 10 countries for most terrorism incidents in 2019. According to Global Terrorism Index, IEP 2022, India ranks 12, with a score of 7432, a marginal improvement two positions from 10th rank in 2021.

The available data points out to the fact that the states that experienced the most terror incidents were Jammu and Kashmir with 257 incidents (37.8%), Chhattisgarh with 145 incidents (21.4%), and Jharkhand with 69 incidents (10.2%). Among the perpetrators, CPI-Maoist continued to be the most destructive group in India and the fourth most destructive group in the world responsible for 298 incidents and 202 fatalities in 2020. They were behind 44% of the total (679) terror attacks in the country, while Lashkar-e-Taiba (LeT) and Hizbul Mujahideen were responsible for 6% of all incidents. According to the records, 29% of the terror incidents were not attributable to any outfit in India[2]. Pakistan has been continuously funding terror groups against India. Media reports suggest Daesh (formerly referred to as ISIL) and other groups are looking to attack targets in India, either directly or through instigating self-initiated attacks[3]. Similarly, Al Qaeda in the Indian Subcontinent (AQIS) has previously targeted India. Major terrorist groups that have

[1]https://www.hindustantimes.com/india-news/terror-attacks-rose-during-pandemic-year-in-india-us-report-101640542605120.html
[2]Chauhan, Neeraj. 2021. "Terror attacks rose during pandemic year in India: US report." Hindustan Times
[3]https://www.gov.uk/foreign-travel-advice/india/terrorism

been active in India include Lashkar-e-Tayyiba, Jaish-e-Mohammed, Hizbul Mujahideen, ISIS, al-Qa'ida in the Indian Subcontinent, and Jamaat-ul-Mujahideen. Indian forces arrested several members of al-Qa'ida ally Ansar Ghazwat-ul-Hind in J&K[4]. Critical Terrorist groups in India are as follows:

(1) **Islamic State -** IS has been attempting to increase its base in India by way of recruitment drives which are seeing some success regardless of the varied socioeconomic differences of the new recruits. In 2021, the National Investigation Agency foiled IS modules and arrested suspects from Delhi, Kerela and Karnataka linked to planned targeted killings[5]; and in 2022 the NIA arrested the family member of a former Karnataka MLA in relation to IS recruitment in India[6]. Indian recruits for IS have operated in various other countries and can pose a hazard to national security if and when they return with new and improved methods of perpetrating terror. For example, Syed Muhammad Arshiyan Haider, an electronic engineering graduate from Aligarh Muslim University, whose family home is in Ranchi, ended up using his skills in an Islamic State team that designed suicide drones and short-range missiles that revolutionised the arsenals of terrorist groups[7]. In 2017, Gujarat ATS foiled an IS module to target religious places by lone wolf attack[8]. According to a charge sheet filed by the NIA at a special court in Bangaluru, Islamic State inspired modules have identified Gujarat, West Bengal and Maharashtra to establish a caliphate by waging a violent jihad[9]. Security forces in 2019, said they had averted a possible terror attack in Assam and New Delhi by busting an IS terror module and arresting 3 persons[10]. It would, therefore, be safe to consider that the Islamic State poses a present and growing hazard to national security including but not limited to national infrastructure and development;

(2) **Jaish-e-Mohammed** - The Jaish-e-Mohammed (JeM) is a relatively new terrorist outfit, compared to other major outfits active in Jammu and Kashmir (J&K). It is an outfit formed, controlled and manned by Pakistan. The outfit was launched on January 31, 2000, by Maulana Masood Azhar in Karachi after he was released from an Indian jail, following the hijacking of the Indian Airlines Flight IC 814[11]. The Jaish-e-Mohammed is part of the Islamist terror network with its base in Pakistan and active in the terrorist violence in J&K. The outfit, like other terrorist outfits in J&K, claims to using violence to force a withdrawal of Indian security forces from J&K. Most Jaish-e-Mohammed attacks have been described as *fidayeen* (suicide terrorist) attacks. In this mode, terrorists of the outfit storm a high security target, including security forces' bases, camps and convoys. Their modus operandi includes suicide bombing and car bombs. The Jaish-e-Mohammed has largely confined its operations within J&K. The only recorded instance of its operations outside J&K has been the December 13, 2001, Parliament attack in New Delhi. However, several of its cadre have, on occasions been arrested or killed by security forces in states other than J&K;

(3) **Lashkar-e Taiba** - Lashkar-e-Taiba, an Islamist militant group, begun in Pakistan in the late 1980s as a militant wing of Markaz-ud-Dawa-wal-Irshad, an Islamist organization influenced by the Wahhabi sect of Sunni Islam. It sought ultimately to establish Muslim rule over the entire Indian subcontinent. Though based in Pakistan,

---

[4]https://www.state.gov/reports/country-reports-on-terrorism-2020/india/

[5]https://economictimes.indiatimes.com/news/defence/nia-cracks-down-on-isis-modules-13-premises-raided-in-six-states/articleshow/93258760.cms?from=mdr

[6]https://indianexpress.com/article/india/nia-arrests-ex-mlas-kin-for-suspected-is-links-7704874/

[7]Swami, Praveen. 2022. "Engineer from Ranchi built drones for IS, revolutionised terror tech. Now he's in Turkish jail." The Print

[8]https://www.business-standard.com/article/news-ani/gujarat-ats-foils-isis-plot-targeting-religious-place-117022600463_1.html

[9]https://economictimes.indiatimes.com/news/defence/is-modules-identified-guj-bengal-maha-for-caliphate/articleshow/86178652.cms?from=mdr

[10]https://economictimes.indiatimes.com/news/defence/isis-module-police-claims-to-have-averted-terror-attack-in-assam-and-new-delhi/articleshow/72239065.cms?from=mdr

[11]https://www.business-standard.com/article/current-affairs/what-is-jaish-e-mohammed-all-you-need-to-know-116010400219_1.html

Lashkar-e-Taiba initially operated in the Indian state of Jammu and Kashmir, on the Pakistan-India border, but by the first decade of the 21st century the group had expanded its reach farther into India. LeT became known to Indian intelligence circles when LeT militants killed sixteen Hindus in Kashmir in 1996 and, following this, LeT was implicated in the New Delhi attacks in 2001 and 2005, the 2006 Bangalore, Nagpur and Varanasi attacks, the 2007 train bombings in Mumbai, and, ultimately, the 2008 Mumbai attacks[12];

(4) **Indian Mujahideen** - According to Indian intelligence, the IM is not a well-knit organization with a hierarchical structure like other more established groups such as the LeT. Rather, it is a loose network of Islamic organizations which includes the Students' Islamic Movement of India (SIMI), certain individuals from the state of Uttar Pradesh with alleged links to the Harkat ul-Jihad-e-Islami (HuJI), and the terror cartel of Aftab Ansari. One plausible reason for individuals forming the IM could be their personal experiences during the Gujarat riot of 2002[13]. NIA reports suggest the group was working on targeting different areas with IEDs;

(5) **Maoists** - Left Wing Extremism poses a significant hazard to India. The States of Chhattisgarh, Jharkhand, Odisha, Bihar, West Bengal, Andhra Pradesh, Telangana, Maharashtra, Madhya Pradesh and Kerala are considered LWE affected, although in varying degrees. On May 28, 2010, a Jnaneshwari Express train was derailed with a bomb by Maoists in the West Midnapore district of West Bengal, India near Jhargram. In 2010, Left-wing extremists unleashed 278 attacks on government buildings and infrastructure works across seven states, destroying 33 schools, 20 panchayat offices, 105 roads/culverts and 38 communication towers[14]. Railways continue to be a favoured target, having recorded 22 Naxal attacks until October 31, 2010. Among the perpetrators in India, CPI-Maoist continued to be the most destructive group in India and the fourth most destructive group in the world responsible for 298 incidents and 202 fatalities in 2020; and

(6) **Samundri Jihad**: Reports in October 2018 and September 2019 claimed terrorists, based out of Pakistan, may be planning attacks on installations like ports, cargo ships and oil tankers in India. The alert came in the backdrop of reports that the LeT has been increasing its capabilities to strike India via sea. The report also claimed terrorists are also being trained in swimming and deep diving by the Jaish-e-Mohammed (JeM), another Pakistan-based terrorist organisation. As per intelligence inputs which the Navy and the Coast Guard received[15], it was learnt that LeT's affiliate organisations like Falah-e-Insaniyat Foundation, Al Dawa Water Rescue, Life Line Water Rescue and Rescue Mili Foundation have been training terrorists in deep water diving at several locations in Punjab province. The plan may also have been be to push suicide attackers through sea and inland water channels[16].JeM, on the other hand, has been training its cadre in 'Samundri Jihad' in Bhawalpur. The matter was corroborated by the Ministry of Home Affairs in answer to a parliamentary question raised in January 2019.

---

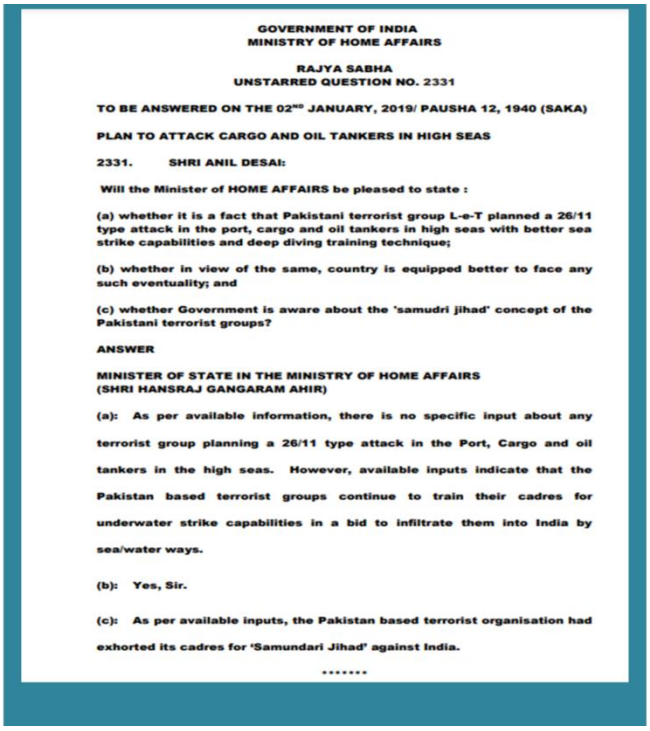
[12]The European Foundation for South Asian Studies. 2021. "Al-Qaeda, ISIS and Lashkar-e-Taiba: Know their modus operandi in South Asia and Europe." India Blooms

[13]Goswami, Namrata. 2009. "Who is the Indian Mujahideen?" Manohar Parrikar Institute for Defence Studies and Analysis

[14]Jain, Bharti. 2010. "Maoist key result area: Destruction of 33 schools, 105 roads, 13 rly properties." The Economic Times

[15] https://www.timesnownews.com/india/article/samundri-jihad-india-navy-coast-guard-put-on-high-alert-for-lashkar-e-toiba-jaish-e-mohammed-attacks-on-ports-cargo-ships-oil-tankers-pakistan-mumbai/298270

[16]September 9, 2019https://www.indiatoday.in/india/story/50-jaish-terrorists-training-in-deep-diving-may-launch-attack-on-india-via-sea-bsf-sources-1597267-2019-09-09



GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

RAJYA SABHA
UNSTARRED QUESTION NO. 2331

TO BE ANSWERED ON THE 02ND JANUARY, 2019/ PAUSHA 12, 1940 (SAKA)

PLAN TO ATTACK CARGO AND OIL TANKERS IN HIGH SEAS

2331. SHRI ANIL DESAI:

Will the Minister of HOME AFFAIRS be pleased to state :

(a) whether it is a fact that Pakistani terrorist group L-e-T planned a 26/11 type attack in the port, cargo and oil tankers in high seas with better sea strike capabilities and deep diving training technique;

(b) whether in view of the same, country is equipped better to face any such eventuality; and

(c) whether Government is aware about the 'samudri jihad' concept of the Pakistani terrorist groups?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI HANSRAJ GANGARAM AHIR)

(a): As per available information, there is no specific input about any terrorist group planning a 26/11 type attack in the Port, Cargo and oil tankers in the high seas. However, available inputs indicate that the Pakistan based terrorist groups continue to train their cadres for underwater strike capabilities in a bid to infiltrate them into India by sea/water ways.

(b): Yes, Sir.

(c): As per available inputs, the Pakistan based terrorist organisation had exhorted its cadres for 'Samundari Jihad' against India.

.....

Figure 11: Response to Parliamentary Question

(c) Crime

The total number of crimes under both the IPC and SLL across the country for all the States and Union Territories in 2020 went up to 66, 01,285, which was a 28%increase from 51, 56,158 in 2019 and a 30%increase from 50, 74,635 in 2018. The crime rate registered per lakh of the population increased from 385.5 in 2019 to 487.8 in 2020. A number of 51,606 rioting cases were registered. The cases of offences against public tranquillity have increased by 12.4% in 2020 over 2019. The cases registered under offences against property have decreased by 24.6%. During 2020, maximum cases reported were of theft (4, 93,172 cases), followed by burglaries (86,223 cases), accounting for 76.6% and 13.4% respectively. Out of 5,613 cases, 80.6% of cases were registered under The Prevention of Damage to Public Property Act (4,524 Cases) followed by 796 (14.2%) cases under The Unlawful Activities Prevention Act. A total of 50,035 cases were registered under Cyber Crimes, showing an increase of 11.8% in registration over 2019 (44,735 cases)[17]

(d) Capability of Domestic Forces

The Ministry of Home Affairs is mandated with maintenance of internal security in India. The elite National Security Guard is India's special response force for anti-hijacking, counter-terrorism, hostage rescue, and other 'special' operations including duties like bomb disposal and creation and management of bomb data centres. The force has 7000+ active personnel and special air support is available to them.

The Central Reserve Police Force is another highly decorated force involved in riot control, counter militancy/insurgency, dealing with left wing extremism, protection of VIPs

[17]National Crime Records Bureau, Crime in India 2020.

and vital installations, fighting aggression during War time, rescue and Relief operations at the time of natural calamities etc. It has a specialized wing for crowd and riot control called the Rapid Action Force (RAF). One of the vital roles of the CRPF, which is not very evident, is guarding vital Central Govt. installations such as Airports, Powerhouses, Bridges, Doordarshan Kendras, All India Radio Stations, residence of Governors and Chief Ministers, Nationalised Banks and other Government establishments in insurgency affected States. With 246 battalions and various other establishments, the CRPF is considered India's largest central armed police force and has a sanctioned strength of more than 300,000 personnel as of 2019[18].

The Central Industrial Security Force is a premier multi-skilled organization with a present strength of 1, 63,590 personnel. The CISF provides security to some of India's most critical infrastructures like nuclear installations, ISRO facilities, seaports, power plants etc[19].

The National Disaster Response Force (NDRF) is an Indian specialized force constituted "for the purpose of special response to a disaster situation or disaster" under the Disaster Management Act, 2005. At present, NDRF has a strength of 12 Battalions with each Battalion consisting of 1149 personnel[20].

Apart from these organizations there exists the Border Security Force, Assam Rifles, Indo-Tibetan Border Police, Sashastra Seema Bal and various state police forces who work in tandem and with intelligence inputs from the Intelligence Bureau and other state intelligence agencies. There are premier investigative agencies as well like the Central Bureau of Investigation (CBI) and National Investigative Agency (NIA) with a high efficiency rate.

(e) Major Incidents

India ranks 12th in the Global Terrorism Index 2022 as per data published by the Institute of Economics and Peace, Australia[21]. In 2021 a total of 314 terror related incidents were recorded in India with a 116 civilian and 104 security personnel losing their lives[22]. For the purpose of this report, some of the major incidents of terrorism, violence and unrest in the recent years are highlighted below:

Table 3: Major incidents of Terrorism, Violence and Unrest in India

S. No	Hazard Type	Event Description	Source/ Group
1.	Terrorism and Militancy	12 coordinated shooting and bombing attacks in Mumbai, 2008	Lashkar e Taiba (LeT)

[18]https://crpf.gov.in/history-crpf.htm

[19]https://www.cisf.gov.in/cisfeng/about-us/

[20]https://ndmindia.mha.gov.in/state-response-force#:~:text=National%20Disaster%20Response%20Force%20(NDRF)&text=At%20present%2C%20NDRF%20comprise%20of,Andhra%20Pradesh%20and%20Arunachal%20Pradesh.

[21]https://reliefweb.int/report/world/global-terrorism-index-2022

[22]www.satp.org/datasheet-terrorist-attack/fatalities/india

2.		2019, car laden suicide bomber hit armed police vehicle causing huge casualty on Jammu Srinagar National Highway	LeT and Jaish e Mohammed
3.	Violence and Unrest	2016, Jat reservation movement. The riots were estimated to have caused a loss of ₹340 billion (US$4.5 billion) in northern India	Jat Groups
4.		2019, CAA protest in Delhi, 22 people killed in Uttar Pradesh. Loss to public property as well.	Opposition Political Parties, Religious Interest groups
5.		2020, North East Delhi Riots. Communal riots causing loss of life and property	Hindu-Muslim Groups
6.		2021, Poll bound violence in West Bengal, communal hatred	Political Parties and Interest groups
7.		2021, Farm Law Protest, disruption of movement, loss to public property	Farmers Union, Political Parties and Interest groups

2.1.2 Security Assessment - Gujarat

(a) Overview

Gujarat is a state on the Western Coast of India with a coastline of about 1,600 km (990 mi) which is the longest mainland coastline in the country. Gujarat is recognized as one of the leading industrialized states of India, contributing to around 20% share in India's industrial production and merchandise exports. Towards the extreme West, Gujarat has the Arabian Sea as well as a land border connected to Pakistan due to which the possibility of infiltration of terrorists always remains high.

(b) Terrorism

In the last 20 years, Gujarat has had a few major terror related incidents. In one of the major incidents, on 24th September, 2002, the Swaminarayan Akshardham Temple at Gandhinagar was attacked by two terrorists killing 33 and injuring more than 80 people[23]. Terrorists carried letters in Urdu which affirmed their connection with a previously unknown terror group called Tehrik-E-Kasas (Movement for Revenge).

In 2008, 17 serial bombings took place in the capital city Ahmedabad killing 56 and injuring over 200 individuals[24]. Abdul Subhan Qureshi, accused in the 2008 Ahmedabad blasts, was in contact with founder leader of Indian Mujahideen, Riyaz Bhatkal. Earlier, in 2006, a bomb blast attack took place in Ahmedabad railway station injuring 25

[23]https://www.hrw.org/reports/2003/india0703/Gujarat-06.htm

[24]https://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=200807260009

individuals[25]. A number of suspected militants continue to be arrested from cities like Surat and Ahmedabad.

Since 2015 there have been no major terror attacks involving high-profile public locations (such as government buildings, public squares and restaurants or foreign owned commercial assets or personnel) in the Gujarat. However, there have been reports in recent times when intelligence agencies have warned Gujarat Police of the possibility of terror attacks in Gujarat as well as Islamic State attempts to open modules in Gujarat to further establish their caliphate[26].

Gujarat has not been untouched by terrorism, and though most of the incidents of terrorism in Gujarat are claimed to be related to the communal riots and clashes in the state in 2002, the state's proximity to Pakistan via the sea route, exposes it as a soft target for jihadis and smugglers. To counter possible hazards from smugglers and terror outfits targeting the Gujarat coast, the Indian Navy in 2015, integrated eight coastal radar stations in the state under the National Command Control Communication Intelligence (NC3I) program. The commissioning of INS Sardar Patel naval base enhanced the NC3I intelligence network[27].

(c) Unrest

(1) **Communal Unrest -** Gujarat has big history of communal and religious unrests from its past. There have been many riots and clashes between locals in different parts of the state. Other than 2002 Godhara riots, in 2006 riots happened in Vadodara. The riots were caused by the municipal council's decision to remove the dargah (shrine) of Syed Chishti Rashiduddin, a medieval Sufi saint. The shrine was between two and three hundred years old. The incident resulted in six to eight people being killed and forty-two injured, 16 of these casualties were from police shooting[28].In Apr 2022, communal tension engulfed three districts – Sabarkantha, Anand and Dwarka on April 10 as Ram Navami processions ended in violence in Sabarkantha and Anand. A Ram Navami rally with loud music passing through Shakkarnagar, a Muslim-dominated area of Khambat, was objected to by the local residents. Soon, the situation escalated into a communal clash[29].Notably, Khambhat has emerged as a hot spot for communal tension since 2002. As per Buniyaad, a minority rights organization based in Gujarat, in February 2012, a dispute over the construction of shops on land under the Waqf Board in Khambhat ended up in large-scale riots. The mobs used acid bulbs, petrol bombs, stones and torched six homes. In November 2016, a minor incident of a Muslim autorickshaw driver colliding with the motorcycle of a person from the Ravar community in Pith Bazar area turned into a riot. The riots, which began with members of both communities pelting stones at each other, spread to neighbouring areas of Rana Chakla, Madai and Vasdavad in Khambat. In the years 2017 and 2018, Khambhat saw sporadic incidents of communal tension. Subsequently, the state government imposed the Disturbed Areas Act in the town that bars sale of property between two religious' communities without prior permission from district authorities. However, that did not stop incidents of communal clashes in Khambhat.

(2) **Labour Unrest -** During the year 2017, 19 incidences of strikes and lockout have been reported which have affected 5286 workers and the total 39779 man-days were lost.

[25]https://www.satp.org/satporgtp/countries/india/database/railwayattack.htm

[26]https://economictimes.indiatimes.com/news/defence/is-modules-identified-guj-bengal-maha-for-caliphate/articleshow/86178652.cms?from=mdr

[27]https://indianexpress.com/article/cities/ahmedabad/eight-coastal-radar-stations-in-state-integrated-with-naval-intel-network/

[28]https://www.indiatoday.in/magazine/states/story/20060515-vadodara-civic-body-demolishes-dargah-in-clean-up-drive-situation-turns-communal-785347-2006-05-15

[29]https://www.newsclick.in/Gujarat-1-Dead-Violence-Ram-Navami-Processions-Muslim-Majority-3-Districts

While during the calendar year 2018, 13 incidences of strikes and lockout have been reported which have affected 5226 workers and the total 43448 man-days were lost[30]. In the year 2019 (up to October, 2019) 6 incidence of strikes and lockout were reported which affected 2047 workers and the total 28834 man days were lost[31].While Gujarat has been trying to project itself as an industry and labour friendly state, the fact remains that Gujarat has indeed seen some unionisation in the recent past. This is natural in the sense that as the industry grows, there is larger congregation of labour, awareness of rights and politicisation of unions. One does not see much unionisation at the Sanand factories, which houses big manufacturing units like Tata Motors and Ford India, apart from their global vendors, Hitachi Hi-Rel Power Electronics, Nestle, Teva, Bosch Rexroth. Industry insiders feel the reason behind the lack of unionisation at Sanand is that it is a relatively new industrial estate. The older ones like Halol have had their fair share of labour issues. All unions sooner or later become politically affiliated. Though the government is pushing for Labour reforms, it would need political maturity, a strong will, and the compulsion to meet industry needs in a time bound manner post a major pandemic. Another major area of concern is the migrant workers who also form a significant part of the work force. In Oct 2008, Sanand, a major industrial hub near Ahmedabad housing around 250 big and small industrial units, faced disruptions for at least three days as most of the factories remained shut with migrant workers staying away from work in the wake of violence following an alleged rape incident. In May 2020, migrant workers in industrial belt of Mora and Hazira clashed with the police when they were pressing for their demand to return to their native villages during COVID-19 lockdown. About 150 workers were arrested in various parts of the state and because of that, workers were reluctant to return to work on re-opening

(3) **Environment and Land Unrest -** Infrastructural projects such as construction of dykes, road widening etc. affects the locals in the vicinity of such projects the most. There have been many protests by locals, landless Dalits and Adivasis in Gujarat against the decision to allot wastelands to corporate for farming instead of distributing the same to the landless Dalits and Adivasis. Gujarat Dalit Sangathan, Saurashtra Dalit Sangathan and Adivasi Mahasabha Gujarat on November 26, 2018 came together to hold a mass protest in Gandhinagar against the government for planning to give 45 Lakh hectares of cultivable wasteland to corporate for farming[32]. Protesters said that the Government did not go back on the provision of the Land Ceiling Act, 1961 that talked about giving land to the landless people in the Dalit community for farming. In another case, in January 2019, farmers in Bhavnagar district came together to oppose limestone mining on fertile land. The protest took place in Mahuva tehsil but turned violent as the dissenting residents clashed with the police and pelted stones, injuring four policemen[33]. Many farmers were also injured as the police lobbed teargas shells to control the crowd. They claim that limestone mining is a hazard to their agriculture and livelihood. Recently in March 2022, tribals protested against the Par Tapi Narmada link project over displacement of 61 villages. About 6,065 hectares of land area will be submerged due to the proposed reservoirs, affecting a total of 61 villages in Gujarat and Maharashtra, of which one will be fully submerged and the remaining 60 partly. In Gujarat, 793 families from 17 villages will be affected by the Kelwan reservoir, 563 families by the Dabdar reservoir across 11 villages, 379 families by Chasmandva reservoir spread over seven villages, 345 families would be affected by Chikkar reservoir across nine

[30]Socio-Economic Review Gujarat State : 2018 - 19

[31]Socio-Economic Review Gujarat State : 2019 - 20

[32]https://www.landportal.org/news/2018/11/dalits-adivasis-protest-gandhinagar-land-rights

[33]https://www.landconflictwatch.org/conflicts/farmers-oppose-limestone-mining-on-fertile-land-in-gujarat-s-bhavnagar-district

villages and 331 families would be affected due to Paikhed reservoir spread over 11 villages. The centre dropped the project on March 29, 2022 after these mass protests[34].

(d) Crime

Gujarat saw an increase in the number of criminal cases under the Indian Penal Code (IPC) registered during the lockdown in 2020. The number of reported criminal cases went from 1.39 lakh in 2019 to 3.81 lakh in 2020. According to the NCRB-Crime in India 2020, Gujarat has the highest charge sheeting rate at 97.1% in 2020, which is highest among all states and Union Territories across the country[35].

According to government figures, crime against Scheduled Castes have increased by 32% while crimes against Scheduled Tribes by 55%. The crime figures of Gujarat shared in the Legislative Assembly in 2021 revealed that on average two murders, four incidents of rape and six kidnappings occurred every day in the state in the last two years. As many as 1,944 murders, 1,853 incidents of attempt to murder, 3,095 rapes and 4,829 incidents of abduction and over 14,000 cases of suicide were reported in different parts of the state in the last two years ending December 31, 2020, according to data shared by the state home department.

There were as many as 933 cases of attempt to murder in the year 2020, around 3874 other thefts and 2704 burglary cases reported. Cases of land disputes and property disputes are low in the state[36].

(e) Major Incidents

For the purpose of this report, some of the major incidents of terrorism, violence and unrest in the state in the recent years are tabulated below: -

Table 4 : Major incidents of terrorism, violence and unrest in Gujarat

S.No.	Hazard type	Event description	Source/group
1.	Terrorism	2002 Akshardham Temple Attack in Ahmedabad	Jaish-e-Mohammad (JeM), Lashkar-e-Taiba (LeT) and the lesser known Tehreek-e-Kasas
2.		2006 Ahmedabad Railway station Bombing	Madrasa students involved with the Lashkar-e-Taiba (LeT)
3.		2008 Ahmedabad Bombings	Indian Mujahideen along with Harkat-ul-Jihad-al-Islami
4.		2015 double murder of BJP leaders in Bharuch	Local module of Dawood Ibrahim gang (Islamic Extremists)

[34]https://www.hindustantimes.com/india-news/river-linking-project-stalled-in-gujarat-after-tribals-protest-101648636472890.html
[35]https://timesofindia.indiatimes.com/city/ahmedabad/crime-in-gujarat-doubled-in-lockdown-year-ncrb/articleshow/86243901.cms
[36]https://ncrb.gov.in/sites/default/files/CII%202020%20Volume%201.pdf

S.No.	Hazard type	Event description	Source/group
5.	Violence and Unrest	2002 Godhra Communal Riots	Hindu-Muslim groups
6.		2006 Vadodara Communal Riots	Hindu-Muslim groups
7.		2013 Bombardier's Savli plant labour strikes in Vadodara District	Makarpura GIDC Employees Union affiliated with Communist Party of India's Labour wing AITUC (All India Trade Union Congress)
8.		2019 Bhavnagar farmers' protest against limestone mining	Local residents and farmers
9		2022 Ram Navami Communal Clash in three districts of Sabarkantha, Dwarka, and Anand	Hindu-Muslim groups
10.		2022 Farmers protests against inadequate power supply	Farmers' Unions with support from Opposition parties in the State Legislative Assembly
11.		2022 Protests against Par-Tapi-Narmada project	Tribal groups

2.1.3 Global Dyke Related Incidents

Dykes and associated infrastructure such as power generation facilities, transport carriageways, railways, canals etc. are a national asset and contain a number of critical components whose destruction or disruption could cause catastrophic results. These could range from casualties, severe flooding, widespread property damage, failure of power supply, transportation or water etc and may have long term consequences. These could even cause structural failure of the dyke infrastructure as well. Certain characteristics of dykes make them difficult to protect because of limitations in controlling access. They are large, can be approached by land, air or water and are often located in remote areas. Most dykes are engineered and built to be robust and can withstand extreme conditions but they still have a few vulnerabilities that could be exploited by potential adversaries or anti-national elements to cause structural damage or to disable or disrupt operations or critical functions.

There are an infinite number of possible combinations of resources, tactics, tools and weapons that could be deployed against dykes in attacks carried out by individuals, small teams of a few persons, or larger groups acting in a coordinated fashion.

Each attack type could be further divided into feasible attack vectors, representing different severity levels (e.g., depending on the number of explosives, the size of the attack force, and the sophistication of the attack planning process). The attack vectors could be defined to span a feasible range of capabilities, from simple attacks to more elaborate operations. In addition, attack types could be further categorized based on the assumed characteristics of the adversary. For example, some types of attacks may be conducted by adversaries with limited resources who may discontinue operations if they are compromised during initial phases. The use of small arms or man-portable explosive devices could be associated with these types of adversaries. However, other types of attacks could be conducted by well-trained adversaries with access to significant resources and backing from state-funded terrorist organizations. These "high level" attacks could involve adversaries fully committed to gaining access to the target with intent to cause significant damage. Vehicle-borne or water-borne explosive devices could represent potential examples of the types of attacks that more sophisticated adversaries might attempt.

Following is an overview of 25 attacks on dykes worldwide between 2001 and 2011 as per available compiled data. These events, which represent attacks on impoundments, power-generation equipment, control facilities, and appurtenant structures, are summarized in the following table.

Table 5 : Dyke Attacks 2001 - 2011

Dyke Attacks Summary				
Facility	Country	Date	Attack Type	Attacker Type
Lhokseumawe Reservoir	Indonesia	August 17, 2001	Explosive Device	Separatist (Suspected)
Panauti Plant	Nepal	November 24, 2001	Explosive Device	Communist Insurgent-Maoist (Suspected)
Kidapawan Reservoir	Philippines	March 19, 2003	Standoff Weapons (Rockets)	Islamic Insurgent (Suspected)
Kajaki Dyke	Afghanistan	May 2, 2003	Standoff Weapons (Rockets)	Islamic Insurgent
Gomal Zam Dyke	Pakistan	September 21, 2004	Assault Team	Islamic Insurgent
Zelenchuck	Russia	September 21, 2004	Assault Team	Islamic Separatist
Dumarao	Philippines	December 15, 2004	Explosive Device	Communist Insurgent (Suspected)

Dyke Attacks Summary				
Facility	Country	Date	Attack Type	Attacker Type
Selaghat Dyke Project	Nepal	December 19, 2004	Explosive Device	Communist Insurgent-Maoist (Suspected)
Mirani Dyke	Pakistan	May 18, 2005	Explosive Device	Unknown
Haditha Dyke	Iraq	August 2, 2005	Explosive Device	Unknown
Haditha Dyke	Iraq	September, 2005	Standoff Weapons (Rockets)	Islamic Insurgent
Kajaki Dyke	Iraq	September 17, 2005	Explosive Device	Islamic Insurgent
Hlaingbwe Dyke	Burma	May, 2007	Explosive Device	Separatist (Suspected)
Hlaingbwe Dyke	Burma	September 2, 2007	Standoff Weapons (Mortar)	Separatist (Suspected)
Waeng Station	Thailand	August 1, 2007	Explosive Device	Islamic Separatist
Kajaki Dyke	Afghanistan	March 30, 2008	Explosive Device	Islamic Insurgent
Tipaimukh Dyke	India	April 26, 2008	Assault Team Explosive Device	Unknown
Mosul Reservoir Dyke	Iraq	May 1, 2009	Explosive Device	Unknown
Balimela Power Station	India	December 19, 2009	Incendiary Device	Communist Insurgent-Maoist (Suspected)
Mytikyina Dyke	Burma	April 17, 2010	Explosive Device	Ethnic Separatist
Thawt Yin Kha Dyke	Burma	April 27, 2010	Explosive Device	Ethnic Separatist

Dyke Attacks Summary				
Facility	Country	Date	Attack Type	Attacker Type
Black Rock Dyke	United States	July 4, 2010	Incendiary Device	Unknown
Baksan Power Plant	Russia	July 20, 2010	Assault Team Explosive Device	Islamic Separatist (Suspected)
Machlagho Dyke	Afghanistan	July 18, 2011	Assault Team	Unknown
Thawt Yin Kha Dyke	Burma	July 20, 2011	Standoff Weapons (Rockets)	Ethnic Separatist (Suspected)

(Source - Worldwide Attacks Against Dykes - US Department of Homeland Security)

2.1.4 Recent Incidents of Interest

Recent incidents of attacks on dykes include the attack on Salma Dyke near Herat, Afghanistan by Taliban in which 16 security personnel were killed in July 2021. Taliban attacked a check point near the dyke and took over the dyke. In India, specific hazard warnings against various dykes have been issued from time to time, including Narmada dyke in 2010, Bhakra Nangal Dyke in 2012 and the latest being issued by the Intelligence Bureau in Mar 2022 regarding safety of dykes in Kerala especially the Idukki Hydro Electric Project after which the security of the project has been enhanced and risk assessment of all dykes in the state is being undertaken to institute suitable measures. Two incidents in the last couple of months in India, targeting water structures/ facilities highlight such risks. These incidents point to the intent of inimical elements and thus need to be taken seriously by security planners and designers. News cuttings are as below.

CID probes dyke 'sabotage' that flooded Silchar, 4 held

Mukut Das & BB Goswami | TNN

Guwahati/Silchar: A CID probe began Tuesday into an alleged act of sabotage in Assam's Cachar district that led to the rain-fed Barak river swamping Silchar through a cut in a dyke, leaving almost the entire town flooded since June 20. Four residents of the district – Kabul Khan, Mithu Hussain Laskar, Nazir Hussain Laskar and Ripon Khan – were arrested over the weekend for their alleged involvement in causing the breach in the dyke. IGP Debaraj Upadhaya said a CID team stationed in Silchar had begun looking into various possibilities, although the case is formally yet to be handed over to the agency.

On whether his team had got any leads, the IGP said, "Making any remark at this point would be premature."

SWAMPED: A June 23 aerial view of flooded Silchar

The four arrests between July 2 and 3 came a whole five weeks after the water resources department lodged a police complaint on May 23 about "unknown miscreants" cutting a portion of the dyke at Bethukandi. The probe gained traction after CM Himanta Biswa Sarma visited south Assam's largest town around a fortnight ago to survey its worst episode of urban flooding in memory. Sarma pointed to the alleged sabotage as the cause of Silchar's flood misery, leading the police to swing into action and arrest the four suspects. He visited the Bethukandi dyke and assured residents of strict action against those responsible for their plight. "A case has been registered by the CID and a special task force will monitor the investigation," the CM said.

Kabul was the first to be arrested, based on a video purportedly depicting the alleged sabotage. The other three were rounded up on Sunday following which all four men were taken to Guwahati for further investigation. Sources said the arrested men claimed they were trying to flush out rainwater from a marshland into the river, not realising that heavy rain thereafter would trigger the opposite of what they set out to do.

Hackers target WRD's flood monitoring system

TIMES NEWS NETWORK

Panaji: Goa police registered a FIR against an unknown person after the flood monitoring system of the water resource department (WRD) came under a ransomware cyber-attack and hackers demanded bitcoin cryptocurrency to decrypt the data.

PI Rahul Parab said that they have asked the representatives of the Hyderabad-based software developer ASTRA Microwave Products Ltd to join the investigation to trace the accused.

WRD executive engineer Sunil Karmarkar said that the attack was carried out on June 21 between 12am and 2 am.

Figure 12: News Articles of Recent Incidents

2.1.5 Analysis of Field Inputs on Security

Various security forces and agencies were consulted to take their views on the likely hazards and also to understand their concerns and limitations, if any, towards mitigation of these hazards. Existing infrastructure and assets were also considered in evaluating the risk matrix. Each of these organisations is a specialist in their respective sphere and has a unique viewpoint. The following agencies were approached for consultation:

Table 6 : Agencies Approached for Consultation

Ser	Organisation	Contact Person	Nature of Discussion
1	N, WR, WS & Kalpasar Department	Mr JK Chaturvedi, Superintendent Engineer	In-Person discussions
2	South Western Air Command, Indian Air Force	Gp Capt GS Sidhu	Telephonic Discussions
3	Commander Coast Guard Region (NW), ICG	Sh Pankaj Agarwal, DIG	In-Person Discussions
4	Flag Officer Commanding, Gujarat Naval Area, Indian Navy	Cdr Vikas Sheoran	In-Person Discussion
5	Border Security Force	Sh ML Garg, DIG	In-Person Discussions
6	National Institute of Advanced Studies	Dr Anshuman Behera	Video Conference

(a) Social Impact Study Inputs from NIAS

At the time of discussions, although the social impact study is yet to be completed, it has emerged that the local population is largely unaware of the project at the moment. The local political leaders, village heads and land owners are aware but the information has not yet percolated down to the rest of the population. Another factor to consider is that the dyke area, especially the envisaged reservoir, is not heavily populated, barring a few villages, and most of the land is revenue land. Due to the nature of soil and topography, the Gulf of Khambhat is a seasonal marshland with few streams of brackish water which remain active post monsoon. The marsh does not provide much grazing for livestock; however, fishing for self-sustenance is undertaken by a few villagers upstream of the proposed dyke. There are no major fishing communities upstream of the dyke and mechanised fishing is not undertaken in the gulf due to shallow depth and silt in the water. At the Bhavnagar end of the proposed dyke, most of the land is marshy and has salt pans that are leased for a limited time by the government. With sparse population and little private landholding, the local population is likely to be largely neutral to the dyke project. A few influential individuals

who own lands in the area will be affected and may oppose the project. However, most of them are amenable to the ruling dispensation and a few words from the top leadership may alleviate their opposition.

Area close to the approach road and dyke end has small villages of Kala Talav and Khetakhatli. There is no agriculture in the area and the population largely works in the 'Nirma' plant at Kala Talav, Bhavnagar. Nirma Ltd is a big company and the plant at Kala Talav produces salt, soaps and detergent etc for which sea water is a major constituent. Presently the plant enjoys free access to salt water of the gulf and discharges its waste in the gulf without having a need for a treatment plant for effluents. Although the plant is sited above the envisaged reservoir level and there is no likely hazard of damage to physical infrastructure or need to relocate, access to salt water will be stopped once the dyke is built. The plant will also have to create an effluent discharge system for discharging waste on the downstream side of the dyke. This would entail laying a water supply and discharge pipeline system with associated pumps and treatment units that would run for a few kilometres. Needless to say, Nirma Ltd is likely to be hostile to the project. The possibility that it can rally the local population, which depends on Nirma for sustenance, may need to be addressed by sustained outreach and interaction by local political leaders and government machinery. It was also brought out that Nirma Ltd has encroached over 35000 acres of revenue land in the upstream area, which will become part of the reservoir once the dyke is built. It is unlikely that Nirma Ltd will be amenable to the project implementation. The local population can be encouraged to relocate from the area by providing them alternate accommodation in a semi-urban area. Since they are not tied to the land by way of ownership, alternate housing with better facilities than presently existing in their village will motivate them to move out. Downstream of the dyke, Ghogha is a census town/taluka with a large Muslim population and it is indicated that radicalisation is taking place in the name of religion and religious cause in Kashmir. This can be a cause for concern if not checked as Ghogha is close to the dyke and dyke infrastructure can easily be targeted from here. A little further down is the village of Kuda which depends on fishing in the gulf for sustenance. As the catch is small and there are no mechanised trawlers, locals do not engage in much trade of fish and would be happy to relocate if given better facilities.

At the Dahej end of the dyke, proximity to Bharuch and Ankleshwar brings prosperity to the region and most locals work in the various industrial units that dot the area. Density of population is higher and, with larger landholding coupled with higher land prices, opposition to the project is likely. The villages have sizeable Muslim populations and radicalisation cannot be ruled out, given that the social impact study team was not allowed to interact with the Muslim residents. Jolva is a prominent village in the area and is understood to be the political centre of the local area. It was indicated that the local leader is unlikely to be supportive of the project.

(b) Inputs from Security Forces in the Location

Interactions with the Indian Coast Guard indicated that the dyke, once constructed, would be a vital asset and, due to its size, provide a large target area to any inimical element. Merely the act of disrupting operations, even without physical damage to infrastructure, would garner a lot of media attention and give a boost to the perpetrators. In order to prevent such an occurrence, 24x7 monitoring would be necessary to deter hazards both from the upstream and downstream sides. Towards this, strategically located cameras, radars, EO/IR (Electro Optical/Infra-Red) cameras and areal monitoring by drones is recommended with live feed being provided to a central operations room. Monitoring of

cargo at commercial ports in the vicinity will be vital since the downstream side has an exploration zone and damage to any oil exploration site can have a spill-over effect at the dyke site. It is also recommended to have isolation zones up to 3 miles on either side and disallow entry of boats and crafts inside this zone. Two jetties, capable of berthing two 20 Ton boats on each, need to be created on the downstream side so that boats can readily be deployed in case of any eventuality.

2.2 Hazards

Hazards are events or actions that can cause irreparable damage to human life and infrastructure and leave long lasting impact on the overall functioning of a system. In order to understand the type of hazards that may affect the Kalpasar Dyke project and to be able to correctly identify and list them for the purpose of the study it would be prudent to understand a little about improvised explosive devices (IEDs). Basis the environmental scan, prevailing security situation and knowledge of IEDs, Hazards have been listed at the end of this section.

2.2.1 Improvised Explosive Impact Study

The purpose of Explosive Impact Study is to assess the impact that various scenarios involving explosives will have on the structure of the dyke and also other critical assets/ infrastructure associated with the dyke. This study is related only to *Improvised Explosives* used by terror or other inimical organisations and does not take into account the damage caused by military grade ordnance like surface, subsurface, air launched ballistic missiles, artillery, and other ordnance launched from military platforms. The disruption that may be caused by an incident involving improvised explosives has been taken into account to factor its outcomes in the ensuing risk assessment. The outcomes are listed below.

2.2.2 Analysis and Outcome

An incident involving improvised explosives can precipitate in many ways such as an attack with Personnel Borne Improvised Explosive Device (PBIED), Vehicle Borne Improvised Explosive Device (VBIED), Water Borne Improvised Explosive Device (WBIED) and Surface Vessel Improvised Explosive Device (SVIED). These can further be manifested in various ways. The result of all these attacks will be different but the similarity will be the media attention that such an event would generate and the accompanying degradation in morale of the general populace.

(a) Attack by PBIEDs

An attack by Personal Based PBIED would necessitate an individual or groups of individuals with man-portable weights of explosive or an explosive device to launch an attack. A lone wolf attack will mean that the explosive quantity will be limited to a few kilograms at best. A group of individuals can carry different components of an IED and assemble the device on site in order to increase the quantum of explosive in the resultant device and lethality of attack. However, a group of men stopping and assembling a device will be readily identifiable unless they masquerade as maintenance teams. Given that a PBIED attack will be in areas of the dyke like where the rail and road network are sited, the likely targets could include the railway tracks, trained personnel, control rooms and slipway controls for the sluice gates. Road and the top slab would largely be safe in case of any such attack. The main motive for such an attack could be to garner media attention and not any tangible damage. Targeting trained personnel, control rooms, operation centres and

administrative areas could, on the other hand, cause disruption in the dyke operations and could even affect infrastructure if the controls for flood regulator are damaged.

(b) Attack by VBIEDs

A VBIED attack, again, would involve the top of the dyke and infrastructure where chances of any physical damage are minimised unless the explosive laden vehicle is driven into a control/operations centre if feasible as per project design. In such a scenario, the resultant damage would be governed by how close the vehicle reaches the infrastructure and how much explosive is carried by it. Since it is difficult to source military grade explosive in large quantities, VBIEDs usually employ commercially available substances and home-made explosives, both of which have considerably low power. Activation of such a device will cause superficial damage if access to the infrastructure such as control and operation centres is limited by employing barricades. The resultant shock wave and fragments will by and large dissipate over the area. However, any personnel in the vicinity could be fatally injured during an explosion.

(c) Attack by Surface and Subsurface based IEDs

A surface and subsurface attack can be perpetrated by either a boat or a craft carrying explosives, a subsurface attack by swimmer or submersible, using tidal stream to deploy a floating charge or launch of a projectile from a surface craft from either the downstream or the upstream side. We need to take a look at each possibility in isolation and assess the result of each independently.

(1) **Surface Vessel Improvised Explosive Device (SVIED) -** Similar to a VBIED, a surface vessel can carry a substantial quantity of explosive (SVIED). Again, the explosives used in such attacks are either commercially available ones or the home-made ones, both of which do not have the power of 'High' Explosives. In case of an attack by a surface vessel on the dyke wall, the dyke thickness coupled with the presence of tetra pods will dissipate all energy of an explosion without causing damage. If the surface vessel attempts to target the flood regulator, the flow of water from the gates and turbulence around the flood regulator would be a deterrent. In case if the surface vessel is able to reach close to the gates, it is opined that damage from an explosion of commercial/homemade charge will not cause significant damage. At the same time, the possibility of launching a Rocket Propelled Grenade, Mortar or a missile from a surface vessel cannot be ruled out. If the surface vessel is within the striking range of ordnance being carried, an attack is highly likely. Given that such ordnance has small payload, the damage that may be caused will be insignificant unless it targets a control room or operation centre but the event will garner undue media coverage. Then again, the construction and design of the building can offset the hazard. The ordnance so launched can, however, strike traffic and disrupt movement on top of the dyke. It will thus be prudent to have an exclusion zone of around 2-3 nautical;

(2) **Subsurface Attack by Underwater Swimmer/Submersible/AUV -** A careful study of the bottom profile and tidal stream indicates that any attempt to launch an attack by an underwater swimmer from seaward side is unlikely. Even a submersible needs a support platform and prevalent silt, currents and sharp crests and troughs in the seabed will make operating a submersible a hazardous endeavour for the perpetrator. Also, the amount of explosive that can be carried by an underwater swimmer is grossly insufficient to cause any damage to the dyke. Scaling the downstream wall to reach top of dyke to carry out an attack is ruled out as without surface support, such an attempt is not bound to succeed. Submersibles have their own limitations and with a support craft, gaining advantage of surprise would be a challenge given the number of small and large ports in the Gulf and the shape of the gulf itself. The construction and thickness of the gates will need a large quantity

of high explosive and cutting charges to create a breach. However, ordnance delivered from the reservoir side through these means including using AUVs can potentially damage flood regulator structures if they are made to reach the intended target;

(3) **Attack Using Floating Explosive Devices -** Elements inimical to the state may try to use the tidal stream to float an improvised device laden with explosives so that the device can then move up and be activated once it is at the target. Again, the explosive payload will be a limiting factor and this method, if ever employed, will be inaccurate at best. Depending on the flow of water, turbulence, tidal movement and design of device itself, it may never reach the target or land up at a spot where it will cause no damage. Coupled with the difficulty in remote activation of such devices, use of this method is highly unlikely; and

(4) **Attack on Flood regulator -** The possibility of attack on flood regulator infrastructure using IEDs to cause collapse of dyke gates or disruption of mechanical arrangements has been considered and it is felt that such an attack from the water is impractical and unlikely. The dyke gates and other mechanical components will need large explosive quantities to be affected and if cutting charges are used, correct placement to get any result will be near impossible. The turbulence, tidal stream and outward flow will act as natural safeguards in this case.

2.2.3 A word on Explosives

Explosives are classified as Low Explosives, Medium Explosives and High Explosives as per their 'Brisance' or shattering power. Low explosives have a lower Brisance or shattering power and tend to kick things out while high explosives have greater Brisance or shattering power and shatter the target. A few examples of explosives and their categorisation is asunder:

Table 7 : Explosive Classification

Sl.No.	Explosive	Classification	Use/Effect
1	Gelatine 20% Strength	Low Explosive	Quarrying. For separating large chunks of rock.
2	Gelatine 50% Strength	Medium Explosive	Demolition. Controlled demolition of structures.
3	TNT (Tri Nitro Toluene)	High Explosive	Shattering. Military applications.
4	RDX (Research & Development Explosive)	High Explosive	Shattering.
5	AN (Ammonium Nitrate)	Low Explosive	Quarrying.
6	ANFO (Ammonium Nitrate Fuel Oil)	Medium Explosive	Mining &Quarrying.

It merits attention that most high explosives are highly controlled and sourcing them in large quantities is difficult even for heavily funded terror groups. Most of these groups use commercial explosives such as Ammonium Nitrate and Gelatine/Dynamite or Ammonium Nitrate mixed with Fuel Oil to increase its potency. Even then, the explosion is

of the nature of a medium explosive with more of a 'pushing' effect and does not shatter the target. Further, during an explosion, energy is radiated outwards from the seat of explosion in a spherical manner and it gets absorbed or reflected by target/surfaces where it is incident. Consider the case of a vehicle towing a flatbed trailer and having an explosive laden container on the flatbed. If in case the explosive detonates, most of the shock wave energy will be discharged upwards and towards the sides, where it meets the least resistance. Downward movement of the shock wave will be checked by the container base, the flatbed surface, chassis and trailer components before it reaches the road/ground surface.

The following tables indicate the distance a shockwave will travel for various types of explosives and the distance at which a well-built RCC structure will be able to provide protection to personnel taking shelter or working inside it.

Table 8 : Shockwave Distance Ammonium Nitrate

AN (Ammonium Nitrate)			
Sl. No.	**Weight of Explosive**	**Distance Shockwave Travels**	**Distance at which RCC structure provides protection**
1	100 Kg	536 m	34 m
2	500 Kg	812 m	52 m
3	1000 Kg	1047 m	66 m
4	2000 Kg	1319 m	84 m

Table 9 : Shockwave Distance Ammonium Nitrate Fuel Oil

ANFO (Ammonium Nitrate Fuel Oil)			
Sl. No.	**Weight of Explosive**	**Distance Shockwave Travels**	**Distance at which RCC structure provides protection**
1	100 Kg	536 m	34 m
2	500 Kg	915 m	58m
3	1000 Kg	1152 m	74 m
4	2000 Kg	1452 m	92 m

Table 10 : Shockwave Distance Gelatine 20% Strength

Gelatine 20% Strength			
Sl. No.	**Weight of Explosive**	**Distance Shockwave Travels**	**Distance at which RCC structure provides protection**
1	100 Kg	536 m	34 m
2	500 Kg	849 m	54 m
3	1000 Kg	1152 m	74 m
4	2000 Kg	1452 m	92 m

Table 11 : Shockwave Distance Gelatine 50% Strength

Gelatine 50% Strength			
Sl. No.	**Weight of Explosive**	**Distance Shockwave Travels**	**Distance at which RCC structure provides protection**
1	100 Kg	536 m	34 m
2	500 Kg	884 m	56 m
3	1000 Kg	1152 m	74 m
4	2000 Kg	1452 m	92 m

Table 12 : Shockwave Distance TNT

TNT (Trinitrotoluene)			
Sl. No.	**Weight of Explosive**	**Distance Shockwave Travels**	**Distance at which RCC structure provides protection**
1	100 Kg	612 m	39 m
2	500 Kg	1047m	53 m
3	1000 Kg	1319 m	84 m
4	2000 Kg	1564 m	100 m

Table 13: Shockwave Distance RDX

RDX (Research & Development Explosive)			
Sl. No.	**Weight of Explosive**	**Distance Shockwave Travels**	**Distance at which RCC structure provides protection**
1	100 Kg	612 m	39 m
2	500 Kg	1047m	53 m
3	1000 Kg	1319 m	84 m
4	2000 Kg	1662 m	106 m

2.2.4 Identified Hazards

Based on the complete understanding of the environment and associated factors the following 26 Hazards have been identified for further analysis and assessment.

Table 14: Hazards

S.No	Hazards
Land Based Hazards	
H1	Directed surveillance
H2	Sabotage
H3	Sabotage (Railway corridor)
H4	Indirect Fire Area Weapons
H5	Vehicle Borne Improvised Explosive Devices (VBIED)
H6	Personnel Borne Improvised Explosive Device (PBIED)
H7	Theft of stores and equipment.
H8	Disruption of transportation.
H9	Demonstrations and blockades.
H10	Mob Violence
H11	Active Shooter
H12	Arson
H13	Road Traffic Incidents
H14	Labour Disputes/ Strikes/ Demonstrations
H15	Disputes with Host Communities
Sea Based Hazards	
H16	Surface Ship Attack
H17	Subsurface Attack
H18	Subsurface Attack by Unmanned Vehicles
H19	Surface Vessel Improvised Explosive Device (SVIED)
H20	Fast Coastal Attack Craft
Air Based Hazards	
H21	Aircraft Impact
H22	Drone Attack
H23	Air Launched Bomb / Missile Attack
H24	Aerial Surveillance by Drones
Information Based Hazards	
H25	Disclosure of Information
H26	Cyber Attack

2.3 Exposure

2.3.1 Background

Once built, Kalpasar Dyke will be an extremely large and long dyke with the largest reservoir area in the world. The reservoir will have the capacity to hold 8000 MCM of water and the water pumping and distribution system which is being created separately will provide fresh water for agriculture, industry, and domestic use to the Saurashtra region. Saurashtra otherwise has a water deficit and water is a scarce resource in the summer months. The dyke will also be a vital road link between Saurashtra and Southern Gujarat

and is likely to be used extensively by vehicular and rail traffic. This will put the dyke in the category of a Vital Asset for Gujarat region which will also be exposed to hazards.

Since resources are always at a premium, there is invariably a need to categorize the Critical assets so that those more exposed to hazards are given greater focus than those which are less exposed. Such Critical assets are invariably those that are essential for supporting the operational role of the organisation. These assets will have a high consequence of failure, but not necessarily a high likelihood of failure.

Identification of such exposed assets that need to be protected is the start point for any security process. It begins with identifying people, property, equipment, materials, activities and operations, information etc which are considered essential to meet the primary, secondary or tertiary charter of the organisation. Only after identifying assets which need to be protected, can the organisation prepare for safeguarding them and allocate the necessary controls/ resources for their protection.

2.3.2 Purpose

The purpose of this section is to identify the assets to be protected at the Kalpasar Project based on their exposure. Once identified and agreed upon, these outcomes shall form the cornerstone for the design of risk mitigation strategies for the protection of the identified assets to an '*as low as reasonably practicable*' level.

It should be noted that this section is not a detailed risk assessment, nor is it a strategic or operational intelligence report, as these would require extensive interaction between the consultant team and state intelligence organisations and falls outside of the project scope.

2.3.3 Asset Exposure & Valuation

The assessment identifies assets supporting the organization's missions, units, or activities and deemed critical by facility operators. It addresses the impact of temporary or permanent loss of assets. For the purpose of this document, assets identified during the preparation of the DPR and Inception Report have been taken into consideration and certain assets have been added based on user interaction and the consultants understanding of operations. Further, assets considered of less operational and mission value have been deleted.

The Exposed critical assets have been identified through the use of the CARVER Matrix developed by the U.S. Special Forces. The CARVER Matrix is a decision-making tool used for rating the relative desirability of potential targets and for properly allocating attack resources. The CARVER assessment factors of Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognisability assist in selecting the best targets to attack. As the factors are analysed and values assigned, a decision matrix is formed, indicating the highest value target to be attacked within the limits of the capability. The fifteen critical assets which are susceptible to exposure are appended below:

Table 15: Carver Matrix

S. No.	Asset Description	Description
1	Dyke (Structure)	Primary structure built across the sea to create a fresh water reservoir on the up-stream side by collecting fresh water of the rivers flowing into the reservoir.
2	Flood Gates/Controls	A 2 km wide concrete structure built into the dyke near the inter-tidal zone on the eastern side of the dyke to allow controlled flow of excess water from the reservoir to the sea. A total of 100 gates are planned on the flood regulator
3	Abutments	Where the dyke structure joins the natural earth or rock foundation are important components. Walls of the flood regulator etc are also sometimes referred to as abutment. In a rock-fill dyke like the one proposed at Kalpasar, there may not be a distinct abutment and therefore for the purpose of this assessment they are treated the same as the dyke structure
4	Control Room	Remote or local control station from where all major machinery and functions of the dyke will be controlled
5	Irrigation Structure	The primary purpose of the dyke is to provide irrigation water to the Saurashtra region. Irrigation structures include canals, conduits, pumping/ lifting station and associated machinery
6	Road Transportation Corridor	The dyke also aims to link the Saurashtra region with South Gujarat thereby cutting down the travel time by road substantially. Though alternate routes would continue to be available, these would be longer and more time consuming.
7	Rail Transportation Corridor	The dyke also aims to link the Saurashtra region with South Gujarat by rail network for both passenger and freight movement thereby cutting down the travel time substantially. Though alternate routes would continue to be available, these would be longer and more time consuming.
8	Solar / Wind Farm	Provides captive power to the dyke. Alternate sources of power would be available through the power grid.

S. No.	Asset Description	Description
9	Trained Operation and Maintenance Personnel	Operations and maintenance personnel as well as experts who would be handling day to day operations / maintenance as well as attend to any major breakdowns
10	Power Transmission and Distribution network	These would typically comprise Switchyard, Transmission lines, Emergency Generators, Transformers etc. to provide electrical supply to the main machinery, pumps and control stations
11	Maintenance Corridor/Galleries	A standalone maintenance corridor has been planned near the crest of the dyke to provide access to the flood regulator gates and other parts of the dyke
12	Machinery Space	Spaces or rooms where machinery and equipment are installed for the control and operation of various functions
13	Administrative Infra / Complex	The area which houses offices of majority of the staff and from where majority of the administrative tasks are undertaken
14	Storage/ Stacking Yard	Storage Yard is generally an open place where construction materials are stored during construction stage of a project. Smaller yards may also be found within a work premise for frequently required items in factories or service agencies
15	Project Site Admin Infra	These a normally temporary office infrastructure created at work sites for project managers, engineers, supervisors etc for day-to-day work during the construction phase.

2.4 Vulnerability

Vulnerability of the exposed assets to various hazards is dependent on the amount of damage that can be inflicted and the effect of such an act or incident upon the asset. Vulnerability is an estimation, thus should be decrypted applying real world knowledge of perpetrators tactics and capabilities which should form the basis of such a judgment.

Breaching security systems and technology requires detailed planning, information, technical knowhow, physical capability and at times insider support amongst many other factors that contribute to success. Project compulsions may take precedence over security features and thus often there are design/ process features that can be tactically exploited by perpetrators/ actors. Based on Arista's real-world experience, these have been identified and derived as TEFs©, Tactically Exploitable Features and form the core part of our methodology for the purpose of judging Vulnerability.

2.4.1 Tactically Exploitable Features (TEFs©)

Every perpetrator when planning a malicious act against a facility, carefully studies the facility before creating their plan of action. Their surveillance may include an onsite reconnaissance, insider information, blueprints etc. through which they would attempt to identify these TEFs©. It is therefore these TEFs© that need to be identified by an `Experts Eye' with an intruder's perspective and attended to during the security designing process. In addition to identifying Vulnerabilities, TEFs© assist in the following two additional functions:

(1) Assist in identification of Asset Sensitivity; and
(2) Identifying areas within the project/ site/ zone which can be exploited and thus contribute to the importance of the design mitigation measures and priority required for a particular critical asset based on the Sensitivity.

Using various criteria as per Arista's methodology, a detailed analysis was undertaken to identify TEFs© during the review and study of detailed drawings. These TEFs© are based on the core understanding of a perpetrator's tactics and how they are likely to conduct attacks on critical infrastructure. Using Arista experts with past boots on ground experience, twelve such critical Tactically Exploitable Features related to the project have been identified which will need to be suitably addressed while planning the detailed security design.

Table 16: TEFs © Identified

TEF© No	TEF©	Asset Affected	Mitigation
TEF 1	Certain parts of Flood Regulator structures/ mechanisms are not in closed space and in open view permitting standoff access to perpetrators	Vertical Lift and Stop lock Gates	Surveillance and Monitoring, Inner Layer Intrusion Detection, Access Control
TEF 2	Surface of downstream guide bund can be damaged with explosives dropped from air to divert runoff creating downstream	Dyke (Structure)	CUAV Solution, Air Defence

	damage		
TEF 3	Control Centre & Machinery Spaces can be damaged, functions disrupted through physical intervention and sabotage	Control Room, Machinery Space	Inner Layer Intrusion Detection, Access Control
TEF 4	Utility Ducts can be misused for tampering essential services and to disrupt functioning of the dyke	Maintenance Corridors and Galleries	Monitoring, Intrusion Detection, Access Control
TEF 5	Railway Tracks on the section on top of the dyke are susceptible to damage by placing explosives and sabotage	Rail Transportation Corridor	Monitoring, Intrusion Detection, Access Control Sensors
TEF 6	Vehicle Entry Points/ Check posts are susceptible to VBIED attacks	Road Transportation Corridor	Monitoring, Intrusion Detection/ Access Control
TEF 7	Water body and area in proximity to flood regulator gates can be exploited for releasing surface or underwater explosive devices	Vertical Lift and Stop lock Gates	Marine Barrier Access Control, Monitoring (Diver Detection System-DDS)
TEF 8	Water intakes on reservoir side can be exploited to deliver smart explosives with the flood stream	Vertical Lift and Stop lock Gates	Intrusion Detection (Sensors), Access Control (Magal Bars)
TEF 9	Boat embarkation points/ ferry points can be used by inimical elements for mounting operations	Vertical Lift and Stop lock Gates	Monitoring and Surveillance (Physical & Drones)
TEF 10	Unpopulated areas in vicinity of dyke can be exploited for launching armed UAVs	Dyke Structure, Rail Transportation Corridor, Road Transportation Corridor	Drone surveillance/ CUAV solutions
TEF 11	Work spaces and posts manned by trained personnel and maintenance staff are soft spots to be exploited by perpetrators	Trained Operation and Maintenance Personnel	Monitoring, Access Control
TEF 12	Viewer gallery, tourist stops on the dyke could be vantage points for attack on personnel and used for surveillance	General public	Monitoring, Access Control

3 Risk Assessment

3.1 Analysis Based on Supporting Project Plans, Designs and Related Studies

Risk is the potential for an adverse outcome from an event or Hazard, determined by the Exposure and Vulnerability of assets and ability to Recover from the possible impact. The following is an elaboration of the analysis based on further examination of project plans, designs and other related studies to understand security gaps and vulnerabilities which may impact a critical asset in the event of an adverse security breach.

A standard framework for evaluating security risks entails determining the hazard source, probable targets, the potential means by which a attack could be carried out, and the knowledge and skills necessary to execute the attack. It is possible to recognize what kind of activities are suspicious and might be signs of a potential hazard by understanding those elements and why a dyke would be targeted.

The potential for dramatic consequences of destruction or disruption of a significant national asset poses an appealing target for terrorists. Individuals or groups with the capacity and intent to cause harm may pose a hazard to the security of this project. Domestic and foreign terrorists, hostile states, dissatisfied people or groups, unhappy workers, and organised adversarial groupings are all potential sources of hazards against critical infrastructure targets. Hazards may originate from people or organisations that are familiar with the tools and machinery utilised in the Infrastructure Sector, while specific information about equipment and operating methods of Dykes can also be obtained from open sources, as well as from existing or former personnel, furthermore, insider information may be held by dissatisfied or corrupted employees. This information can be used to compromise the security of the project and associated infrastructure.

This analysis aims to further improve understanding of the security risks and provide tools, guidelines, information, best practices, and resources to facilitate a more effective concept, design and security plan development.

3.1.1 Analysis of Dyke Structure

The Dyke Structure is the primary structure built across the sea to create a fresh water reservoir on the up-stream side by collecting fresh water of the rivers flowing into the reservoir. An analysis of the risks posed to the Dyke structure is as follows:

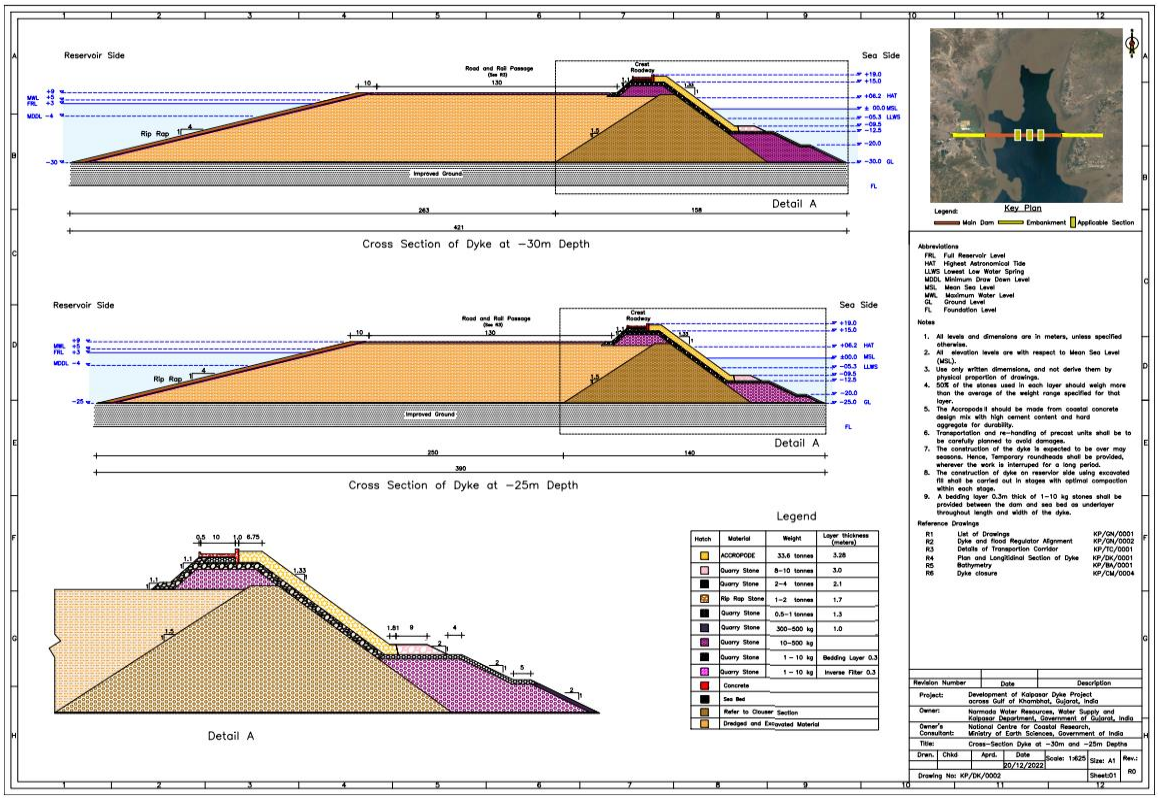


Figure 13: Kalpasar Dyke Cross-Section

(a) **Directed Surveillance**: Terrorists use surveillance to locate target facilities and organise their attack. In the past, terrorists have monitored targets for extended periods to find flaws and devise the most effective ways to strike them. Dykes pose a more challenging security monitoring task than facilities in a more metropolitan environment because of their typically isolated location. The risk of malicious directed surveillance on the Dyke structure is considered **high**, especially since the Dyke is unique in having a sixteen-lane highway and rail corridor with large planned movement of men and material.

(b) **Sabotage**: The Dyke's inherent strength in design and thickness makes the primary structure of the Dyke impervious to sabotage, however sabotage to the flood regulator gates and other mechanisms may compromise the structure of the Dyke. The risk of sabotage to the primary structure of the Dyke is therefore considered **high**.

(c) **Sabotage (Railway Corridor)**: The crest of the Dyke is designed to have a sixteen-lane road carriageway with a central median, a pedestrian walkway to one side and a railway freight corridor on the other side with two railway tracks. Part of the Rail and Road corridor is also designed to go over the flood regulator on a viaduct. Sabotage to the railway corridor can result in a cascading effect which has the capacity to damage the structure of the crest of the Dyke as well as the flood regulator. The risk of damage to the structure of the Dyke through sabotage to the railway corridor is considered **very high**.

(d) **Indirect Fire Area Weapons**: Indirect fire weapons consisting of projectiles, missiles or bombs can have minimal impact on the inherent strength of the Dyke structure. The risk of indirect fire area weapons to the Dyke structure is considered **moderate**.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED)**: VBIEDs are substantially larger than hand delivered IEDs, ranging from 100kg to, in extreme instances, 2,500kg in size. VBIEDs may be employed singly or in multiples, detonating simultaneously or sequentially depending upon the bomber's purpose. They may be delivered by individuals or groups (suicide bombers) on martyrdom missions who are prepared to die in the course of their attack. As the crest of the Dyke is designed to carry a sixteen-lane road carriageway as well as a two-track freight corridor, the possibility of a malicious VBIED attack increases. Depending on the size of the explosives deployed, there is a possibility of some damage to the structure of the crest of the Dyke. The risk of VBIED impact on the structure of the Dyke is considered **moderate**.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** PBIEDs may be delivered by an individual or group and placed by hand. Such devices may be concealed in any form of bag or container. Alternatively, it may be worn about the body of an individual on a martyrdom mission (suicide bomber) who is prepared to die in the completion of their mission. Such an explosive may cause minor damage to the crest of the Dyke but may be insufficient to cause significant damage to the primary structure of the Dyke and therefore the risk of a PBIED attack on the Dyke structure is considered **low**.

(g) **Theft of Stores and Equipment:** Organised theft of materials during the construction of the Dyke may compromise the costs and maintenance of the project. Once the Dyke is operational, theft of vital equipment that may interfere with the functioning of the flood regulator may have a cascading effect on the Dyke structure. The risk of theft of stores and equipment to the primary structure of the Dyke is considered **moderate**.

(h) **Disruption of Transportation:** Considered **low** risk to the primary structure of the Dyke.

(i) **Demonstrations and Blockades:** Considered **low** risk to the primary structure of the Dyke.

(j) **Mob Violence:** Considered **low** risk to the primary structure of the Dyke.

(k) **Active Shooter:** Considered **low** risk to the primary structure of the Dyke given its inherent strength in design.

(l) **Arson:** Considered l**ow** risk to the primary structure of the Dyke.

(m) **Road Traffic Incidents:** A traffic incident involving either a vehicle colliding with another vehicle or colliding with a structure on the Dyke will not significantly impact the primary structure of the Dyke given its inherent strength in design. The risk of road traffic incidents impacting the structure of the Dyke is considered **moderate**.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **low** risk to the primary structure of the Dyke.

(o) **Disputes with Host Communities:** Considered **low** risk to the primary structure of the Dyke;

(p) **Surface Ship Attack:** An attack against the Dyke during armed conflict from a surface ship using naval guns or missiles may impact the structure of the Dyke. Given the proximity of the Dyke to hostile neighbours and the high value of the project, the likelihood of surface ship attack during a **wartime** situation is considered high. Risk to the structure of the Dyke under a surface ship attack is considered **very high**.

(q) **Subsurface Attack:** An attack against the Dyke through small submersible craft using torpedoes or human delivered ordnance through the reservoir side is considered likely. The risk to the structure of the Dyke in the event of such an attack during **wartime** is considered **very high**.

(r) **Subsurface Attack by Unmanned Vehicles:** An attack delivered from AUVs (autonomous unmanned vehicles) on the Dyke using explosive devices is likely to impact the structure of the Dyke depending on the payload capability of the vehicle. Risk to the structure of the Dyke in the event of a subsurface attack by unmanned vehicles is considered **high**.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** SVIEDS are a means of delivering a large IED to targets in a marine environment. The size of any device is limited by the handling characteristics of the craft used to transport it but may range up to 1000kg or more. Previous examples of SVIEDs have targeted vessels in ports, vessels under way and military port infrastructure. Risk to the structure of the Dyke in the event of an SVIED attack from the reservoir side is considered **Low**.

(t) **Fast Coastal Attack Craft:** Similar to surface ship attack. These craft use stealth and speed to close in the target to carry out ballistic attacks on a selected target. Risk to the primary structure of the Dyke through a FCAC attack is considered **high.**

(u) **Aircraft Impact:** Aircraft impact includes an accidental or deliberate direct impact by a conventional aircraft or helicopter. Risk to the primary structure on the crest of the Dyke in the case of an aircraft impact is considered **very high**.

(v) **Drone Attack:** A drone attack includes accidental or deliberate direct impact or weapon released by an unmanned aerial vehicle. Risk to the primary structure of the Dyke in the event of a drone attack is considered **high**.

(w) **Air Launched Bomb/Missile Attack:** Risk to the primary structure of the Dyke is considered **very high** in the event of an air launched bomb/missile attack during **wartime**.

(x) **Aerial Surveillance by Drones:** There is a high probability of surveillance by drones to capture information about weak areas and targets on the Dyke. Risk to the primary structure of the Dyke through drone surveillance is considered **very high**;

(y) **Disclosure of Information:** Disclosure of sensitive information may result in adversaries discovering weaknesses to be exploited in the Dyke structure. The risk to the Dyke structure in the event of an information leak is considered **moderate**.

(z) **Cyber Attack:** Malicious access to the Dyke's cyber network may impact the functioning of the Dyke and consequently may compromise the Dyke structure. The risk of cyber attack to the primary Dyke structure is considered **moderate**.

3.1.2 Analysis of Flood regulator Design

The Flood regulator is a 2 km wide concrete structure built into the Dyke near the inter-tidal zone on the eastern side of the Dyke to allow flow of excess water from the reservoir to the sea. Part of the Rail and Road corridor is also designed to go over the flood regulator on a viaduct. To control and regulate the amount of water in the reservoir, the flood regulator has been designed with a total of 100 Stop-log gates. These are the most critical and vulnerable sections of the Dyke with potential for targeted damage and disruption my malicious groups or individuals.

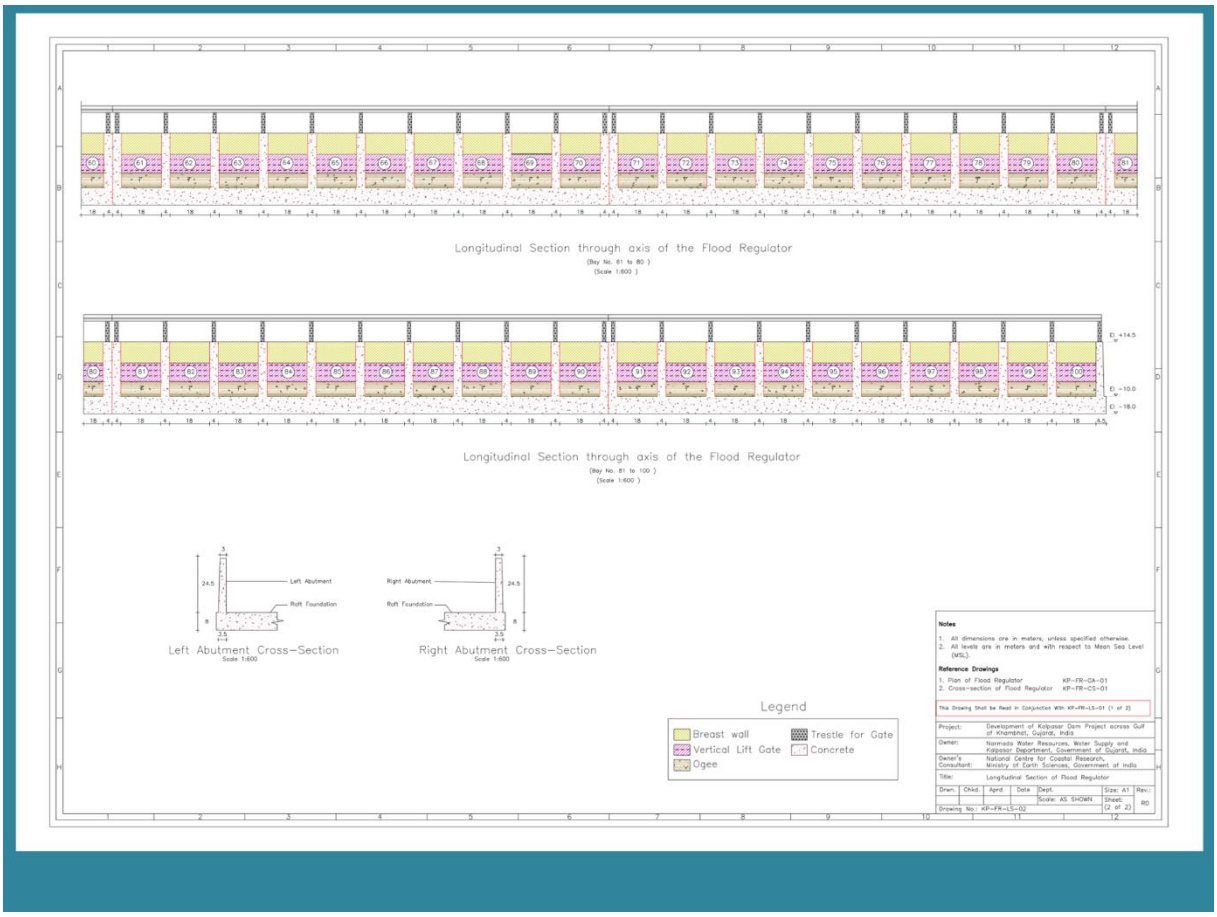


Figure 14 : Cross-Section Flood Regulator

Each of the gates is to be installed on concrete bedding reinforced with steel and curtain walls. These vertical lift gates are lowered and hoisted using reels of steel wire ropes and hoisting mechanisms.

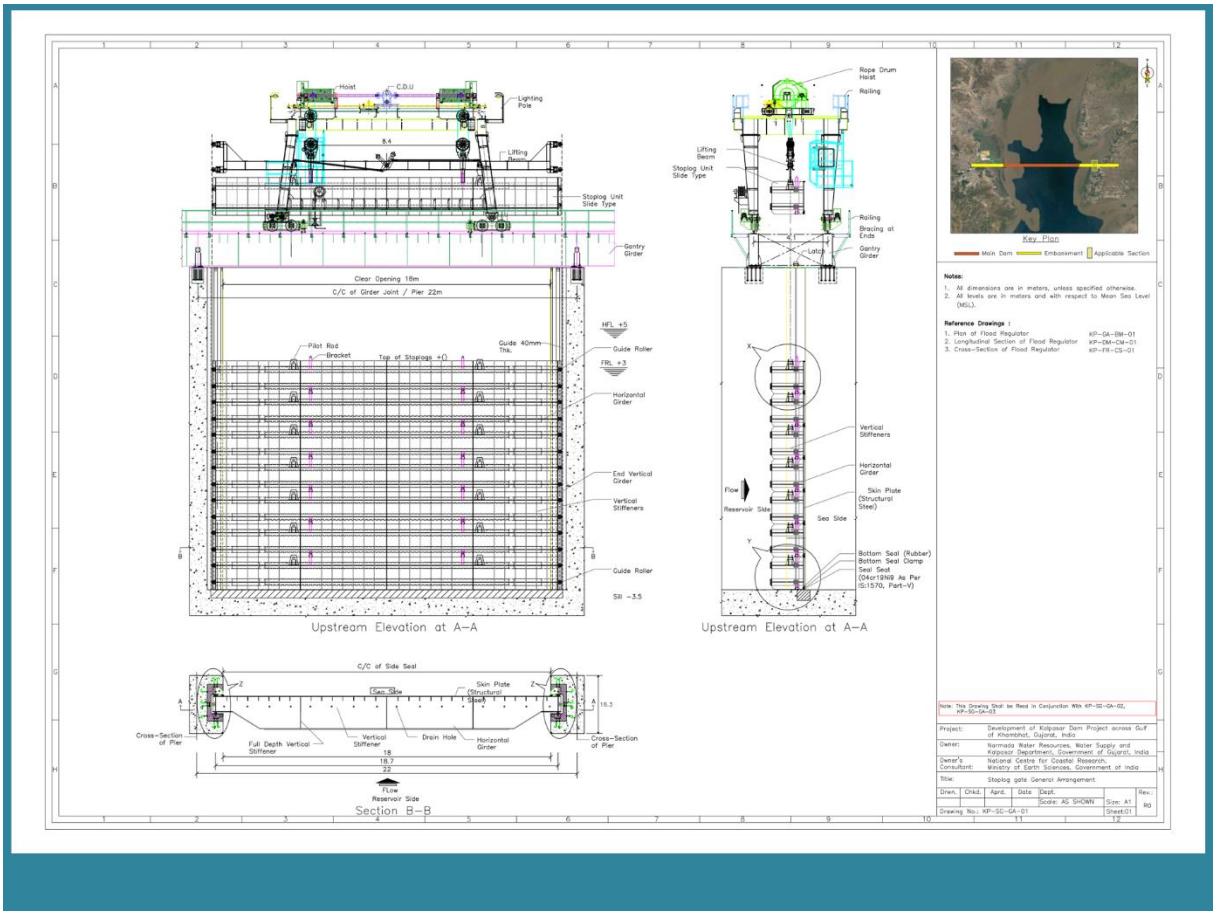


Figure 15 : Stop Log Gate General Arrangement

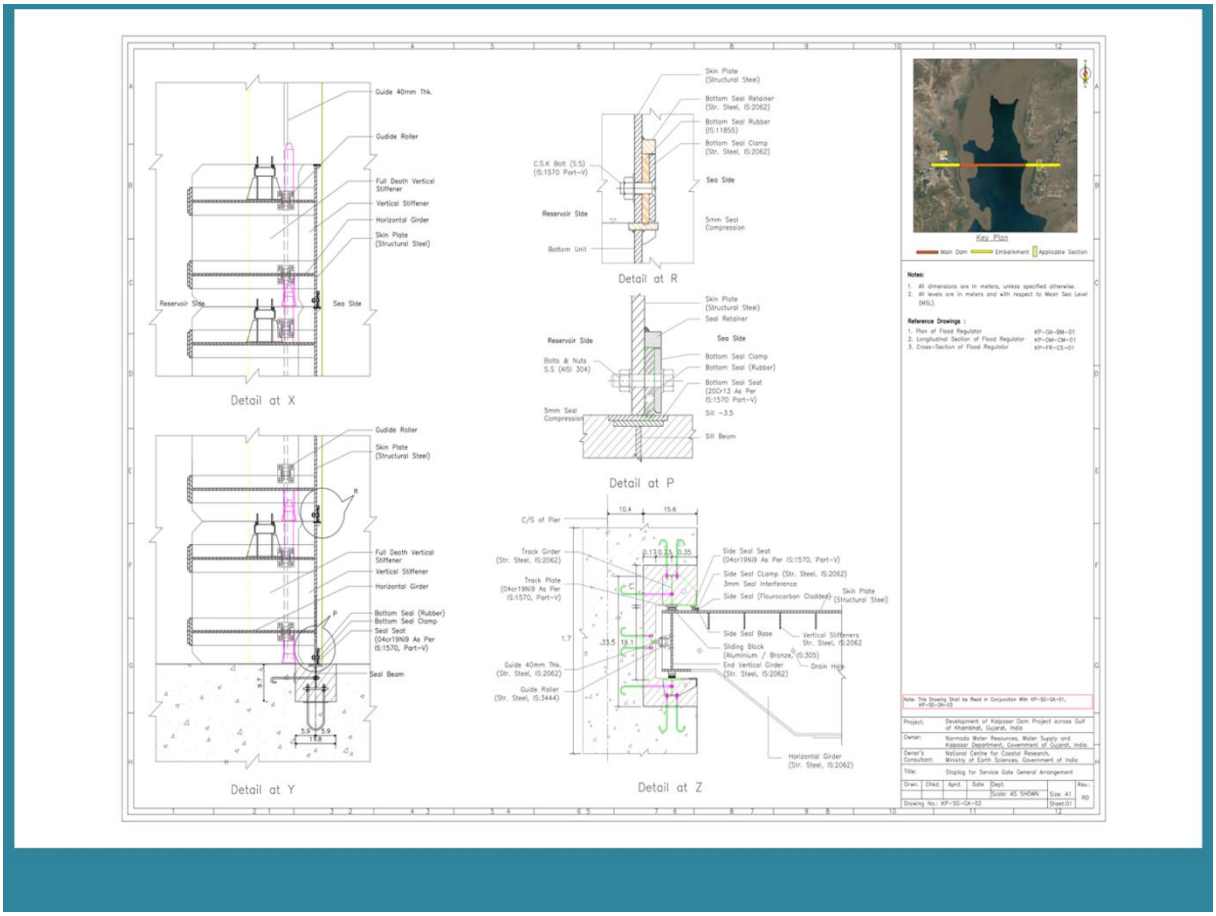


Figure 16 : Stop Log Service Gate General Arrangement

The flood regulator also has a concrete stilling basin towards the seaward side. On top, the flood regulator is horizontally separated from the road and rail carriageways. Control center for the flood regulator gates will also be located at a distance from the carriageways. The hoisting and lowering mechanism for the gates is mounted above the gates and is inaccessible from the seaward side.

(a) **Directed Surveillance:** There is a very high likelihood of malicious surveillance directed towards the flood regulator and the mechanisms that control the gates. Such surveillance may expose the weak points of the flood regulator and leave it vulnerable to attack. Risk to the flood regulator under directed surveillance is considered **very high**.

(b) **Sabotage:** There is a very high likelihood of sabotage directed towards the flood regulator and the mechanisms that control the gates. Such sabotage may cause a cascading effect on the Dyke, compromising its functioning and structure. Risk of sabotage to the flood regulator is considered **very high**.

(c) **Sabotage (Railway corridor):** While the railway corridor is designed to be separated from the flood regulator and is designed to go over the flood regulator on a viaduct, a significant event on the corridor has the chance of impact on the flood regulator. Risk to the flood regulator in the event of sabotage to the railway corridor is considered **high**.

(d) **Indirect Fire Area Weapons:** In the event of an artillery attack on the Dyke, targeted shelling to the flood regulator has the likelihood of causing significant damage. Risk to the flood regulator in the event of such an attack is considered **high**.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** The roadway is designed to be located on the reservoir side of the Dyke, it is designed to be physically separated from the flood regulator and is designed to go over the flood regulator on a viaduct, moreover, the roadway is designed to withstand impact and moderate seismic activity. The risk of impact to the flood regulator through a VBIED event on the roadway is considered **moderate**.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** Pedestrian access to the flood regulator is restricted due to its inherent design. Risk of impact to the flood regulator through a PBIED event is considered **low**.

(g) **Theft of Stores and Equipment:** It is likely that theft of the movable parts of the flood regulator may occur, including components of the mechanisms that control the gates; however, it is improbable that significant theft of such heavy equipment is possible given the overall design of the Dyke. Risk to the flood regulator through theft of stores and equipment is considered **moderate**.

(h) **Disruption of Transportation:** Any disruption to transportation is unlikely to cause any effect on the flood regulator. Disruption of transportation is considered **low** risk to the flood regulator.

(i) **Demonstrations and Blockades:** Protests are unlikely to cause any effect on the flood regulator. Demonstrations and blockades are considered **low** risk to the flood regulator.

(j) **Mob Violence:** Mob violence may have an impact on the control room which is responsible for the proper functioning of the flood regulator machinery. In such an event that mob violence affects the control room it is considered **moderate** risk to the flood regulator.

(k) **Active Shooter:** An active shooter may have an impact on the control room which is responsible for the proper functioning of the flood regulator machinery. In such an event that an active shooter affects the control room it is considered **moderate** risk to the flood regulator.

(l) **Arson:** Arson may have an impact on the control room which is responsible for the proper functioning of the flood regulator machinery. In such an event that arson affects the control room it is considered **moderate** risk to the flood regulator.

(m) **Road Traffic Incidents:** Road traffic incidents, whether accidental or with malicious intent, are unlikely to cause any effect on the flood regulator. Road traffic incidents are considered **low** risk to the flood regulator.

(n) **Labour Disputes/Strikes/Demonstrations:** Protests or disputes are unlikely to cause any effect on the flood regulator. Demonstrations are considered **low** risk to the flood regulator.

(o) **Disputes with Host Communities:** Disputes are unlikely to cause any effect on the flood regulator. Disputes with host communities are considered **low** risk to the flood regulator.

(p) **Surface Ship Attack:** An attack against the Dyke during **wartime** from a surface ship using naval guns or missiles may impact the structure of the Dyke including the flood regulator. Given the proximity of the Dyke to hostile neighbours and the high value of the project, the likelihood of surface ship attack during a wartime situation is considered high. Risk to the flood regulator under a surface ship attack is considered **very high**.

(q) **Subsurface Attack:** An attack against the Dyke through submersible craft using torpedoes or human delivered ordnance through the reservoir side is considered likely and the impact of such an attack on the flood regulator considered very high. Such attacks, especially those delivered by Special Forces or state sponsored forces trained for Samundari Jihad using small submersible craft may be used even in less than war situations and have an element of deniability. The risk to the flood regulator in the event of such an attack is considered **very high**.

(r) **Subsurface Attack by Unmanned Vehicles:** An attack delivered from AUVs (autonomous unmanned vehicles) or small craft on the Dyke, using explosive devices is likely to be targeted at the flood regulator and the mechanisms that control the gates, especially from the reservoir side. Risk to the flood regulator in the event of a subsurface attack by unmanned vehicles is considered **very high**.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** SVIEDS are a means of delivering a large IED to targets in a marine environment. The size of any device is limited by the handling characteristics of the craft used to transport it but may range up to 1000kg or more. Previous examples of SVIEDs have targeted vessels in ports, vessels under way and military port infrastructure. It is highly probable that the flood regulator and the mechanisms that control the gates may be targeted. Risk to the flood regulator in the event of an SVIED attack from the reservoir side is considered **very high**.

(t) **Fast Coastal Attack Craft:** Similar to surface ship attack. These craft use stealth and speed to close in the target to carry out ballistic attacks on a selected target. Risk to the flood regulator through a FCAC attack is considered **high**.

(u) **Aircraft Impact:** Risk to the flood regulator in the case of an aircraft impact is considered **very high**.

(v) **Drone Attack:** Risk to the flood regulator in the case of a drone attack is considered **very high**.

(w) **Air Launched Bomb/Missile Attack:** Risk to the flood regulator in the case of an air launched bomb or missile attack is considered **very high**.

(x) **Aerial Surveillance by Drones:** There is a very high probability of surveillance by drones to capture information about weak areas and targets on the flood regulator. Risk to the flood regulator through drone surveillance is considered **very high**.

(y) **Disclosure of Information:** Disclosure of sensitive information may result in adversaries discovering weaknesses to be exploited in the flood regulator and mechanisms that control the gates, leaving the flood regulator vulnerable to attack. The risk to the flood regulator in the event of an information leak is considered **high**.

(z) **Cyber Attack:** Malicious access to the Dyke's cyber network is likely to adversely impact the functioning of the Dyke. The risk of cyber-attack to the flood regulator and mechanisms that control the gates is considered **very high**.

3.1.3 Analysis of Abutments

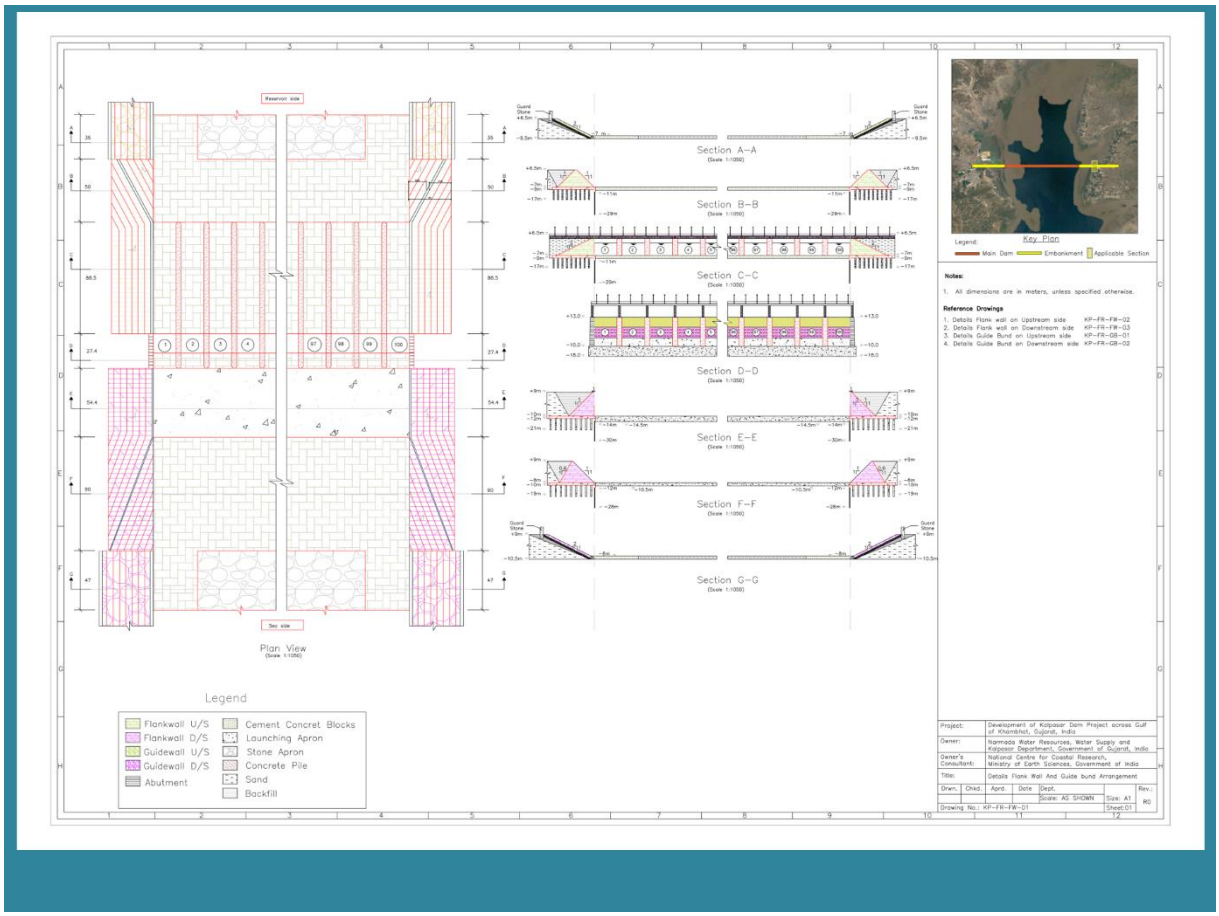


Figure 17 : Flank Wall, Abutment and Guide Bund Arrangement

An Abutment is where the Dyke structure joins the natural earth or rock foundation and is an important component of the Dyke.

(a) **Directed Surveillance:** Given that the abutment is structurally an integral part of the primary Dyke structure, little or no interest may be directed toward it by adversaries. Any surveillance on the Dyke may be toward weaker potentially areas, surveillance directed on the abutments is considered a moderate risk.

(b) **Sabotage:** The Dyke's inherent strength in design and thickness makes the primary structure of the Dyke, including the abutments impervious to sabotage, however sabotage to the flood regulator gates and other mechanisms may compromise the structure of the Dyke

including the abutments. The risk of sabotage to the abutments of the Dyke is therefore considered **moderate**.

(c) **Sabotage (Railway Corridor):** Sabotage to the railway corridor can result in a cascading effect which has the capacity to impact the structure of the Dyke including the abutments. The risk of damage to the abutments of the Dyke through sabotage to the railway corridor is considered **moderate**.

(d) **Indirect Fire Area Weapons:** Indirect fire weapons consisting of projectiles, missiles or bombs can have minimal impact on the inherent strength of the Dyke structure including the abutments. The risk of indirect fire area weapons to the Dyke structure is considered **moderate**.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** The roadway is designed to be located on the reservoir side of the Dyke; moreover, the roadway is designed to withstand impact and moderate seismic activity. The risk of VBIED impact on the abutments of the Dyke is considered **moderate**.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** PBIEDs may be delivered by an individual or group and placed by hand. Such devices may be concealed in any form of bag or container. Alternatively, it may be worn about the body of an individual on a martyrdom mission (suicide bomber) who is prepared to die in the completion of their mission. Such an explosive may be insufficient to cause significant damage to the primary structure of the Dyke including the abutments therefore the risk of a PBIED attack on the abutments is considered **low**

(g) **Theft of Stores and Equipment:** Organised theft of materials is considered **low** risk to the abutments.

(h) **Disruption of transportation:** Considered **low** risk to the abutments.

(i) **Demonstrations and Blockades:** Considered **moderate** risk to the abutments.

(j) **Mob Violence:** Considered **moderate** risk to the abutments.

(k) **Active Shooter:** Considered **low** risk to the abutments.

(l) **Arson:** Considered **low** risk to the abutments.

(m) **Road Traffic Incidents:** A traffic incident involving either a vehicle colliding with another vehicle or colliding with a structure on the Dyke will not significantly impact the primary structure of the Dyke given its inherent strength in design. The risk of road traffic incidents impacting the structure of the Dyke is considered **moderate**.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **low** risk to the abutments.

(o) **Disputes with Host Communities:** Considered **low** risk to the abutments.

(p) **Surface Ship Attack:** An attack against the Dyke during armed conflict from a surface ship using naval guns or missiles may impact the structure of the Dyke including the abutments. Given the proximity of the Dyke to hostile neighbours and the high value of the project, the likelihood of surface ship attack during a wartime situation is considered high. Risk to the abutments of the Dyke under a surface ship attack is considered **moderate**.

(q) **Subsurface Attack:** The risk to the abutments of the Dyke in the event of an attack by a submersible is considered **low**.

(r) **Subsurface Attack by Unmanned Vehicles:** Considered **low** risk to the abutments.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **low** risk to the abutments.

(t) **Fast Coastal Attack Craft:** Considered **low** risk to the abutments.

(u) **Aircraft Impact:** Aircraft impact includes an accidental or deliberate direct impact by a conventional aircraft or helicopter. Risk to any part of the Dyke including the abutments in the case of an aircraft impact is considered **high**.

(v) **Drone Attack:** Risk to the abutments in the case of a drone attack is considered **moderate**.

(w) **Air Launched Bomb/Missile Attack:** Risk to the abutments in the case of an air launched bomb/missile attack is considered **high**.

(x) **Aerial Surveillance by Drones:** Considered **moderate** risk to the abutments.

(y) **Disclosure of information:** Considered **low** risk to the abutments.

(z) **Cyber Attack:** Considered **low** risk to the abutments.

3.1.4 Analysis of Control Room

The Control Room is a remote or local control station from where all major machinery and functions of the Dyke will be controlled.

(a) **Directed Surveillance:** There is a very high likelihood of malicious surveillance directed towards the control room of the Dyke. Such surveillance may expose the weak points of the functions and machinery of the Dyke and leave it vulnerable to attack. Risk to the control room under directed surveillance is considered **very high**.

(b) **Sabotage:** There is a very high likelihood of sabotage directed towards the control room of the Dyke. Such sabotage may cause a compromise to the smooth operations and functioning of the Dyke machinery and may cause a cascading effect on the Dyke structure itself. Risk of sabotage to the control room is considered **very high**.

(c) **Sabotage (Railway Corridor):** The control room is physically separated from the railway corridor; however, sabotage to the railway corridor may result in a compromise on the regular functioning of the control room and subsequently the functioning of the Dyke. Risk to the control room in the event of sabotage to the railway corridor is considered **high**.

(d) **Indirect Fire Area Weapons:** Risk to the control room under attack from indirect fire area weapons is considered **high**.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** Risk the control room under VBIED attack is considered **high**.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** Risk to the control room under PBIED attack is considered **high**.

(g) **Theft of Stores and Equipment:** Risk of theft of stores and equipment from the control room is considered **very high**.

(h) **Disruption of Transportation:** Considered **moderate** risk to the control room.

(i) **Demonstrations and Blockades:** Considered **moderate** risk to the control room.

(j) **Mob Violence:** Considered **very high** risk to the control room and personnel therein.

(k) **Active Shooter:** Considered **high** risk to the control room and personnel therein.

(l) **Arson:** Considered **high** risk to the control room.

(m) **Road Traffic Incidents:** Considered **moderate** risk to the control room.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **moderate** risk to the control room.

(o) **Disputes with Host Communities:** Considered **moderate** risk to the control room.

(p) **Surface Ship Attack:** Given the proximity of the Dyke to hostile neighbours and the high value of the project, the likelihood of surface ship attack during a wartime situation is considered high. It is likely that the control room may be considered a viable target. Risk to the control room under a surface ship attack is considered **very high**.

(q) **Subsurface Attack:** Considered **moderate** risk to the control room.

(r) **Subsurface Attack by Unmanned Vehicles:** Considered **low** risk to the control room.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **low** risk to the control room.

(t) **Fast Coastal Attack Craft:** Similar to surface ship attack. These craft use stealth and speed to close in the target to carry out ballistic attacks on a selected target. Considered **high** risk to the control room.

(u) **Aircraft Impact:** Considered **very high** risk to the control room.

(v) **Drone Attack:** Considered **very high** risk to the control room.

(w) **Air Launched Bomb/Missile Attack:** Considered **very high** risk to the control room.

(x) **Aerial Surveillance by Drones:** Considered **high** risk to the control room.

(y) **Disclosure of information:** As the main hub of activities controlling the machinery and smooth functioning of the Dyke, it is likely that disclosure of any information regarding these functions can compromise the security of the Dyke. Disclosure of information, whether with or without malicious intent is considered **very high** risk to the control room.

(z) **Cyber Attack:** Cyber-attacks on a Dyke control system are a real and potent hazard and can have a crippling effect on operations. Challenges consist of factors that increase the probability of a cyber-attack and factors that limit the ability to implement ideal security enhancements. Components impacted could include but are not restricted to the facilities, systems, equipment, services, and diagnostics that provide the functional monitoring, control and protection capabilities necessary for effective and reliable operation. Cyber-attack is considered **very high** risk to the control room.

3.1.5 Analysis of Irrigation Structure

The primary purpose of the Dyke is to provide irrigation water to the Saurashtra region. Irrigation structures include canals, conduits, pumping/ lifting station and associated machinery. It is likely that with the malicious intent of disrupting irrigation to these areas, the irrigation structure may be targeted and compromised.

(a) **Directed Surveillance:** There is a **high** likelihood of malicious surveillance directed towards the irrigation pumping stations of the Dyke.

(b) **Sabotage:** Sabotage to the pumping stations, and associated mechanisms, is considered **very high** risk to the irrigation structure of the Dyke.

(c) **Sabotage (Railway Corridor):** Considered **low** risk to the irrigation structure.

(d) **Indirect Fire Area Weapons:** Considered **moderate** risk to the irrigation structure.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** Considered **moderate** risk to the irrigation structure.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** Considered **moderate** risk to the irrigation structure.

(g) **Theft of Stores and Equipment:** Theft or tampering of mechanisms that control the irrigation structure is likely. Theft of equipment is therefore considered **high** risk to the irrigation structure.

(h) **Disruption of Transportation:** Considered **low** risk to the irrigation structure.

(i) **Demonstrations and Blockades:** Considered **moderate** risk to the irrigation structure.

(j) **Mob Violence:** Considered **moderate** risk to the irrigation structure.

(k) **Active Shooter:** Considered **low** risk to the irrigation structure.

(l) **Arson:** Considered **low** risk to the irrigation structure.

(m) **Road Traffic Incidents:** Considered **low** risk to the irrigation structure.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **moderate** risk to the irrigation structure.

(o) **Disputes with Host Communities:** Disputes with host communities may lead to tampering of the machinery that controls the irrigation structure and is therefore considered **high** risk to the irrigation structure.

(p) **Surface Ship Attack:** Considered **low** risk to the irrigation structure.

(q) **Subsurface Attack:** Considered **low** risk to the irrigation structure.

(r) **Subsurface attack by Unmanned Vehicles:** Considered **low** risk to the irrigation structure.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **low** risk to the irrigation structure.

(t) **Fast Coastal Attack Craft:** Considered **low** risk to the irrigation structure.

(u) **Aircraft Impact:** Considered **very high** risk to the irrigation structure.

(v) **Drone Attack:** It is unlikely that a drone attack will be targeted at the irrigation structure given more viable targets, however in the event of a drone attack on the irrigation structure the likelihood of effect on the structure. Drone attack risk to the irrigation structure is considered **moderate**.

(w) **Air Launched Bomb/Missile Attack:** In the likelihood of a wartime situation, such an attack is considered **very high** risk to the irrigation structure.

(x) **Aerial Surveillance by Drones:** Considered **high** risk to the irrigation structure.

(y) **Disclosure of information:** Considered **moderate** risk to the irrigation structure.

(z) **Cyber Attack:** Considered **high** risk to the operations of the mechanisms of the irrigation structure.

3.1.6 Analysis of Road Transportation Corridor

The Dyke aims to link the Saurashtra region with South Gujarat thereby cutting down the travel time by road substantially. Though alternate routes would continue to be available,

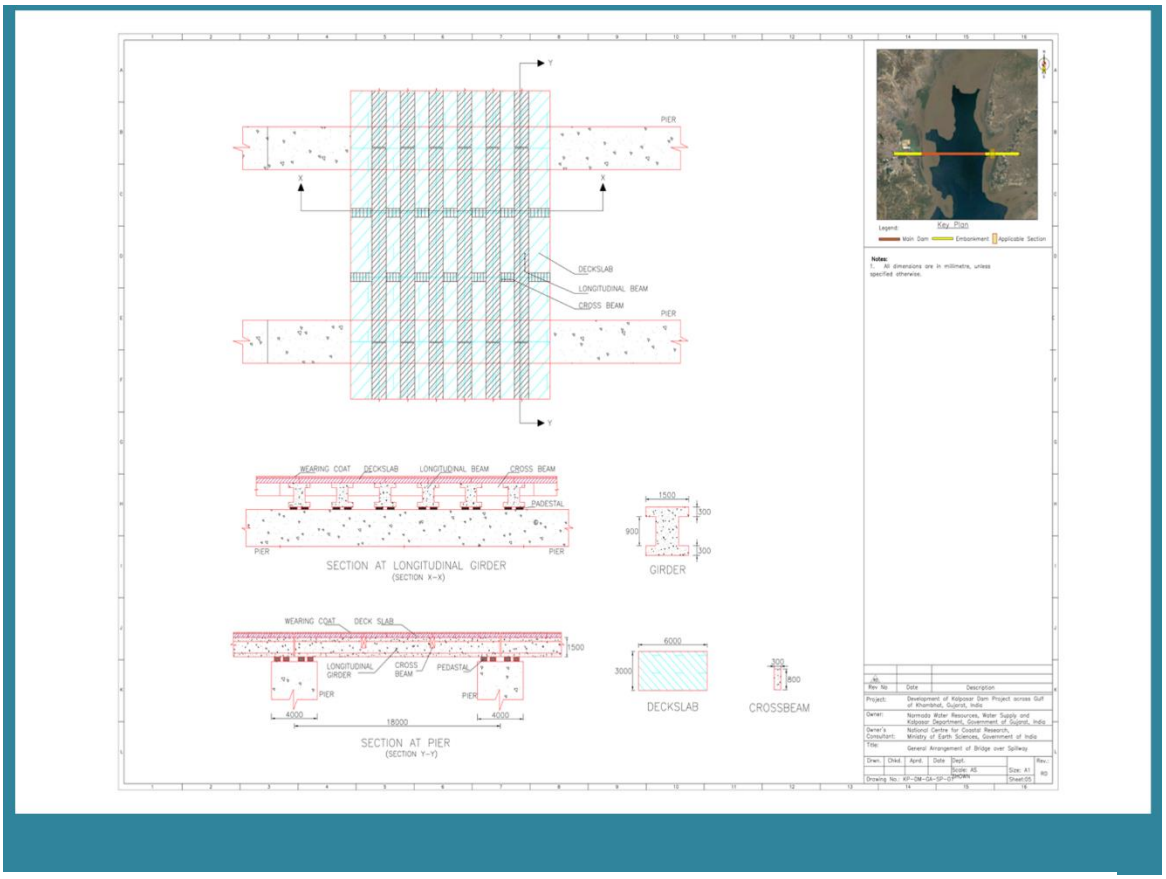


Figure 18 : General Arrangement Bridge over Flood regulator

these would be longer and more time consuming. The crest of the Dyke is designed to have a sixteen-lane road carriageway with a central median, a pedestrian walkway to one side and a railway freight corridor on the other side with two railway tracks. Part of the Rail and Road corridor is designed to go over the flood regulator of the Dyke on a viaduct supported by pillars.

As per the design, a Security Hold Area is being planned in the inter-tidal zone of the road transportation corridor for physical checking or screening of vehicles. As per the plan, suitable ramps are being suggested so that vehicles can be diverted to the security hold area and can merge with existing traffic once checking is completed.

Median openings for U Turns and emergency lanes for breakdown vehicles to park for repairing activities are being designed at 5km intervals along the road transportation corridor. Moreover, on the reservoir side of the road transportation corridor, a tree zone of 5m has been proposed so that lighting will not affect the aquatic life of the reservoir. Additionally, a setback distance of 3m is being considered between the road and rail corridors.

(a) **Directed Surveillance:** Considered **moderate** risk to the road transportation corridor.

(b) **Sabotage:** Considered **high** risk to the road transportation corridor.

(c) **Sabotage (Railway Corridor):** Sabotage to the railway corridor can have a cascading impact on the road transportation corridor and is therefore considered **high** risk to the road transportation corridor.

(d) **Indirect Fire Area Weapons:** Considered **moderate** risk to the road transportation corridor.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** Considered **high** risk to the road transportation corridor.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** Considered **moderate** risk to the road transportation corridor.

(g) **Theft of Stores and Equipment:** Considered **moderate** risk to the road transportation corridor.

(h) **Disruption of Transportation:** Considered **moderate** risk to the road transportation corridor.

(i) **Demonstrations and Blockades:** Considered **high** risk to the road transportation corridor.

(j) **Mob Violence:** Considered **moderate** risk to the road transportation corridor.

(k) **Active Shooter:** Considered **moderate** risk to the road transportation corridor.

(l) **Arson:** Considered **moderate** risk to the road transportation corridor.

(m) **Road Traffic Incidents:** Considered **high** risk to the road transportation corridor.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **moderate** risk to the road transportation corridor.

(o) **Disputes with Host Communities:** Considered **moderate** risk to the road transportation corridor.

(p) **Surface Ship Attack:** An attack against the Dyke during armed conflict from a surface ship using naval guns or missiles may impact the Dyke and the road transportation corridor on the Dyke's crest. Given the proximity of the Dyke to hostile neighbours and the high value of the project, the likelihood of surface ship attack during a wartime situation is considered **high** risk to the road transportation corridor.

(q) **Subsurface Attack:** An attack against the Dyke through small submersible craft using torpedoes or human delivered ordnance is considered likely. Such attacks, especially those delivered by Special Forces or state sponsored forces trained for Samundari Jihad using small submersible craft may be used even in less than war situations and have an

element of deniability. The risk to the road transportation corridor in the event of such an attack is considered **high**.

(r) **Subsurface Attack by Unmanned Vehicles:** Considered **low** risk to the road transportation corridor.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **low** risk to the road transportation corridor.

(t) **Fast Coastal Attack Craft:** Considered **moderate** risk to the road transportation corridor.

(u) **Aircraft Impact:** Considered **very high** risk to the road transportation corridor.

(v) **Drone Attack:** Considered **high** risk to the road transportation corridor.

(w) **Air Launched Bomb/Missile Attack:** In an armed conflict situation an air launched bomb attack is considered **very high** risk to the road transportation corridor.

(x) **Aerial Surveillance by Drones:** Considered **high** risk to the road transportation corridor.

(y) **Disclosure of Information:** Considered **low** risk to the road transportation corridor.

(z) **Cyber Attack:** Considered **moderate** risk to the road transportation corridor.

3.1.7 Analysis of Rail Transportation Corridor

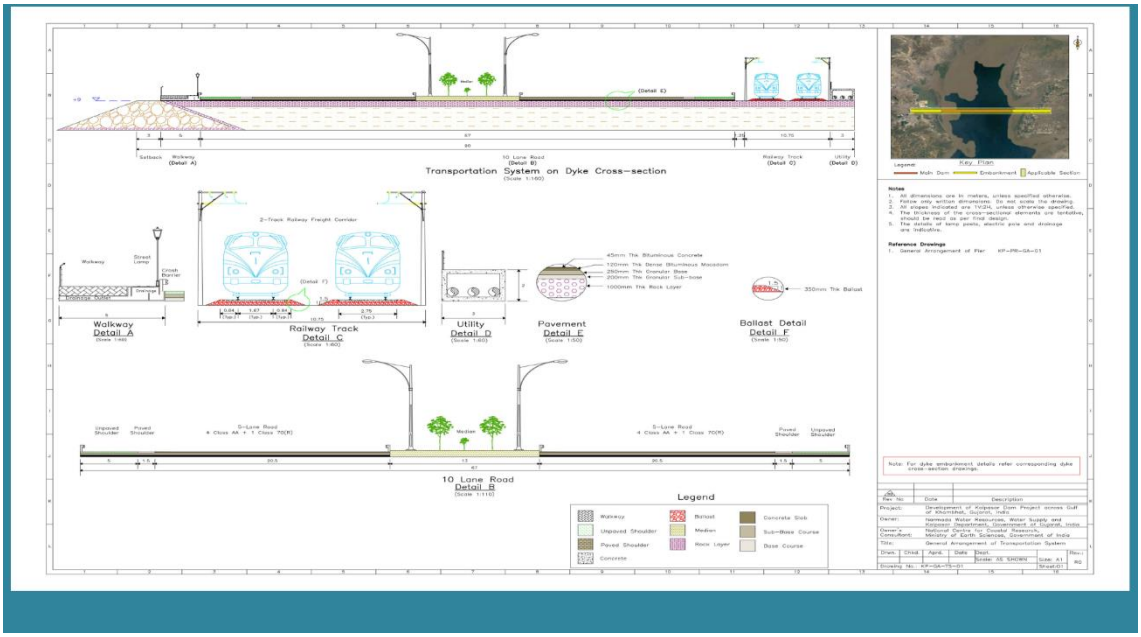


Figure 19 : Layout Transportation Corridor

The Dyke aims to link the Saurashtra region with South Gujarat by rail network for both passenger and freight movement thereby cutting down the travel time substantially. Though alternate routes would continue to be available, these would be longer and more time consuming.

There is a provision being made for fencing all along the railway corridor to prevent trespassing of humans and animals and consequent run over while a 900mm wide footpath is being proposed along one side of the track. The railway corridor is designed to go over the flood regulator on a viaduct and the pier will be designed with space for inspection and replacement of bearings.

(a) **Directed Surveillance:** Considered **moderate** risk to the rail transportation corridor.

(b) **Sabotage:** Considered **high** risk to the rail transportation corridor.

(c) **Indirect Fire Area Weapons:** Considered **moderate** risk to the rail transportation corridor.

(d) **Vehicle Borne Improvised Explosive Devices (VBIED):** Considered **moderate** risk to the rail transportation corridor.

(e) **Personnel Borne Improvised Explosive Device (PBIED):** Considered **moderate** risk to the rail transportation corridor.

(f) **Theft of Stores and Equipment:** Considered **high** risk to the rail transportation corridor.

(g) **Disruption of Transportation:** Considered **moderate** risk to the rail transportation corridor.

(h) **Demonstrations and Blockades:** Considered **moderate** risk to the to the rail transportation corridor.

(i) **Mob Violence:** Considered **moderate** risk to the rail transportation corridor.

(j) **Active Shooter:** Considered **moderate** risk to the rail transportation corridor.

(k) **Arson:** Considered **moderate** risk to the rail transportation corridor.

(l) **Road Traffic Incidents:** Considered **low** risk to the rail transportation corridor.

(m) **Labour Disputes/Strikes/Demonstrations:** Considered **moderate** risk to the rail transportation corridor.

(n) **Disputes with Host Communities:** Considered **moderate** risk to the rail transportation corridor.

(o) **Surface Ship Attack:** Considered **high** risk to the rail transportation corridor.

(p) **Subsurface Attack:** Considered **high** risk to the rail transportation corridor.

(q) **Subsurface Attack by Unmanned Vehicles:** Considered **moderate** risk to the rail transportation corridor.

(r) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **moderate** risk to the rail transportation corridor.

(s) **Fast Coastal Attack Craft:** Considered **moderate** risk to the rail transportation corridor.

(t) **Aircraft Impact:** Considered **high** risk to the rail transportation corridor.

(u) **Drone Attack:** Considered high risk to the rail transportation corridor.

(v) **Air Launched Bomb/Missile Attack:** In an armed conflict situation risk of an air launched bomb attack on the rail transportation corridor is considered **high**.

(w) **Aerial Surveillance by Drones:** Considered **high** risk to the rail transportation corridor.

(x) **Disclosure of information:** Considered **low** risk to the rail transportation corridor.

(y) **Cyber Attack:** Considered **moderate** risk to the rail transportation corridor.

3.1.8 Analysis of Solar/Wind Farm

Provides captive power to the Dyke as alternate sources of power would be available through the power grid.

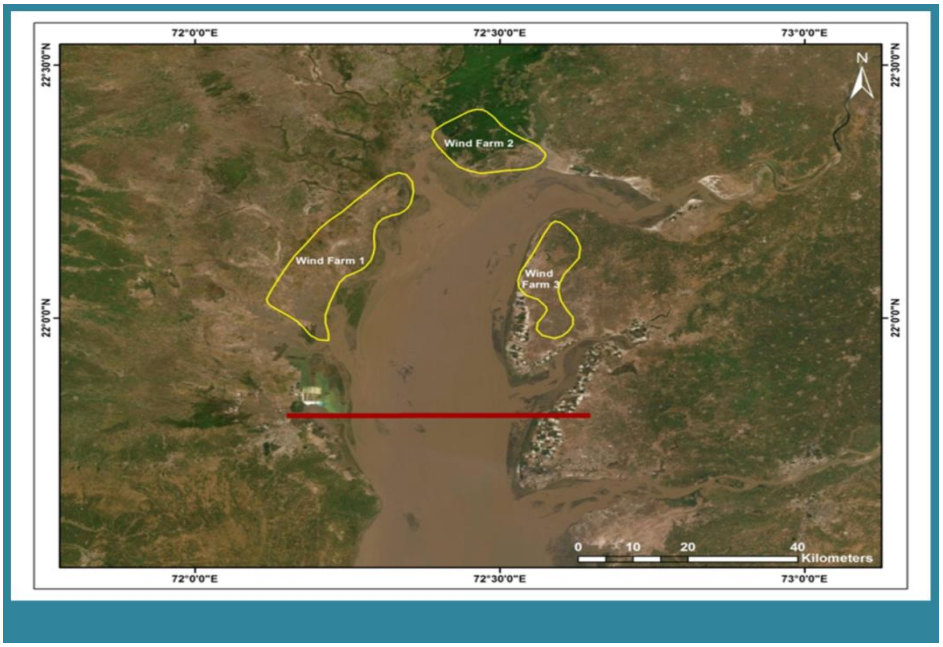


Figure 20 : Wind Farm Locations

(a) **Directed Surveillance:** Considered **moderate** risk to the solar/wind farm.

(b) **Sabotage:** Considered **moderate** risk to the solar/wind farm.

(c) **Sabotage (Railway Corridor):** Considered **low** risk to the solar/wind farm.

(d) **Indirect Fire Area Weapons:** Considered **moderate** risk to the solar/wind farm.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** Considered **moderate** risk to the solar/wind farm.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** Considered **moderate** risk to the solar/wind farm.

(g) **Theft of Stores and Equipment:** Given the high value of movable parts used in such projects and ease of access to the general public within the vicinity of the project, it is likely that attempts may be made either by the Dyke's hired personnel or the general public to tamper with or lift some high value components of the solar/wind farm. Risk of theft of stores and equipment from the solar/wind farm is therefore considered **high**.

(h) **Disruption of Transportation:** Considered **moderate** risk to the solar/wind farm.

(i) **Demonstrations and Blockades:** Considered **moderate** risk to the solar/wind farm.

(j) **Mob Violence:** Considered **moderate** risk to the solar/wind farm.

(k) **Active Shooter:** Considered **low** risk to the solar/wind farm.

(l) **Arson:** Considered **moderate** risk to the solar/wind farm.

(m) **Road Traffic Incidents:** Considered **low** risk to the solar/wind farm.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **moderate** risk to the solar/wind farm.

(o) **Disputes with Host Communities:** Considered **moderate** risk to the solar/wind farm.

(p) **Surface Ship Attack:** Considered **moderate** risk to the solar/wind farm.

(q) **Subsurface Attack:** Considered **moderate** risk to the solar/wind farm.

(r) **Subsurface Attack by Unmanned Vehicles:** Considered **low** risk to the solar/wind farm.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **moderate** risk to the solar/wind farm.

(t) **Fast Coastal Attack Craft:** Considered **moderate** risk to the solar/wind farm.

(u) **Aircraft Impact:** Considered **high** risk to the solar/wind farm.

(v) **Drone Attack:** Considered **high** risk to the solar/wind farm.

(w) **Air Launched Bomb/Missile Attack:** Considered **high** risk to the solar/wind farm.

(x) **Aerial Surveillance by Drones:** Considered **high** risk to the solar/wind farm.

(y) **Disclosure of Information:** Considered **moderate** risk to the solar/wind farm.

(z) **Cyber Attack:** Considered **high** risk to the to the solar/wind farm.

3.1.9 Analysis of Trained Operation and Maintenance Personnel

Operations and maintenance personnel as well as experts who would be handling day to day operations / maintenance as well as attend to any major breakdowns

(a) **Directed Surveillance:** As key personnel to the functioning of the Dyke, it is likely that operation and maintenance personnel of the Dyke may be of special interest to adversaries, either as a means of acquiring compromising information or grooming as possible co-conspirators to their cause. Risk of directed surveillance is therefore considered **very high** to the trained operation and maintenance personnel.

(b) **Sabotage:** n/a

(c) **Sabotage (Railway Corridor):** Considered **high** risk to the trained operation and maintenance personnel.

(d) **Indirect Fire Area Weapons:** Considered **high** risk to the trained operation and maintenance personnel.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** Considered **very high** risk to the trained operation and maintenance personnel.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** Considered **high** risk to the trained operation and maintenance personnel.

(g) **Theft of Stores and Equipment:** n/a

(h) **Disruption of Transportation:** Considered **high** risk to the trained operation and maintenance personnel.

(i) **Demonstrations and Blockades:** Considered **moderate** risk to the trained operation and maintenance personnel.

(j) **Mob Violence:** Considered **high** risk to the trained operation and maintenance personnel.

(k) **Active Shooter:** Considered **high to very high** risk to the trained operation and maintenance personnel.

(l) **Arson:** Considered **high** risk to the trained operation and maintenance personnel.

(m) **Road Traffic Incidents:** Considered **high** risk to the trained operation and maintenance personnel.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **high** risk to the trained operation and maintenance personnel.

(o) **Disputes with host communities:** Considered **high** risk to the trained operation and maintenance personnel.

(p) **Surface ship attack:** Considered **very high** risk to the trained operation and maintenance personnel.

(q) **Subsurface attack:** Considered **high** risk to the trained operation and maintenance personnel.

(r) **Subsurface attack by unmanned vehicles:** Considered **moderate** risk to the trained operation and maintenance personnel.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **moderate** risk to the trained operation and maintenance personnel.

(t) **Fast Coastal Attack Craft:** Considered **high** risk to the trained operation and maintenance personnel.

(u) **Aircraft Impact:** Considered **very high** risk to the trained operation and maintenance personnel.

(v) **Drone Attack:** Considered **very high** risk to the trained operation and maintenance personnel.

(w) **Air Launched Bomb/Missile Attack:** Considered **very high** risk to the trained operation and maintenance personnel.

(x) **Aerial Surveillance by Drones:** Considered **high** risk to the trained operation and maintenance personnel.

(y) **Disclosure of information:** Considered **very** high risk to the trained operation and maintenance personnel.

(z) **Cyber Attack:** Considered **low** risk to the trained operation and maintenance personnel.

3.1.10 Analysis of Power Transmission and Distribution Network

These would typically comprise Switchyard, Transmission lines, Emergency Generators, Transformers etc. to provide electrical supply to the main machinery, pumps and control stations

(a) **Directed Surveillance:** Considered **high** risk to the power transmission and distribution network.

(b) **Sabotage:** Considered **very high** risk to the power transmission and distribution network.

(c) **Sabotage (Railway Corridor):** Considered **very high** risk to the power transmission and distribution network.

(d) **Indirect Fire Area Weapons:** Considered **moderate** risk to the power transmission and distribution network.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** Considered **high** risk to the power transmission and distribution network.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** Considered **moderate** risk to the power transmission and distribution network.

(g) **Theft of Stores and Equipment:** Considered **very high** risk to the power transmission and distribution network.

(h) **Disruption of Transportation:** Considered **moderate** risk to the power transmission and distribution network.

(i) **Demonstrations and Blockades:** Considered **moderate** risk to the power transmission and distribution network.

(j) **Mob Violence:** Considered **moderate** risk to the power transmission and distribution network.

(k) **Active Shooter:** Considered **moderate** risk to the power transmission and distribution network.

(l) **Arson:** Considered **moderate** risk to the power transmission and distribution network.

(m) **Road Traffic Incidents:** Considered **low** risk to the power transmission and distribution network.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **high** risk to the power transmission and distribution network.

(o) **Disputes with Host Communities:** Considered **moderate** risk to the power transmission and distribution network.

(p) **Surface Ship Attack:** Considered **high** risk to the power transmission and distribution network.

(q) **Subsurface Attack:** Considered **moderate** risk to the power transmission and distribution network.

(r) **Subsurface Attack by Unmanned Vehicles:** Considered **moderate** risk to the power transmission and distribution network.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **moderate** risk to the power transmission and distribution network.

(t) **Fast Coastal Attack Craft:** Considered **moderate** risk to the power transmission and distribution network.

(u) **Aircraft Impact:** Considered **very high** risk to the power transmission and distribution network.

(v) **Drone Attack:** Considered **high** risk to the power transmission and distribution network.

(w) **Air Launched Bomb/Missile Attack:** Considered **very high** risk to the power transmission and distribution network.

(x) **Aerial Surveillance by Drones:** Considered **high** risk to the power transmission and distribution network.

(y) **Disclosure of Information:** Considered **high** risk to the power transmission and distribution network.

(z) **Cyber Attack:** Considered **very high** risk to the power transmission and distribution network.

3.1.11 Analysis of Maintenance Corridor/Galleries

A standalone maintenance corridor has been planned near the crest of the Dyke to provide access to the flood regulator gates and other parts of the Dyke

(a) **Directed Surveillance:** Considered **moderate** risk to the maintenance corridor/galleries.

(b) **Sabotage:** Considered **high** risk to the to the maintenance corridor/galleries.

(c) **Sabotage (Railway Corridor):** Considered **moderate** risk to the maintenance corridor/galleries.

(d) **Indirect Fire Area Weapons:** Considered **moderate** risk to the maintenance corridor/galleries.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** Considered **low** risk to the maintenance corridor/galleries.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** Considered **moderate** risk to the maintenance corridor/galleries.

(g) **Theft of Stores and Equipment:** Considered **moderate** risk to the maintenance corridor/galleries.

(h) **Disruption of Transportation:** Considered **low** risk to the maintenance corridor/galleries.

(i) **Demonstrations and Blockades:** Considered **moderate** risk to the maintenance corridor/galleries.

(j) **Mob Violence:** Considered **moderate** risk to the maintenance corridor/galleries.

(k) **Active Shooter:** Considered **moderate** risk to the maintenance corridor/galleries.

(l) **Arson:** Considered **moderate** risk to the maintenance corridor/galleries.

(m) **Road Traffic Incidents:** Considered **moderate** risk to the maintenance corridor/galleries.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **high** risk to the maintenance corridor/galleries.

(o) **Disputes with Host Communities:** Considered **high** risk to the maintenance corridor/galleries.

(p) **Surface Ship Attack:** Considered **high** risk to the maintenance corridor/galleries.

(q) **Subsurface Attack:** Considered **high** risk to the maintenance corridor/galleries.

(r) **Subsurface Attack by Unmanned Vehicles:** Considered **low** risk to the maintenance corridor/galleries.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **low** risk to the maintenance corridor/galleries.

(t) **Fast Coastal Attack Craft:** Considered **high** risk to the maintenance corridor/galleries.

(u) **Aircraft Impact:** Considered **high** risk to the maintenance corridor/galleries.

(v) **Drone Attack:** Considered **high** risk to the maintenance corridor/galleries.

(w) **Air Launched Bomb/Missile Attack:** Considered high risk to the maintenance corridor/galleries.

(x) **Aerial Surveillance by Drones:** Considered **high** risk to the maintenance corridor/galleries.

(y) **Disclosure of Information:** Considered **high** risk to the maintenance corridor/galleries.

(z) **Cyber Attack:** Considered **moderate** risk to the maintenance corridor/galleries.

3.1.12 Analysis of Machinery Space

Spaces or rooms where machinery and equipment are installed for the control and operation of various functions

(a) **Directed Surveillance:** Machinery spaces are the backbone of the operations of a Dyke and most vulnerable to attack. In the past, terrorists have monitored targets for extended periods to find flaws and devise the most effective ways to strike them. The risk of malicious directed surveillance on the machinery spaces of the Dyke is considered **high**.

(b) **Sabotage:** There is a very high likelihood of sabotage directed towards the mechanisms of the Dyke. Such sabotage may cause a cascading effect on the Dyke, compromising its functioning and structure. Risk of sabotage to the machinery space is considered **very high**.

(c) **Sabotage (Railway Corridor):** While the railway corridor is designed to be separated from the machinery space and is designed to go over the flood regulator on a viaduct, a significant event on the corridor has the likelihood of impact on the flood regulator and other machinery of the Dyke. Risk to the machinery space in the event of sabotage to the railway corridor is considered **high**.

(d) **Indirect Fire Area Weapons:** In the event of an artillery attack on the Dyke, targeted shelling to the flood regulator has the likelihood of causing significant damage to the machinery space. Risk to the flood regulator and other machinery space in the event of such an attack is considered **high**.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** Considered **moderate** risk to the machinery space.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** Pedestrian access to the flood regulator and the machinery therein is restricted due to its inherent design. Risk of impact to the machinery spaces in the flood regulator through a PBIED event is considered low however there is likelihood that other machinery spaces of the Dyke remain accessible and vulnerable to a lone wolf attack and is therefore considered as **high** risk to the machinery space.

(g) **Theft of Stores and Equipment:** Considered **very high** risk to the machinery space.

(h) **Disruption of Transportation:** Considered **low** risk to the machinery space.

(i) **Demonstrations and Blockades:** Considered **moderate** risk to the machinery space.

(j) **Mob Violence:** Considered **high** risk to the machinery space.

(k) **Active Shooter:** Considered **moderate** risk to the machinery space.

(l) **Arson:** Considered **high** risk to the machinery space.

(m) **Road Traffic Incidents:** Considered **low** risk to the machinery space.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **high** risk to the machinery space.

(o) **Disputes with Host Communities:** Considered **high** risk to the machinery space.

(p) **Surface Ship Attack:** Considered **very high** risk to the machinery space.

(q) **Subsurface Attack:** Considered **high** risk to the machinery space.

(r) **Subsurface Attack by Unmanned Vehicles:** Considered **high** risk to the machinery space.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **high** risk to the machinery space.

(t) **Fast Coastal Attack Craft:** Considered **high** risk to the machinery space.

(u) **Aircraft Impact:** Considered **very high** risk to the machinery space.

(v) **Drone Attack:** Considered **very high** risk to the machinery space.

(w) **Air Launched Bomb/Missile Attack:** Considered **very high** risk to the machinery space.

(x) **Aerial Surveillance by Drones:** Considered **high** risk to the machinery space.

(y) **Disclosure of Information:** Considered **very high** risk to the machinery space.

(z) **Cyber Attack:** Considered **very high** risk to the machinery space.

3.1.13 Analysis of Administrative Infra/Complex

The area which houses offices of majority of the staff and from where majority of the administrative tasks are undertaken

(a) **Directed Surveillance:** Considered **high** risk to the administrative/infra complex.

(b) **Sabotage:** Considered **high** risk to the administrative/infra complex.

(c) **Sabotage (Railway Corridor):** Considered **low** risk to the administrative/infra complex.

(d) **Indirect Fire Area Weapons:** Considered **moderate** risk to the administrative/infra complex.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** Considered **high** risk to the administrative/infra complex.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** Considered **high** risk to the administrative/infra complex.

(g) **Theft of Stores and Equipment:** Considered **high** risk to the administrative/infra complex.

(h) **Disruption of transportation:** Considered **moderate** risk to the administrative/infra complex.

(i) **Demonstrations and blockades:** Considered **high** risk to the administrative/infra complex.

(j) **Mob Violence:** Considered **high** risk to the administrative/infra complex**.**

(k) **Active Shooter:** Considered **high** risk to the administrative/infra complex.

(l) **Arson:** Considered **high** risk to the administrative/infra complex.

(m) **Road Traffic Incidents:** Considered moderate risk to the administrative/infra complex.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **moderate** risk to the administrative/infra complex.

(o) **Disputes with host communities:** Considered **high** risk to the administrative/infra complex.

(p) **Surface Ship Attack:** Considered **high** risk to the administrative/infra complex.

(q) **Subsurface Attack:** Considered **high** risk to the administrative/infra complex.

(r) **Subsurface Attack by Unmanned Vehicles:** Considered **moderate** risk to the administrative/infra complex.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **moderate** risk to the administrative/infra complex.

(t) **Fast Coastal Attack Craft:** Considered **moderate** risk to the administrative/infra complex.

(u) **Aircraft Impact:** Considered **very high** risk to the administrative/infra complex.

(v) **Drone Attack:** Considered **high** risk to the administrative/infra complex.

(w) **Air Launched Bomb/Missile Attack:** Considered **very high** risk to the administrative/infra complex.

(x) **Aerial Surveillance by Drones:** Considered **high** risk to the administrative/infra complex.

(y) **Disclosure of Information:** Considered **high** risk to the administrative/infra complex.

(z) **Cyber Attack:** Considered **very high** risk to the administrative/infra complex.

3.1.14 Analysis of Storage Stacking Yard

Storage Yard is generally an open place where construction materials are stored during construction stage of a project. Smaller yards may also be found within a work premises for frequently required items in factories or service agencies

(a) **Directed surveillance:** Considered **high** risk to the storage stacking yard.

(b) **Sabotage:** Considered **high** risk to the storage stacking yard.

(c) **Sabotage (Railway Corridor):** Considered **moderate** risk to the storage stacking yard.

(d) **Indirect Fire Area Weapons:** Considered **moderate** risk to the storage stacking yard.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** Considered **high** risk to the storage stacking yard.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** Considered **moderate** risk to the storage stacking yard.

(g) **Theft of Stores and Equipment:** Considered **very high** risk to the storage stacking yard.

(h) **Disruption of Transportation:** Considered **high** risk to the storage stacking yard.

(i) **Demonstrations and Blockades:** Considered **high** risk to the storage stacking yard.

(j) **Mob Violence:** Considered **high** risk to the storage stacking yard.

(k) **Active Shooter:** Considered **moderate** risk to the storage stacking yard.

(l) **Arson:** Considered **high** risk to the storage stacking yard.

(m) **Road Traffic Incidents:** Considered **moderate** risk to the storage stacking yard.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **high** risk to the storage stacking yard.

(o) **Disputes with Host Communities:** Considered **high** risk to the storage stacking yard.

(p) **Surface Ship Attack:** Considered **high** risk to the storage stacking yard.

(q) **Subsurface Attack:** Considered **moderate** risk to the storage stacking yard.

(r) **Subsurface Attack by Unmanned Vehicles:** Considered **low** risk to the storage stacking yard.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **low** risk to the storage stacking yard.

(t) **Fast Coastal Attack Craft:** Considered **moderate** risk to the storage stacking yard.

(u) **Aircraft Impact:** Considered **high** risk to the storage stacking yard.

(v) **Drone Attack:** Considered **high** risk to the storage stacking yard.

(w) **Air Launched Bomb/Missile Attack:** Considered **high** risk to the storage stacking yard.

(x) **Aerial Surveillance by Drones:** Considered **high** risk to the storage stacking yard.

(y) **Disclosure of information:** Considered **high** risk to the storage stacking yard.

(z) **Cyber Attack:** Considered **moderate** risk to the storage stacking yard.

3.1.15 Analysis of Project Site Admin Infra

These a normally temporary office infrastructure created at work sites for project managers, engineers, supervisors etc for day-to-day work during the construction phase.

(a) **Directed surveillance:** Considered **high** risk to the project site admin infra.

(b) **Sabotage:** Considered **high** risk to the project site admin infra.

(c) **Sabotage (Railway Corridor):** Considered **low** risk to the project site admin infra.

(d) **Indirect Fire Area Weapons:** Considered **moderate** risk to the project site admin infra.

(e) **Vehicle Borne Improvised Explosive Devices (VBIED):** Considered **high** risk to the project site admin infra.

(f) **Personnel Borne Improvised Explosive Device (PBIED):** Considered **high** risk to the project site admin infra.

(g) **Theft of Stores and Equipment:** Considered **high** risk to the project site admin infra.

(h) **Disruption of Transportation:** Considered **moderate** risk to the project site admin infra.

(i) **Demonstrations and Blockades:** Considered **high** risk to the project site admin infra.

(j) **Mob Violence:** Considered **high** risk to the project site admin infra.

(k) **Active Shooter:** Considered **high** risk to the project site admin infra.

(l) **Arson:** Considered **high** risk to the project site admin infra.

(m) **Road Traffic Incidents:** Considered **moderate** risk to the project site admin infra.

(n) **Labour Disputes/Strikes/Demonstrations:** Considered **high** risk to the project site admin infra.

(o) **Disputes with Host Communities:** Considered **high** risk to the project site admin infra.

(p) **Surface Ship Attack:** Considered **high** risk to the project site admin infra.

(q) **Subsurface Attack:** Considered **high** risk to the project site admin infra.

(r) **Subsurface Attack by Unmanned Vehicles:** Considered **moderate** risk to the project site admin infra.

(s) **Surface Vessel Improvised Explosive Device (SVIED):** Considered **moderate** risk to the project site admin infra.

(t) **Fast Coastal Attack Craft:** Considered **moderate** risk to the project site admin infra.

(u) **Aircraft Impact:** Considered **very high** risk to the project site admin infra.

(v) **Drone Attack:** Considered **high** risk to the project site admin infra.

(w) **Air Launched Bomb/Missile Attack:** Considered **high** risk to the project site admin infra.

(x) **Aerial Surveillance by Drones:** Considered **very high** risk to the project site admin infra.

(y) **Disclosure of information:** Considered **very high** risk to the project site admin infra.

(z) **Cyber Attack:** Considered **very high** risk to the project site admin infra.

3.2 Risk Assessment

Assessing Risk is an important part of the security designing process as it provides the basis for defining the hazards, exposure, vulnerabilities, ability to recover, scale, areas, type of controls required and provides the `***Why'*** behind the exercise. Risk categorisation further assists in translating the Security Concept and Principles into the design. The exercise thus helps identifying the ideal controls, infrastructure, technical or processes that need to be planned as part of the Security Design.

Using criteria which are both analytical and through field observed work, the Risk Assessment for Kalpasar Dyke aims to identify various hazards that may be posed to the dyke infrastructure by inimical elements and incorporate procedures and physical measures to mitigate these hazards.

3.2.1 Hazards

(a) Background

The first step in a risk management program is a hazard assessment. A hazard assessment considers the full spectrum of hazards (i.e., criminal, accidental, terrorist, war/ armed conflict etc.) for a given facility/location and it evaluates the capability and intent of various potential sources of hazard and the circumstances surrounding those actions and conduct, to uncover any facts or evidence that indicate that violence or damage is likely to be carried out. It is a professional judgement based on analysis, as to the intent and capability of a particular or multiple hazard causes against particular asset / facility.

(b) Purpose

This Hazard Assessment is for forming the basis for the Conceptual Security Design and Master Plan that shall be recommended for the protection of assets at the Kalpasar site. The following Hazard Assessment is based on our initial assessment of the hazard scenarios, hazard source and the capability required to be considered hazardous to the assets at the Kalpasar site.

(c) Hazard Scales

The definition of a hazard for this assessment is any event/ act or deliberate omission that has the potential to cause damage or destruction to any asset of the project or cause disruption in the services being provided by the project since the purpose of this assessment is to assist in the design of the project security and defence systems.

Hazard in the Security context is a combination of adversary's capability and intent which are derived from a combination of factors regarding adversary's skills and resources which include knowledge, technology, weapons and tools, support structure and finances.

Further, intent is derived from objectives/ goals, need and history of similar actions. The security hazard scales are as below:

Table 17: Hazard Scales

Scale	Hazard	Description
5	**Very High**	The likelihood of a hazardous, weapon, and tactic being used against the site or asset is imminent. Internal decision-makers and/or external law enforcement and intelligence agencies determine the hazard is credible.
4	**High**	The likelihood of a hazardous, weapon, and tactic being used against the site or asset is expected. Internal decision-makers and/or external law enforcement and intelligence agencies determine the hazard is credible.
3	**Moderate**	The likelihood of a hazardous, weapon, and tactic being used against the site or asset is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the hazard is known, but is not verified.
2	**Low**	The likelihood of a hazardous, weapon, and tactic being used in the region is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the hazard exists, but is not likely.
1	**Very Low**	The likelihood of a hazardous, weapon, and tactic being used in the region or against the asset is very negligible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the hazard is non-existent or extremely unlikely.

3.2.2 Hazard Analysis

(a) Hazard Identification

Major security hazards that could affect the safety, security and operational efficiency of the Kalpasar dyke have been identified as under after detailed analysis undertaken in this study as also interactions and deliberations with various stakeholders in assessing the capability and intent of adversaries that has resulted in the final score.

Table 18: Hazard Score

S.No	Hazard		Score
H1	Directed surveillance	Surveillance directed at particular individuals of facility. Directed surveillance can be carried out overtly or covertly, and can involve human agents. Targeting methods include the interception of communications, the use of communications "traffic" data, visual surveillance devices, and devices	5

		that sense movement, objects or persons.	
H2	Sabotage	Sabotage is a deliberate action aimed at weakening a company through subversion, obstruction, disruption, and/or destruction.	4.5
H3	Sabotage (Railway corridor)	Sabotage is a deliberate action aimed at weakening a company through subversion, obstruction, disruption, and/or destruction.	4.5
H4	Indirect Fire Area Weapons	Indirect fire weapons include artillery units equipped with either field guns (howitzers), or heavy mortars. Artillery is that part of an army that controls the bigger, long-range weapons, formerly referred to as cannons	2.5
H5	Vehicle Borne Improvised Explosive Devices (VBIED)	VBIEDs are substantially larger than hand delivered IEDs, ranging from 100kg to, in extreme instances, 2,500kg in size. VBIEDs may be employed singly or in multiples, detonating simultaneously or sequentially depending upon the bomber's purpose. They may be delivered by individuals or groups (suicide bombers) on martyrdom missions who are prepared to die in the course of their attack.	3.5
H6	Personnel Borne Improvised Explosive Device (PBIED)	PBIEDs may be delivered by an individual or group and placed by hand. Such devices may be concealed in any form of bag or container. Alternatively, it may be worn about the body of an individual on a martyrdom mission (suicide bomber) who is prepared to die in the completion of their mission.	3
H7	Theft of stores and equipment.	Organised theft of high value goods from worksite or field camps. May involve theft from the worksite or diversion of goods in transit. Large scale theft of raw materials which effect building costs. e.g. cabling	5
H8	Disruption of transportation.	Any significant delay, interruption, or stoppage in the flow of trade caused by a natural disaster, heightened threat level, an act of terrorism, or any	5

		transportation security incident	
H9	Demonstrations and blockades.	Civil unrest, for whatever cause, resulting in a temporary breakdown of law and order in a contained geographic area. Protests may or may not be directly related to operations or interests.	5
H10	Mob Violence	A disturbance of the peace by several persons, assembled and acting with a common intent in executing a lawful or unlawful enterprise in a violent and turbulent manner.	4
H11	Active Shooter	An individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms and there is no pattern or method to their selection of victims	3.5
H12	Arson	Arson, in general, is the crime of maliciously, voluntarily, and wilfully setting fire to the building, buildings, or other property of another or of burning one's own property for an improper purpose, as to collect insurance.	3.5
H13	Road Traffic Incidents	A Road Traffic Incident usually involves at least one road vehicle being in collision with, either another vehicle, another road user, or a stationary roadside object, and which may result in injury or property damage.	5
H14	Labour Disputes/ Strikes/ Demonstrations	Threat of balloted or wildcat strikes by local employees, whether unionized or not.	5
H15	Disputes with Host Communities	Threat of disputes with host communities over employment, contracting, land use, environmental or similar issues. Such disputes may be peaceful or violent in nature and may result in demonstrations, work stoppages, vandalism or other security incidents.	4
H16	Surface Ship Attack	Attack delivered from surface ship using naval guns or missiles. Typically used against high value targets during war / war - like situations	5
H17	Subsurface Attack	Attack delivered from manned submarines or small craft using torpedoes or human delivered	5

		ordnance. Such attacks, especially those delivered by special forces using small submersible craft my be used even in less than war situations and have an element of deniability	
H18	Subsurface Attack by Unmanned Vehicles	Attack delivered from unmanned submarines or small craft. The unmanned craft in most cased acts as WBIED	3
H19	Surface Vessel Improvised Explosive Device (SVIED)	WBIEDS are a means of delivering a large IED to targets on or adjacent to the sea. The size of any device is limited by the handling characteristics of the craft used to transport it but may range up to 1000kg or more. Previous examples of WBIEDs have targeted vessels in ports, vessels under way and military port infrastructure.	4
H20	Fast Coastal Attack Craft	Similar to surface ship attack. These craft use stealth and speed to close in the target to carry out audacious attack by guns / missiles on the selected target	3.5
H21	Aircraft Impact	Accidental / Deliberate direct impact by a conventional aircraft / helicopter	3.5
H22	Drone Attack	Accidental / Deliberate direct impact or weapon release by a unmanned aerial vehicles	4.5
H23	Air Launched Bomb / Missile Attack	Deliberate attack by use of aircraft as mode of delivery. Generally in the domain of military forces during war / war like situation	4
H24	Aerial Surveillance by Drones	Monitoring by use of drones with camera payload either real time or remote. Capability commonly exists as a result of technology availability.	5
H25	Disclosure of Information	The theft of information the loss or unauthorised release of which can lead to political, social or economic or security impact	5
H26	Cyber Attack	Targeting information systems, command & control networks, system software etc. using all forms of existing Cyber tools	5

(b) Hazard Analysis

Twenty-Six active hazards have been shortlisted keeping in mind the location and nature of the project and present-day realities. As per our analysis the major active hazards

to the project emerge from Directed Surveillance, Sabotage, Theft of Stores and Equipment, Disruption of Transportation, Demonstrations and Blockades, Road Traffic Incidents, Labour Disputes/ Strikes/ Demonstrations, Surface Ship Attack, Subsurface Attack, Aerial Surveillance by Drones, Drone Attack, Disclosure of Information and Cyber Attack scoring Very High on the hazard scores.

(c) Cyber Hazard Scenarios

Cyber hazards today are an independent form of attack and therefore need to be understood and mitigation strategies formed through an independent analysis. Notwithstanding, considering the importance of such hazards, basic scenarios have been captured in this section to identify the same as a critical future study.

Cyber-attacks on a dyke control system are a real and potent hazard and can have a crippling effect on operations. Challenges consist of factors that increase the probability of a cyber-attack and factors that limit the ability to implement ideal security enhancements. Control System is a general term that encompasses several types of control systems and it is defined as the facilities, systems, equipment, services, and diagnostics that provide the functional monitoring, control and protection capabilities necessary for effective and reliable operation. These are highly network-based and use common and open standards for communication protocols; many controllers are also Internet Protocol (IP) addressable which are typically connected to remote controllers via private and/or public networks provided by telecommunications companies. In addition, common telecommunications technologies such as the internet, public-switched telephone networks, or cable or wireless networks are often used. The potential for system accessibility resulting from this interoperability exposes assets to cyber infiltration and subsequent manipulation of sensitive operations. Furthermore, increasingly sophisticated cyber-attack tools can exploit flaws in components, telecommunication methods, and common operating systems found in modern control systems.

Control systems may have poorly designed connections between control systems and enterprise networks, use unauthenticated command and control data, and not provide adequate access control for remote access points. Evolving cyber hazards, changes in cyber-intrusion technologies, and developments in information technology need to be considered while building security into control systems with long lifecycles. The potential for system accessibility resulting from interoperability exposes network assets to cyber infiltration and subsequent manipulation of sensitive operations. Furthermore, increasingly sophisticated cyber-attack tools can exploit flaws in COTS components, telecommunication methods, and common operating systems found in modern control systems.

3.2.3 Exposure

(a) Exposure Assessment

Exposure represents the infrastructure or critical asset exposed to a hazard. As brought out in the previous section CARVAR matrix has been used to identify and select critical assets based on their exposure score. A semi-quantitative numerical rating has been utilised to scale the elements of the CARVER matrix. Numerically depicted; **5** is the most extreme or critical exposure with **1** indicating the least exposure. Generally, the higher the score the higher the hazard exposure and risk to the asset. The scale is as follows:

Table 19: Exposure Scale

Scale	Criticality	Description
5	**Vital**	Vital for achieving organisational, business or project objective
4	**Crucial**	Crucial for achieving organisational, business or project objective
3	**Essential**	Essential achieving organisational, business or project objective
2	**Required**	Required for achieving organisational, business or project objective
1	**Not Essential**	Not Essential for achieving organisational, business or project objective

(b) Exposure Analysis

The Exposure Assessment has been conducted using CARVER methodology. It should be noted that the identified Hazards Scenarios are based on the consultants' understanding of the current and likely Indian regional and domestic hazards. Any alteration in the hazard type, escalation or de-escalation shall influence the outcome of the assessment.

(1) **Criticality** - Single points of failure, degree of importance to the Dyke and communication network functioning;
(2) **Accessibility** - Ease of access, Defence System Effectiveness;
(3) **Recuperability** - The time and effort required to recover from an adverse event;
(4) **Vulnerability** - Level of exposure to attack based on the likely adversary capabilities;
(5) **Effect** - Scope and magnitude of consequences that would result from malicious actions or attack; and
(6) **Recognisability** - Ability of an adversary to recognize an asset as a target, then locate the asset.

The scores obtained to quantify exposure of various project assets are as per table below:

Table 20: Exposure Score

Asset Description	C	A	R	V	E	R	Total	CARVER Score
Dyke (Structure)	5.0	5	5	2	5	5	27.0	4.5
Flood	5.0	5	5	4	5	5	29.0	4.8

Gates/Controls								
Abutments	3.0	3	5	2	3	5	21.0	3.5
Control Room	5.0	3	4	3	5	4	24.0	4.0
Irrigation Structure	5.0	5	4	3	4	3	24	4.0
Road Transportation Corridor	3	3	3	3	3	3	18.0	3.0
Rail Transportation Corridor	3	3	3	3	4	4	20.0	3.3
Solar / Wind Farm	3	3	3	3	4	4	20.0	3.3
Trained Operation and Maintenance Personnel	4	5	4	5	4	4	26.0	4.3
Power Transmission and Distribution network	5	4	4	4	4	4	25	4.2
Maintenance Corridor / Galleries	3.0	3	2	4	3	2	17	2.8
Machinery Space	5	3	5	4	4	4	25	4.2
Administrative Infra / Complex	3	3	3	3	5	5	22	3.7
Storage/ Stacking Yard	4	4	2	4	4	4	22	3.7
Project Site Admin Infra	3.0	4	3	5	5	5	25	4.2

3.2.4 Vulnerability

(a) Vulnerability Assessment

Vulnerability accounts for the susceptibility to damage of the assets exposed to the effects generated by the hazard. Personnel are highly vulnerable to a Lone Sniper attack as would be physical infrastructure like a slipway or an abutment. For the purpose of this assessment, the type of construction and internal placement of assets have been considered to arrive at the vulnerability score.

This assessment is based purely on the assessment of gaps and vulnerabilities as identified by Arista's team of veterans from their resident knowledge, site visits and issues disclosed by user during the visit. The same could be further strengthened through formal exchange of the user's list of current and future critical assets, current SOPs and response capability.

The vulnerabilities of dykes to manmade attacks greatly depend on site-specific conditions and characteristics that could be exploited by potential adversaries to cause structural damage or to disable or disrupt operations or critical functions. TEFs© listed in the previous section have been used to identify Vulnerabilities based on the core understanding of a perpetrator's tactics and how they are likely to conduct attacks on critical infrastructure and the potential of damage that can be caused. Since the 'Technological' and 'Process' controls are not yet in place or articulated at this point in time, the vulnerability assessment is more subjective in nature based on consultant's expert team observations. These would however be refined later when the equipment and process have been adopted into the design and follow on phases. The Vulnerability scales are as below:

Table 21: Vulnerability Scale

Scale	Vulnerability	Description
5	**Extreme**	Can cause extreme damage to asset type resulting in complete loss/ fatality or total disruption of functions.
4	**Serious**	Can cause serious damage to asset type resulting in major loss/ serious injury or severe disruption of functions.
3	**Moderate**	Can cause moderate damage to asset type resulting in partial loss/ injuries or partial disruption of functions.
2	**Minor**	Can cause minor damage to asset type resulting in some loss or delays in functions.
1	**Negligible**	Can cause negligible damage to asset type with no loss/ disruption of functions.

(b) Vulnerability Analysis

The weaknesses that can be exploited by an aggressor to make an asset susceptible to damage have been analysed. Keeping in mind the existing capabilities, intent shown by adversaries, availability of `off the shelf' technology, and the commensurate potential of damage that can be caused our findings revel that Surveillance and attacks by Drones Cyber Attack and sabotage can cause serious to extreme damage. As per classification, the dyke is thus extremely vulnerable to Drone and Cyber-attacks, since this can be achieved by bypassing every physical security design feature and attack can be undertaken from standoff distances. Apart from this the flood gates, control room, trained manpower also remain extremely vulnerable. The scores obtained are as per table below:

Table 22: Vulnerability Score

Vulnerability	Dam (Structure)	Spill Gates/Controls	Abutments	Control Room	Irrigation Structure	Road Tansportation Corridor	Rail Transportation Corridor	Solar / Wind Farm	Trained Operation and Maintenance	Power Transmission and Distribution	Maintenance Corridor / Galleries	Machinery Space	Administrative Infra / Complex	Storage/ Stacking Yard	Project Site Admin Infra
Directed surveillance	2	4	2	4	2	2	3	1	4	4	3	4	5	4	5
Sabotage	2	5	3	5	4	2	5	3	1	5	4	4	4	4	4
Sabotage (Railway corridor)	4	3	3	3	1	3	4	1	4	5	2	4	1	3	1
Indirect Fire Area Weapons	3	4	3	3	3	3	3	3	5	4	3	4	3	3	3
Vehicle Borne Improvised Explosive Devices (VBIED)	2	1	4	3	2	4	2	3	5	4	1	2	3	4	3
Personnel Borne Improvised Explosive Device (PBIED)	1	2	3	4	3	3	2	3	5	3	3	5	4	3	4
Theft of stores and equipment.	1	2	1	4	3	2	3	3	1	4	2	4	4	5	4
Disruption of transportation.	1	1	1	2	1	3	3	2	3	2	1	1	2	3	2
Demonstrations and blockades.	1	1	2	2	3	3	3	2	2	2	3	2	3	3	3
Mob Violence	1	2	2	5	2	3	3	3	4	3	3	4	4	5	4
Active Shooter	1	1	2	5	1	3	3	1	5	3	3	3	4	3	4
Arson	1	2	1	4	1	2	3	3	5	3	3	3	4	4	4
Road Traffic Incidents	1	1	1	2	1	3	1	2	5	1	2	1	2	3	2
Labour Disputes/ Strikes/ Demonstrations	1	1	1	3	2	1	2	3	4	3	3	3	3	3	4

Disputes with Host Communities	1	1	2	4	2	2	2	3	5	4	3	3	4	3	4
Surface Ship Attack	3	3	2	3	3	2	2	3	4	2	3	3	3	3	3
Subsurface Attack	4	3	2	4	1	4	4	3	4	4	4	4	4	4	4
Subsurface Attack by Unmanned Vehicles	4	4	1	1	1	3	3	1	4	2	4	2	1	1	1
Surface Vessel Improvised Explosive Device (SVIED)	4	5	1	1	1	1	3	1	2	2	1	3	1	1	1
Fast Coastal Attack Craft	2	3	1	2	1	1	3	1	2	3	1	4	2	2	2
Aircraft Impact	4	3	2	4	3	3	3	3	4	4	4	3	3	3	3
Drone Attack	4	5	2	5	4	5	4	4	5	5	4	4	5	3	5
Air Launched Bomb / Missile Attack	3	4	4	5	4	3	3	4	5	5	4	4	4	4	4
Aerial Surveillance by Drones	5	5	4	5	4	4	4	4	5	5	4	4	5	3	4
Disclosure of Information	4	4	2	4	2	3	3	4	4	4	3	4	3	3	4
Cyber Attack	3	4	1	5	3	3	3	4	4	5	3	4	5	3	5

3.2.5 Recuperability

(a) Recuperability Assessment

The ability of an organisation to recover from a situation plays a vital role in assessing the impact the situation or event would have on the organisation. Recuperability is a factor of process and procedures, effectiveness of countermeasures, efficiency of response, operational redundancy and training. In addition, documentation, review, communication and implementation towards continuous improvement of these factors are also assessed towards arriving at a recoverability score. The recoverability scores have been assessed by Arista's team of veterans based on their experience and user interaction during site visit. The lower the score the more unsatisfactory is the recuperability. The scale is as follows:

Table 23: Recuperability Scale

Scale	Recuperability	Description
1	**Unsatisfactory**	Processes, procedures neither documented nor reviewed and training of personnel is unsatisfactory. The countermeasures, response mechanisms and operational redundancies do not exist.
2	**Weak**	Processes, procedures sketchily documented or reviewed and training of personnel is weak. The countermeasures, response mechanisms and operational redundancies are not optimally in place nor tested or improvements required communicated and incorporated.
3	**Satisfactory**	Processes, procedures documented and reviewed occasionally and training of personnel is satisfactory. The countermeasures, response mechanisms and operational redundancies are partially in place and tested some times. Improvements required communicated and incorporated at times.
4	**Good**	Processes, procedures documented and reviewed systematically and training of personnel is good. Effective countermeasures, response mechanisms and operational redundancies in place and periodically tested. Improvements required communicated and incorporated.
5	**Excellent**	Processes, procedures documented and reviewed systematically and training of personnel is excellent. Highly effective countermeasures, response mechanisms and operational redundancies in place and routinely tested. Improvements required communicated and incorporated methodically.

(b) Recuperability Analysis

Recuperability is in the ability to speedily neutralise hazard and resume operations to meet operational objectives. It is a factor of process and procedures, effectiveness of countermeasures, efficiency of response, operational redundancy and training, as well as their documentation, review, communication and implementation towards continuous improvement of recoverability.

The cumulative recuperability score for each hazard is depicted in the table below. It can be seen that recuperability against Aircraft Impact, Air Launched Bomb/ Missile Attack, and Surface Ship Attack is the least and thus unsatisfactory. This is owing to the fact that these methods of attack can carry out large scale destruction thereby causing greater down time. On the asset site damage to the Dyke Structure, Flood Gates / Controls, Control Room, Transportation Corridor and Machinery Spaces is the most difficult to recover from or time consuming. The scores achieved are as follows:

Table 24: Recuperability Score

Recuperability	Dyke (Structure)	Flood Gates/Controls	Abutments	Control Room	Irrigation Structure	Road Tansportation Corridor	Rail Transportation Corridor	Solar / Wind Farm	Trained Operation and Maintenance Personnel	Power Transmission and Distribution network	Maintenance Corridor / Galleries	Machinery Space	Administrative Infra / Complex	Storage/ Stacking Yard	Project Site Admin Infra
Directed surveillance	0.9	1.1	2.1	1.2	0.8	2	2.5	0.9	1.2	1.9	2	1.7	2.1	2.2	1.8
Sabotage	0.8	1.5	2.8	1.4	1.1	0.9	4.9	3.1	2.1	1.2	1.9	1.3	2.2	1.6	1.9
Sabotage (Railway corridor)	1.1	1.2	2.9	1.3	2.8	1.3	2.1	2.4	1.7	1.5	1.6	1.9	2.4	3.1	2.7
Indirect Fire Area Weapons	3.1	1.5	2.9	1.4	2.8	2.9	2.8	2.6	2.8	4.1	2.8	1.8	1.9	2.9	1.9
Vehicle Borne Improvised Explosive Devices (VBIED)	2.1	1.1	4.1	1.5	1.8	1.9	1.9	2.7	1.4	1.9	2.7	1.9	1.2	2.1	1.1
Personnel Borne Improvised Explosive Device (PBIED)	2.8	4.1	4.9	1.9	3	3.1	2.2	3.3	2.1	2.9	2.9	1.9	1.9	2.8	2.1
Theft of stores and equipment.	1.1	2.2	2.6	1.3	1.4	1.4	1.4	1.6	2.2	1.1	2.2	1.3	1.9	1.1	2.2
Disruption of transportation.	1.9	2.8	2.6	1.9	2.1	2.2	2.6	1.7	1.1	2.2	2.4	2.7	1.7	1.1	2.1
Demonstrations and	2.1	2.1	1.7	1.9	3.1	3	1.3	2.1	2.2	2.1	1.9	2.2	1.3	1	1.3

blockades.															
Mob Violence	2.8	2.2	2.2	1.6	1.9	2.5	2.1	1.9	2.1	2.3	1.9	2.1	2	2.3	2
Active Shooter	2.8	1	2.9	2	2.4	2.2	3.1	2.8	2.1	2.2	2.1	3.2	2.2	3.1	1.9
Arson	2.2	2.1	2.3	1.7	2.4	2.1	3.2	3	2.1	3	2.1	1.5	2.1	2	2.1
Road Traffic Incidents	1.1	2.1	1.1	2.1	2.3	1.6	2.2	3.2	1.8	2.7	2.1	2.2	2.2	2.1	1.5
Labour Disputes/ Strikes/ Demonstrations	2.1	1.1	2.2	2.1	1.4	1	1.5	1.2	2.1	1.1	1.3	1.3	2.4	1.1	2.1
Disputes with Host Communities	2.2	2.1	5	3.2	1.1	2.1	2.2	2	2	4	1.3	1.5	1.7	1.4	1.8
Surface Ship Attack	1	0.9	1.6	1	5	1.1	1	3	1.3	1	1.1	1	1.2	1.6	1.3
Subsurface Attack	1	1	5	3	2.1	1.8	1.9	2.1	2.1	3.2	2	1.6	2	4	2
Subsurface Attack by Unmanned Vehicles	2.1	1	2.3	2.7	2.8	4	3	2.2	3	1.7	5	1	1.1	2.1	1
Surface Vessel Improvised Explosive Device (SVIED)	5	1	2.4	2.3	2.4	2.3	3	1.1	1.5	2.1	2.4	1.4	1.1	2.1	1.1
Fast Coastal Attack Craft	1.1	1.5	1.5	1	1.9	1.1	2.1	1.1	1	2.3	0.7	1.2	1.2	2.1	1.2
Aircraft Impact	1	1	1	1	1	1	1.5	1.3	1	1.4	2	1	1	1.5	1
Drone Attack	2	1.5	1.3	1.5	4	2	2	1.5	1.5	2.3	2	1.3	2	1.1	2
Air Launched Bomb / Missile Attack	1	1	1.8	1.3	1.3	1.5	1.6	2	1.3	1.6	2	1	1	2.1	2
Aerial Surveillance by Drones	1.6	1.4	3	2.1	2.2	1.9	2.2	2.1	2.3	2.3	1.9	1.8	2.1	1.6	1.2
Disclosure of Information	4.1	1.5	3.9	1.1	2.2	4.1	4	2.9	1.2	1.5	1.3	1.2	1.2	1.4	1.2
Cyber Attack	2.8	1.1	1.4	1.2	1.4	2.1	2.2	2.1	5	1.5	2.1	1.1	1.5	2.3	1.6

3.2.6 Risk Scores / Matrix

In order to analyse risk, different types of action that can be brought to bear on each critical asset have been systematically re-evaluated through a comprehensive risk assessment process as undertaken above. It is the interplay of *Hazard, Exposure and Vulnerability* along with the ability to recover or *Recuperability* of the organization that provides a final risk score. In order to proceed with the security design process, it is imperative to know which critical asset has the maximum risk from a particular type of hazard. The risk matrix answers the ***Why*** behind the design by highlighting the sensitivity of the critical asset and helps evolving a risk treatment and mitigation plan which can be incorporated into the design process.

(a) Risk Scoring Scale

Risk assessment combines and analyses all factors to provide an overall picture of potential risks to an asset and using this information risk scores can be assigned to finally enable prioritisation of risks and their mitigation as well as treatment. The risk scoring scale is placed below for reference.

Table 25: Risk Scale

Scale	Risk	Description
5	**Very High**	The risk needs to be treated and mitigation measures instituted immediately. Activity closely monitored or stopped to obviate risk.
4	**High**	The risk needs to be treated and mitigation measures instituted without delay. Activity closely monitored and corrective action put in place till comprehensive mitigation measures are instituted.
3	**Moderate**	Mitigation required and measures should be considered based on the principle of "ALARP" (as low as reasonably practicable).
2	**Low**	Evaluate Residual Risk and accept those risks which are tolerable based on organisation's risk appetite and mitigate balance risks.
1	**Very Low**	Accept the risk in accordance with organisations security policy. Reassess periodically.

(b) Risk Analysis

Capabilities, motivation, resources and modus operandi, of twenty-six hazards have been enunciated below. In order to evolve a risk treatment and mitigation plan, objective scores assist in identifying critical assets through a risk-based approach, classification of assets indicating their Sensitivity as also evolving a Zoning Plan to evaluate the adequacy of security measures as required in the Operational Requirements. The scores achieved are placed at Table 17. Analysis indicates that the flood regulator, Machinery Spaces, Trained Operations and Maintenance Personnel and Control Room are assets exposed to the highest risk. Other assets which are at high risk include Project Site Administrative Infrastructure, Storage and Stacking Yard, Administrative and Machinery Spaces, Power Transmission and Distribution Network and Controls. These have been further individually analysed in the next section based on designs and plans obtained for greater in-depth understanding.

In the subsequent sections of the study, security concept and features including technology will be designed on the basis of the under-mentioned risks calculated. Acceptance of critical assets and risk score arrived at by the study team forms an important step towards further development of the study. *The findings of this Risk Assessment have been shared with the Kalpasar Project Management Committee as the Inception Report to seek acceptance prior formulation of the Conceptual Security Design and Master Plan, a go ahead for which was received. Accordingly, the subsequent Sections of this report have been developed keeping in mind the outcomes of the mutually accepted Risk Assessment.*

Table 26: Final Risk Scores

Risk Score	Dyke (Structure)	Flood Gates/Controls	Abutments	Control Room	Irrigation Structure	Road Tansportation Corridor	Rail Transportation Corridor	Solar / Wind Farm	and Maintenance Personnel	and Distribution network	Maintenance Corridor / Galleries	Machinery Space	Administrative Infra / Complex	Storage/ Stacking Yard	Project Site Admin Infra
Directed surveillance	50.0	81.8	21.4	75.0	56.3	22.5	27.0	25.0	75.0	47.4	33.8	52.9	53.6	40.9	62.5
Sabotage	56.3	75.0	24.1	80.4	81.8	50.0	23.0	21.8	10.7	93.8	47.4	69.2	40.9	56.3	47.4
Sabotage (Railway corridor)	81.8	56.3	23.3	51.9	8.0	51.9	42.9	9.4	52.9	75.0	28.1	47.4	9.4	21.8	8.3
Indirect Fire Area Weapons	21.8	60.0	23.3	48.2	24.1	23.3	24.1	26.0	40.2	22.0	24.1	50.0	35.5	23.3	35.5
Vehicle Borne Improvised Explosive Devices (VBIED)	21.4	20.5	22.0	45.0	25.0	47.4	23.7	25.0	80.4	47.4	8.3	23.7	56.3	42.9	61.4
Personnel Borne Improvised Explosive Device (PBIED)	8.0	11.0	13.8	47.4	22.5	21.8	20.5	20.5	53.6	23.3	23.3	59.2	47.4	24.1	42.9
Theft of stores and equipment.	20.5	20.5	8.7	69.2	48.2	32.1	48.2	42.2	10.2	81.8	20.5	69.2	47.4	102.3	40.9
Disruption of transportation.	11.8	8.0	8.7	23.7	10.7	30.7	26.0	26.5	61.4	20.5	9.4	8.3	26.5	61.4	21.4
Demonstrations and blockades.	10.7	10.7	26.5	23.7	21.8	22.5	51.9	21.4	20.5	21.4	35.5	20.5	51.9	67.5	51.9
Mob Violence	8.0	20.5	20.5	70.3	23.7	27.0	32.1	35.5	42.9	29.3	35.5	42.9	45.0	48.9	45.0

Active Shooter	8.0	22.5	15.5	56.3	9.4	30.7	21.8	8.0	53.6	30.7	32.1	21.1	40.9	21.8	47.4
Arson	10.2	21.4	9.8	52.9	9.4	21.4	21.1	22.5	53.6	22.5	32.1	45.0	42.9	45.0	42.9
Road Traffic Incidents	20.5	10.7	20.5	21.4	9.8	42.2	10.2	14.1	62.5	8.3	21.4	10.2	20.5	32.1	30.0
Labour Disputes/ Strikes/ Demonstrations	10.7	20.5	10.2	32.1	32.1	22.5	30.0	56.3	42.9	61.4	51.9	51.9	28.1	61.4	42.9
Disputes with Host Communities	10.2	10.7	9.0	28.1	40.9	21.4	20.5	33.8	56.3	22.5	S	45.0	52.9	48.2	50.0
Surface Ship Attack	67.5	75.0	28.1	67.5	13.5	40.9	45.0	22.5	69.2	45.0	61.4	67.5	56.3	42.2	51.9
Subsurface Attack	90.0	67.5	9.0	30.0	10.7	50.0	47.4	32.1	42.9	28.1	45.0	56.3	45.0	22.5	45.0
Subsurface Attack by Unmanned Vehicles	42.9	90.0	9.8	8.3	8.0	16.9	22.5	10.2	30.0	26.5	18.0	45.0	20.5	10.7	22.5
Surface Vessel Improvised Explosive Device (SVIED)	18.0	112.5	9.4	9.8	9.4	9.8	22.5	20.5	30.0	21.4	9.4	48.2	20.5	10.7	20.5
Fast Coastal Attack Craft	40.9	45.0	15.0	45.0	11.8	20.5	32.1	20.5	45.0	29.3	32.1	75.0	37.5	21.4	37.5
Aircraft Impact	90.0	67.5	45.0	90.0	67.5	67.5	45.0	51.9	90.0	64.3	45.0	67.5	67.5	45.0	67.5
Drone Attack	45.0	75.0	34.6	75.0	22.5	56.3	45.0	60.0	75.0	48.9	45.0	69.2	56.3	61.4	56.3
Air Launched Bomb / Missile Attack	67.5	90.0	50.0	86.5	69.2	45.0	42.2	45.0	86.5	70.3	45.0	90.0	90.0	42.9	45.0
Aerial Surveillance by Drones	70.3	80.4	30.0	53.6	40.9	47.4	40.9	42.9	48.9	48.9	47.4	50.0	53.6	42.2	75.0
Disclosure of Information	22.0	60.0	11.5	81.8	20.5	16.5	16.9	31.0	75.0	60.0	51.9	75.0	56.3	48.2	75.0
Cyber Attack	24.1	81.8	16.1	93.8	48.2	32.1	30.7	42.9	18.0	75.0	32.1	81.8	75.0	29.3	70.3

3.2.7 Overall Risk Evaluation & Observations

The vulnerabilities and weak points of the dyke are likely to be exploited by perpetrators with malicious intent. The exercise of analysing plans and drawings in the previous section has been aimed towards identifying and evaluating these weak points which can be damaged/disrupted resulting in a compromise to the security and safety of the dyke and associated surroundings. Further, examining the project based on TEFs© permits evaluating outcomes that will affect the Security Design process. Keeping in mind both the risk assessment and TEFs© the overall evaluation and observations of key critical assets are highlighted in the succeeding paragraphs.

(a) Evaluation & Observation - Dyke Structure, Abutments, Irrigation Structure, Solar/ Wind Farm, Power Transmission and Distribution Network

The inherent strength of the dyke structure, including abutments, in design and materials used ensures that the structures will remain stable unless specifically targeted in a warlike situation using military grade ordnance. During peace using improvised explosive devices the risks are limited however, sabotage and surveillance especially using drones to gain information for future targeting cannot be ruled out. Similarly, irrigation structures, solar and wind farm as well as power transmission and distribution network are all more susceptible during wartime, while sabotage and cyber-attacks during peace time pose greater risk.

(b) Evaluation & Observation - Flood Gates, Control Rooms, Machinery Spaces, Maintenance Corridor

Flood regulator gates, control rooms, machinery spaces and maintenance corridor remain the most vulnerable critical assets of the project with a variety of very high risks. Total of 100 gates in the flood regulator and amount of water stored in the reservoir on the landward side will almost guarantee substantial water flow and turbulence on the seaward side which will prevent boats and crafts from approaching near the gates. Any hazard of attack from boats and small crafts from the seaward side of the flood regulator will be dissipated.

The planned massive concrete stilling basin will be impervious to any damage from explosions involving even very large quantities of explosives when carried by boats and surface crafts from seaward side. Sub-surface craft will find it extremely difficult to approach the flood regulator due to subsurface currents in the water and also varying depths in the gulf. The stilling basin design will also prevent damage even if some very determined adversary is able to reach the structure.

From the reservoir side, boats and surface crafts are more likely to succeed in reaching the flood regulator because of greater depths in the reservoir and considerably less flow rate of the water being discharged into the gulf.

The vulnerable part will most likely be the mechanism which physically hoists and lowers the gates. Guides and concrete piles may be near impenetrable but the steel wire ropes which lift and lower the gates will be vulnerable to attacks from shaped/cutting explosive charges, mechanical cutters and gas cutters. If an adversary with intent to disrupt the dyke does get access to the reels and motors, they can, as well, be jammed and damaged by various means.

Both the control room, machinery space and maintenance corridor of the dyke are the hub of operational activity with highly sensitive equipment which if disrupted can have catastrophic effect on the overall functioning of the dyke. If specifically targeted, in cohesion when water levels are high due natural/ seasonal conditions they can be highly vulnerable to attacks with the aim of crippling the operations of the dyke. Sabotage and cyber-attack in peacetime pose greater risks, while their susceptibility to improvised explosives is moderate to low in war time.

(c) Evaluation & Observation - Road and Rail Transportation Corridor

The road and rail transportation corridors are a unique feature of this project and not many dykes exist where public at large is permitted to access the feature for regular use. This poses tremendous challenges in the design of security to ensure functionality without disruption of activities as well as robust security to various elements of the dyke.

Examination of the traffic study undertaken and the designs prepared, show that a large number of security related issues have clearly been taken care. The corridors are designed to pass over the crest of the dyke on a strengthened concrete structure with a rock base. The road corridor is on the reservoir side thus preventing general public from being able to approach close to flood regulator, maintenance corridors and machinery spaces which are at greater risk. The three-meter setback between the road and rail corridor prevents crossover of vehicles to target dyke features/ operations as well as the railway corridor itself.

The railway corridor which is to the seaward side offers a buffer zone to people and vehicles to undertake any targeting. While there are inherent hazards of sabotaging the tracks to create an incident during peacetime, the impact on the structure will be limited. To carry out an incident of value using IEDs to damage either of these structures is limited. Any such attempt would be to temporarily disrupt operations to gain limelight or media attention. Both the corridors are therefore less susceptible to risks during peace time; however, they present a very strategic target for adversaries during wartime using military grade ordnance.

(d) Evaluation & Observation - Trained Operation and Maintenance Personnel

The softest underbelly of any facility is the human resource without which activity or operation is not feasible. Further, targeting the workforce causes huge impact on the moral and further functionality. The ability to recover from loss of trained manpower who have built expertise in management and operation of a complex critical asset like the Kalpasar Dyke is very tough and time consuming.

The trained operations and maintenance manpower thus remains most vulnerable both during peacetime and wartime as they are easy to target and offer high gains to the adversary. They are susceptible to all forms of improvised explosive devises, active shooters, and wartime collateral loss of life and most other forms of hazards.

(e) Evaluation & Observation - Administrative Infra / Complex, Storage/ Stacking Yard, Project Site Admin Infra

The administrative infra/ complex, storage/ stacking yard, project site administrative infrastructure are all vital functional areas of the project. Their construction will be of

regular material with limited hardening. The flow of activity, movement of a variety personnel, including vendors, contactors, labour other than the project staff itself, presents a soft target to adversaries with limited capabilities but with high intent to create an incident. These assets therefore remain at high risk to a variety of hazards both during peace and wartime.

3.3 Sensitivity Based Classification of Assets

3.3.1 Risk Sensitivity Based Classification

Based on the assessed risk and TEFs©, assets have been classified into *four* broad categories of *Sensitivity*, to enable provision of the requisite security features and control measures corresponding to the Risk they are exposed to. This method of classification further helps in identifying assets of similar risk sensitivity and while planning infrastructure, if feasible, consolidating them in areas/ zones for the provision of defensive layers and defence in depth to the more sensitive areas.

Table 27 below is a consolidation of *two* factors - the Risk scores obtained and the TEFs©. The risk scores obtained of hazards against each critical asset and their frequency, or the number of times a score is rated *Very High*, *High* and so on as appeared against a critical asset has been recorded. The basis of classification of an asset based on risk scores is follows:

(1) If frequency of risk score Very High is 10 or more, the asset has been categorised with a Very High Sensitivity;

(2) If frequency of risk score Very High and High combined is 20 or more the asset has also been categorised with a Very High Sensitivity due to the overall impact;

(3) If the frequency of risk score Very High and High combined is 18-20 the asset has been categorised with a High Sensitivity;

(4) If the frequency of risk score Very High and High combined is 15-18 the asset has been categorised with a Moderate Sensitivity; and

(5) If the frequency of risk score Very High and High combined is less than 15 the asset has been categorised with a Low Sensitivity.

To take an example, Flood Gates and Control Room both have Very High Sensitivity as their frequency of Very High-risk score recorded is 11 and 10 respectively. At the same time Trained Manpower and Maintenance Personnel which are soft targets have been also classified with Very High Sensitivity as their combined risk scores of Very High and High is 20.

3.3.2 TEF© Sensitivity Based Classification

The available project design and plans have been examined to arrive at TEFs© which have been listed at Table 16 above. The TEFs© impact certain critical assets while they have no bearing on others. TEF© based Sensitivity of an asset depends on the frequency or number of TEFs© affecting a particular asset and the basis of classification is as follows:-

(1) If *three* or more TEFs© affect a particular asset, it has been categorised with a Very High Sensitivity;

(2) If *two* TEFs© affect a particular asset, it has been categorised with a High Sensitivity

(3) If *one* TEF© affects a particular asset, it has been categorised with a Moderate Sensitivity; and

(4) If no TEF© affects a particular asset, it has been categorised with a Low Sensitivity.

For example, four TEFs© are affecting the Flood Gates, thus Sensitivity is Very High, while the Dyke structure Sensitivity has been rated High as there are two TEFs© affecting the same.

3.3.3 Final Sensitivity Based Classification

Based on the two factors of risk and TEFs© the asset Sensitivity classification has been arrived. Although the Dyke Structure, Road and Rail Transportation corridors were assessed as Low in the Risk Sensitivity, however due to High TEF© score, their overall Sensitivity has been upgraded to Moderate. Final classification of major assets based on Sensitivity as per scale affecting each critical asset is tabulated below:-

Table 27: Sensitivity Scores

Critical Asset	No of Risks as per Scale affecting Critical Asset				Asset Sensitivity Based on Risk Category	Asset Sensitivity Based on TEFs	Final Asset Sensitivity
	Very High	High	Moderate	Low			
Dyke (Structure)	6	5	6	9	Low	2	Moderate
Flood Gates/Controls	11	3	7	5	Very High	4	Very High
Abutments	-	2	11	13	Low	-	Low
Control Room	10	8	6	2	Very High	1	Very High
Irrigation Structure	3	5	8	10	Low	-	Low
Road Transportation Corridor	1	10	12	3	Low	2	Moderate
Rail Transportation Corridor	-	8	16	2	Low	2	Moderate
Solar / Wind Farm	-	6	16	4	Low	-	Low
Trained Operation and Maintenance Personnel	7	13	3	3	Very High	1	Very High
Power Transmission and Distribution network	6	7	12	1	Low	-	Low
Maintenance Corridor / Galleries	-	11	11	4	Low	1	Moderate
Machinery Space	8	13	3	2	Very High	1	Very High
Administrative Infra / Complex	3	15	7	1	High	-	High
Storage/ Stacking Yard	1	15	8	2	Moderate	-	Moderate
Project Site Admin Infra	4	15	6	1	High	-	High

3.4 Zoning

Zoning is essential to ensure that protection of critical assets is designed keeping in mind defence in depth, in a layered concept. As a hazard progresses towards a critical asset, it is essential that various elements of the security design effectively contribute towards its mitigation. Every security design needs to take care of security processes, SOPs and not just infrastructure and technology. Zoning helps cater to these in the design process and in incorporating appropriate risk mitigation features.

3.4.1 Criteria for Zone Sensitivity

While creating zones, asset sensitivity, geographic location/ contiguity, operational function and administrative command and control have been taken into consideration. Critical assets along with their risk sensitivity have been clubbed into zones. Analysing the risk sensitivity of assets within each zone allows designating *Zone Sensitivity*. This ensures that there is a balance between overall controls required for a Zone as well as individual controls for a critical asset.

All critical assets of the dyke have been placed as per their Site designation and thereafter keeping in mind the criteria defined above, they have been dived into *three* zones as indicated at Figures 19 and 20 below. Zone sensitivity has been decided based on the number of critical assets in a particular zone and the risk sensitivity of these assets as well as their overall impact on the zone. Based on the above, the under mentioned Zones, along with their critical assets, have been created to assist in the security design process.

3.4.2 Zones

(a) Zone 1

Majority of Critical Assets that have been placed in this zone have been rated with Very High Sensitivity and are mostly geographically co-located for ease of security designing and subsequent management of security.

(1) Flood Gates;
(2) Control Room;
(3) Machinery Spaces;
(4) Trained Manpower; and
(5) Maintenance Corridor.

(b) Zone 2

Critical Assets in this zone have been rated with High Sensitivity and some may be geographically co-located, while others may be located separately once project designs are finalised. With the available information at the time of this study for ease of security designing and subsequent management of security they all have been considered as one Zone. If at a later date it necessitates a new zone needs to be created, the design features of the new zone will remain same as for a zone with High sensitivity.

(1) Master Control Room;
(2) Admin Infra Complex;
(3) Storage Stacking Yard; and
(4) Project Site.

(c) Zone 3

All critical assets in this zone are interrelated with respect to location and functionality and also have similar Moderate sensitivity.

(1) Dyke Structure;
(2) Abutments;
(3) Road/ Rail Corridor; and
(4) Power transmission and Distribution network.

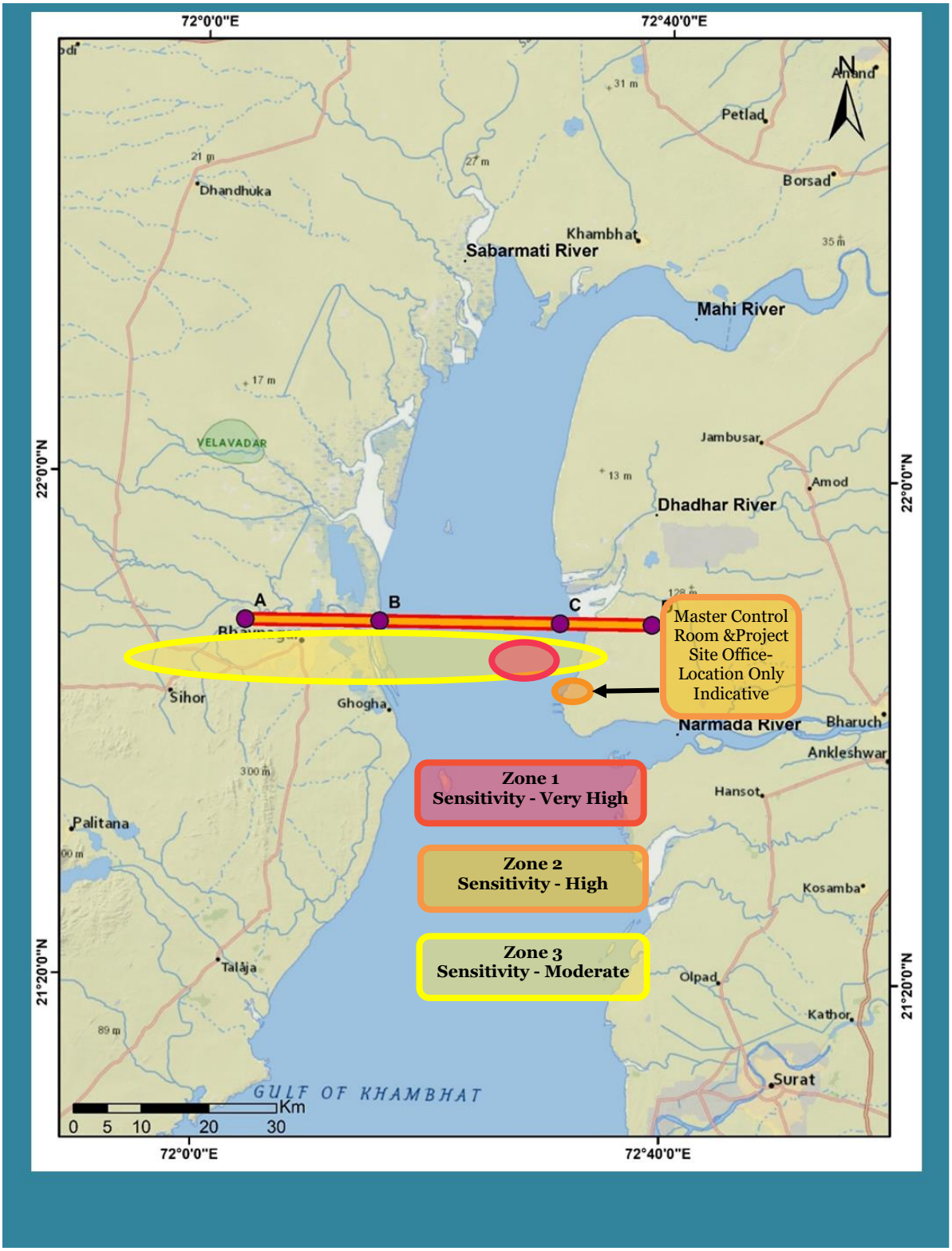


Figure 21: Zones as per Sensitivity

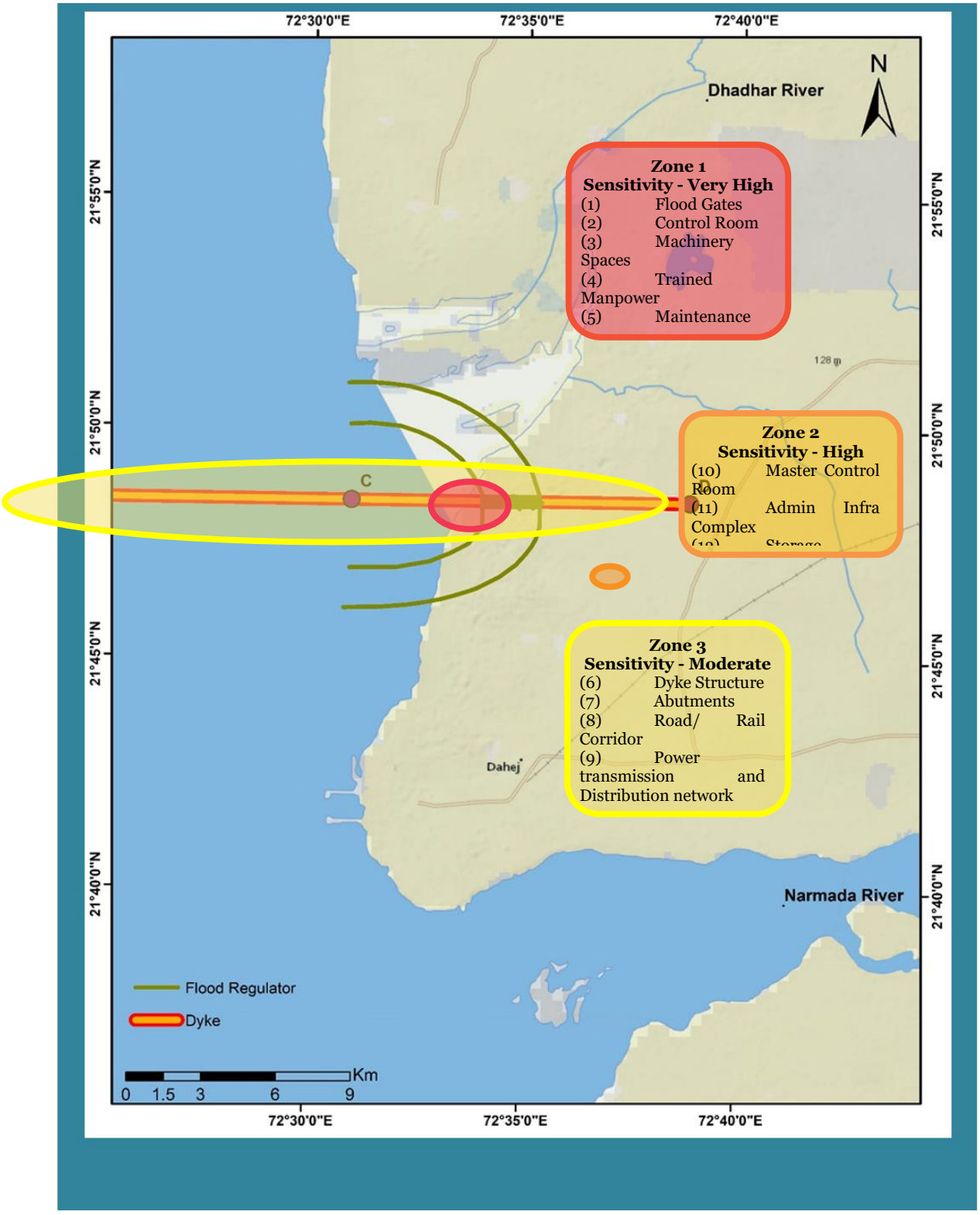


Figure 22: Zones with their Critical Assets

4 Mitigation Plans

4.1 Security Concept Plan

4.1.1 Introduction

The security philosophy of Kalpasar Project is tailored to protect key national assets. Fundamentally, this security is provided through the applications of physical, technological and procedural treatments integrated to operate in unison. This security philosophy of layered treatments provides an integrated system which forms the Kalpasar Dyke Security Design (KDSD).

In the application of the security philosophy, the number and nature of layers is aimed to commensurate the criticality, hazard and overall risk to each vulnerability within the asset. The application of a risk-based approach designed on the criticality and hazard to each vulnerability ensures that security treatments provided are fit for purpose and effectively mitigate the risk to an *'as low as reasonably practicable'* level.

4.1.2 Security Design Principles

The security environment is always very dynamic owing toa variety of factors. Rapid changes in technology, its easy access leading to improvement in adversary capabilities, geopolitical changes impacting adversary intent, critical assets being added over time and other local conditions are some reasons. These drivers collectively contribute to the fluidity of the environment and thus with an understanding of the local conditions and task requirements, it is important to define specific Security Design Principles for a given task. These principles help in tailor making the Security Concept required for the specific task at hand, and guide the future designing process. Based on an expert analysis, site/ plans review and knowledge of security processes, the Security Design Principles essential for designing the security package and KDSD are as mentioned below.

Table 28: Security Design Principles

Security Design Principles	
1	Security measures should commensurate with the Risk
2	There is no such thing as an impenetrable barrier
3	A security system is only as strong as its weakest part
4	Protection in depth with a layered concept
5	Denial as a principle at some stage, for specific critical assets
6	Minimum consequence of system failure through redundancy and contingency plans

7	Security must be designed so that when a breach occurs, it becomes known immediately
8	The time of penetration must be greater than the time of detection plus time of intervention
9	Localization and containment of hazards as per a zone plan
10	Incompatible uses must be appropriately segregated (e.g., operational areas should be separate from administrative)
11	Use appropriate mix of people, processes, infrastructure and technology
12	Optimization of manpower with judicious use of technology

4.1.3 Security Concept Design Basis

The Design Concept for the Kalpasar Dyke is to provide a flexible template that can be used to augment the KDSD by incorporating security treatments or measures to mitigate hazards as they might occur. The intrinsic components of the KDSD must be capable of performing the following ***D6***functions for the system to be comprehensive and effective in the protection of this key asset:

(1) **Deter** intrusion or attack;
(2) **Detect** intrusion or attack;
(3) **Discern** between intrusion or attack;
(4) **Delay** intrusion or attack;
(5) **Deny** intrusion or attack and initiate an appropriate response; and
(6) **Defeat** intrusion or attack by initiating an appropriate response.

The ***D6*** concept identifies the key elements of security. However, a clear common understanding of the meaning of the terms is essential so that planners/ designers/ stakeholders can implement the concept under a common framework without multiple interpretations and disparate design. There are multiple interpretations of the terms by various expert groups, adopting one which is acceptable and recognised by a national government body makes it easier for common acceptance. Centre for the Protection of National Infrastructure (CPNI) is the government authority for protective security advice to the UK national infrastructure. The interpretation of terms below is an adoption of the same as applicable.

(a) Deter

The first line of defence for any project site is physical deterrence, which aims to discourage or deter a prospective enemy by implying that success is unlikely due to strong defences. These preventative measures, which are typically located around a site's perimeter, are useful for giving potential offenders reason to reconsider their actions or a sense of the potential repercussions. Deterrence achieves the following:

(1) Disallows adversary's access to the information and other resources they require to conduct attack planning;
(2) Dissuade adversaries from conducting an attack through emphasis of the likelihood of failure and capture;
(3) Project a sufficiently hostile view of the environment to an adversary so as to make an attack difficult or too unachievable to progress; and
(4) Amplify the effectiveness of security measures and messaging.

Examples of **security deterrents** include:
(1) Watch out for warning signs like "CCTV in operation";
(2) Make sure the CCTV cameras are visible from outside of your boundaries;
(3) Security Lights and motion sensors are important because most robberies take place at night. By lighting your perimeter, you may lower the risk to your site;
(4) Fences could be electric, high, razor wire, revolving spikes, anti-climb paint, barbed wire on top, or covered in dense bramble bushes;
(5) Static guarding along the perimeter of your property may be necessary; and
(6) Gates and access control systems can deter opportunistic robbers by making entry as challenging as feasible.

(b) Detect

It's critical that you have additional defences in place because deterrents won't discourage every possible assailant. It is important to be able to identify, monitor, and react to threats. The security team can start an appropriate reaction to a hazard as early in the attack timeframe as possible thanks to detection techniques that are present both within and outside of a Site. Detection achieves the following:
(1) To identify hazard or attack behaviours at every stage of an attack – planning, reconnaissance, deployment;
(2) Initiate an appropriate response to a hazard or attack as early in the attack timeline as possible; and
(3) Monitor for the loss of information or assets which have been moved off site.

Examples of **detecting techniques** are as follows:
(1) CCTV cameras: Fixed and pan-tilt-zoom models are both highly recommended;
(2) Alarm systems - to notify security personnel of attempts at unauthorised entrance;
(3) Security Lighting: To assist the cameras in detecting motion inside the perimeter; and
(4) To assist teams in determining the location and direction of security breaches, motion sensors, contact sensors, and glass break detectors are important. These include fence-mounted sensors, subsurface movement sensors, and/or passive infrared sensors. microwave beams, infrared beams, etc.).

(c) Discern

In order to initiate appropriate measures towards physical security it is important to know and discern between friend or foe. The value of judging whether measures need to be implemented prevents wastage of effort and resources in the eventuality of false alarms. Discern as a principle this becomes critical to the process and it achieves the following:
(1) Confirm if it is an actual incident or false alarm;
(2) Differentiate between trespassing, an intrusion or an attack; and
(3) Differentiate between authorised and unauthorised entry, movement, presence.

Examples of **techniques to discern** are as follows:
(1) Employing identification tools like biometric access cards, visitor management systems, RFID tags;
(2) Deployment of perimeter flood lights, revolving search lights to improve visual identification; and
(3) Utilisation of drones to identify adversary or decern as a false alarm.

(d) Delay

The next line of defence should be to delay security measures since they extend the amount of time between detection and an attack breaching the perimeter. This is necessary to allow adequate time for the proper response to be activated and deployed and the threat to be neutralised. Delay achieves the following:

(1) Maximising the time between the detection of an attack (at any of the stages in the attack timeline) and an attack reaching an asset's perimeter; and

(2) Limit availability/access to information in order to prevent an adversary developing an optimised attack plan – thereby increasing the attack timeline and further increasing the chances of detection.

Examples **delay tactics** include:

(1) External Physical Barriers - fences, gates, access control, trenches;

(2) Locks and safes are interior physical barriers; and

(3) Barriers to digital security, include access restriction and encrypted passwords.

(e) Deny

The goal of deny is to prevent unauthorized individuals from entering while permitting authorized individuals to pass through. To accomplish this, deny usually employs access control technology or a manned security gate at the entry point. The purpose of undertaking monitoring functions at this level is to offer visual confirmation for the biometric or card access system. Deny achieves the following:

(1) Deny unauthorised access through intended access points; and

(2) Provide an enforceable stand-off to reduce the effectiveness of hazards.

Examples of **detecting techniques** are as follows:

(1) Ground Laid Concertina Barrier closer to the site;

(2) Placing Bollards, Road Blockers, Tyre Shredder, Crash Rated Sliding Gates at entrances; and

(3) In case of airborne challenges placing Counter UAV Systems.

(f) Defeat

Defeat involves response from security staff who aim to catch the offender. This last line of defense frequently involves law enforcement and surveillance is employed to document the capture and evaluate the response's success. Defeat achieves the following:

(1) Determine what external response is required to the range of hazards a site faces and ensure measures are in place to initiate the response.

(2) An effective response counters the anticipated activity of an unauthorised person within a time appropriate to the delay measures.

Examples **defeat tactics** include:

(1) Exercising the plans with external response forces, including communicating with neighbours.

(2) Preparing measures to prevent, resist, or mitigate the impact of an attack or event.

Based on study of the documents, drawings, understanding of the local conditions through a site review and the defined security design principles above, the ***D6*** concept has been evolved. It is essential that such critical assets be protected by the deployed security systems in a manner that they provide defence in depth with denial and defeat at the final stage. An integrated approach combining technology and process is essential to be effective.

Surveillance, intrusion detection, access control with today's analytics capability, supported by sensors, alarms, supporting hardware monitored through a central control room is thus essential. Technology by itself can be effective only up to a certain point and needs to be complemented with sound processes including SOPs, command and control structures, response mechanisms and trained manpower. Though 100% security is a myth, it is essential that all elements form part of the design concept as the absence of any may lead to gaps in the planned security architecture. The ***D6*** Security Design Concept is represented at Figure 21below.

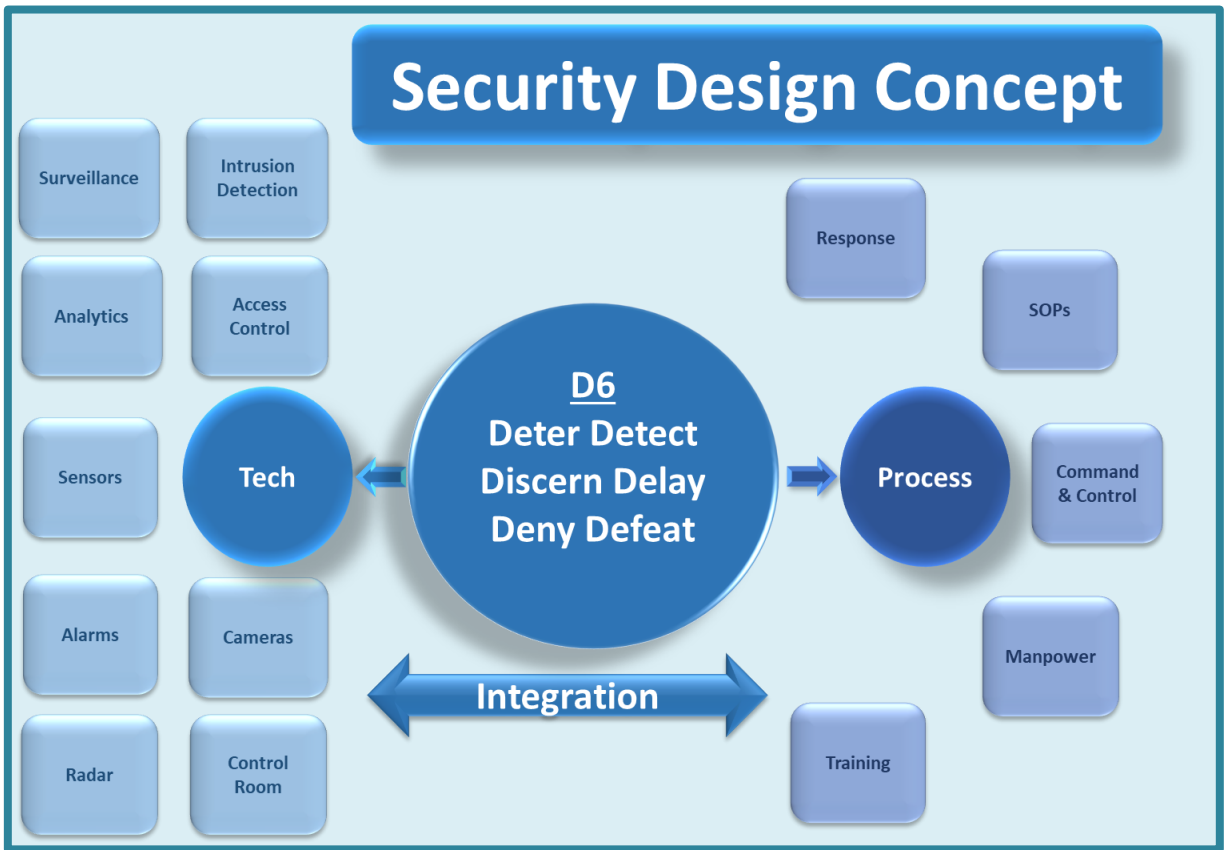


Figure 23: Security Design Concept

4.1.4 Security Layers or Defence in Depth

Another essential idea in physical security is defence-in-depth, which is frequently incorporated into thorough physical protection systems. The concept of selecting a particular control (security measure) at any location follows the philosophy of creating multiple layers of defence around a critical assets or zone. Defence-in-depth, often referred to as layered defence or protection in depth, is based on the use of multiple, solid levels of security measures. A fundamental degree of defence-in-depth is achieved by three general tiers of defence.

(1) **Outer Layer**: The outer perimeter, also known as the outer defensive layer, is made up of perimeter fencing, barriers, protective lighting, intrusion detection systems, surveillance systems and other security tools that are used to prevent, identify, evaluate and delay attacks as well as help in mounting a successful defence;

(2) **Middle Layer**: Building exteriors, doors and locks, windows and utility openings, utility ducts, protective lighting, intrusion detection and surveillance systems, and other comparable security measures are all included in this security layer; and
(3) **Inner Layer**: An attacker who has gotten past the outer and intermediate tiers of defences will be protected by access control systems, intrusion detection systems, protective lighting, and other security measures. Internal hazards may also be protected from by inner layer defences.

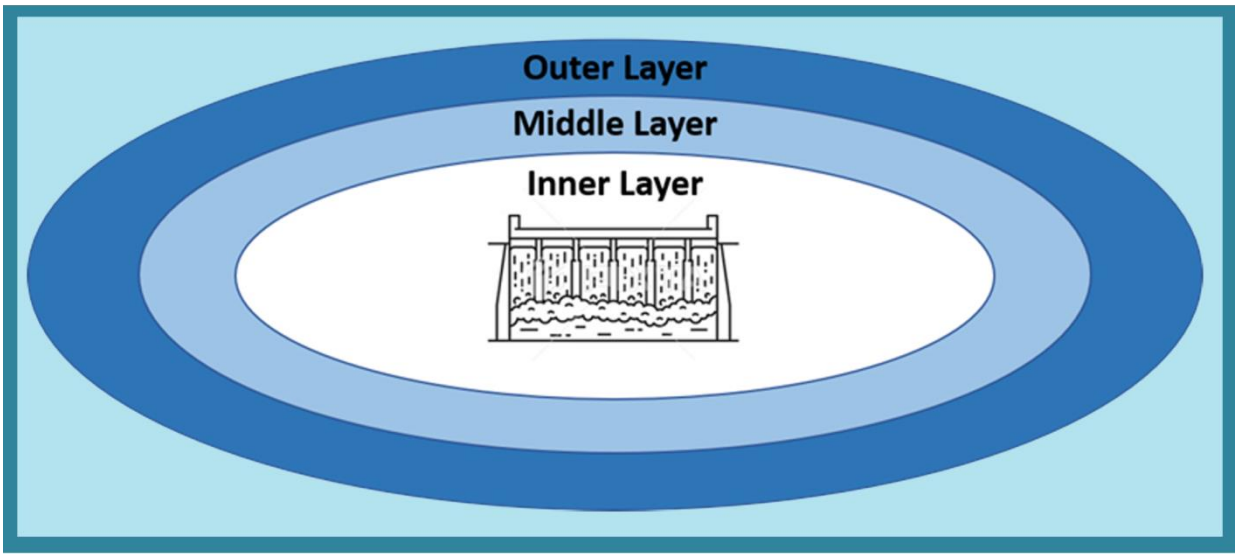


Figure 24 : Security Layers

4.1.5 Macro Level Sub Facility and Security Layers Details

Based on defence in depth, the Macro Level Sub Facility and Security Layer Details of the minimum level of protection as per the D6 concept that ideally should be considered for each sub facility and layer including the type of equipment profile as per the risk-based sensitivity of the area a zone is listed at Table 29 below.

Table 29: Layer Wise Optimal D6 Elements

Risk Sensitivity Rating	Sub Facility	Location	Deter	Detect	Discern	Delay	Deny	Destroy
5-Very High	**(1) Flood Gates (2) Control Room (3) Machinery Spaces (4) Trained Manpower (5) Maintenance Corridor**	**Outer Layer**	Perimeter Wall	Buried Ground Pressure Sensor Cable	Flood Lights	Power Fence Marine Barrier		QRT
			Watch Towers	CCTV System (Thermal/ IP cameras with IR illumination)	Revolving Search Lights			
			View Cutters	Drainage Intrusion Detection System	Water Security Lights			
			LRADS					
		Middle Layer		Fibre Optic Fence Sensor Cable	Biometric Access Control at Entry Points	12' Anti Climb Fence with Concertina Coil above `Y' Beams		
		Inner Layer		Fibre Optic Fence Sensor Cable (As required			Ground Laid Concertina Barrier	Command & Control Centre

Risk Sensitivity Rating	Sub Facility	Location	Deter	Detect	Discern	Delay	Deny	Destroy
				Basis)			12' Anti Climb Fence with Concertina Coil above `Y' Beams (Around C&C Centre/ Sensitive areas)	Mobile Standby Command Post
		Main Entry		Sanitization Zone	VMS		Bollards/ Road Blockers	BP Sentry Post
				UVSS	RFID Tag		Tyre Shredder	
				DFMD	Biometric Access Control		Crash Rated Sliding Gate	
				HHMD				
				Baggage Scanner				
				Full Vehicle Scanner				
				HH Vapour Detector				
		Misc		Micro UAVs			Counter UAV System	PSIM
								Centralised Alarm

Risk Sensitivity Rating	Sub Facility	Location	Deter	Detect	Discern	Delay	Deny	Destroy
								System
								PA System
								SOPs
4-High	**(1) Master Control Room** **(2) Admin Infra Complex** **(3) Storage Stacking Yard** **(4) Project Site**	**Outer Layer**	Perimeter Wall	Buried Ground Pressure Sensor Cable	Flood Lights	Power Fence		Perimeter Road
			Watch Towers	CCTV System (Thermal/ IP cameras with IR illumination)	Revolving Search Lights			QRT
			View Cutters	Drainage Intrusion Detection System	Water Security Lights			
			LRADS					
		Middle Layer		Fibre Optic Fence Sensor Cable	Biometric Access Control at Entry Points	12' Anti Climb Fence with Concertina Coil above `Y' Beams		
		Inner Layer		Fibre Optic Fence Sensor Cable (As required			Ground Laid Concertina Barrier	Command& Control Centre

Risk Sensitivity Rating	Sub Facility	Location	Deter	Detect	Discern	Delay	Deny	Destroy
				Basis)			12' Anti Climb Fence with Concertina Coil above `Y' Beams Around C&C Centre/ Sensitive areas	
		Main Entry		Sanitization Zone	VMS		Bollards/ Road Blockers	BP Sentry Post
				UVSS	RFID Tag		Tyre Shredder	
				DFMD			Crash Rated Sliding Gate	
				HHMD				
				Baggage Scanner				
				Full Vehicle Scanner				
				HH Vapour Detector				
		Misc					Counter UAV System	PSIM
								Centralised Alarm System

Risk Sensitivity Rating	Sub Facility	Location	Deter	Detect	Discern	Delay	Deny	Destroy
								PA System
								SOPs
3-Moderate	**(1) Dyke Structure (2) Abutments (3) Road/ Rail Corridor (4) Power transmission and Distribution network**		Perimeter Wall	OFC based Vibration Detection System	Flood Lights			Perimeter Road
			Concertina Coil on `Y' Beams	CCTV System (Thermal/ IP cameras with IR illumination)	Revolving Search Lights			
			Audio Warning System	Drainage Intrusion Detection System				
		Middle Layer						
		Inner Layer						Command & Control Centre
		Main Entry		Sanitization Zone	VMS		Bollards/ Road Blockers	BP Sentry Post
				UVSS	RFID Tag		Tyre Shredder	
				DFMD			Crash	

Risk Sensitivity Rating	Sub Facility	Location	Deter	Detect	Discern	Delay	Deny	Destroy
				HHMD			Rated Sliding Gate	
				Baggage Scanner				
		Misc.						Control Software
								PA System
								SOPs
2-Low	**(1) Irrigation Structure (2) Solar and Wind Farm**	**Outer Layer**	Perimeter Wall	CCTV System (Thermal/ IP cameras with IR illumination)	Flood Lights			Perimeter Road
			Concertina Coil on `Y' Beams	Drainage Intrusion Detection System	Revolving Search Lights			
			Audio Warning System					
		Middle Layer						SOPs
		Inner Layer						Command & Control Centre
		Main Entry		Sanitization Zone	VMS		Tyre Shredder	BP Sentry Post
				DFMD	RFID Tag		Crash Rated	
				HHMD				

Risk Sensitivity Rating	Sub Facility	Location	Deter	Detect	Discern	Delay	Deny	Destroy
				Baggage Scanner			Sliding Gate	
		Misc.						Control Software

4.1.6 Security Hazard Levels/ States of Readiness

At various given times it is not necessary that the security hazard levels are always the same. They vary based on a variety of conditions and intelligence inputs and thus any security feature which is planned may not always be of optimum functionality. However, it needs to be considered that when a security hazard level is at highest rating the design should have sufficient features, commensurate technologies and procedures that can be implemented if such security hazard demands highest State of Readiness in anticipation of a hazard. It is important to note that the various technologies proposed in the previous section need to be implemented keeping in mind the hazard levels and required State of Readiness. To take an example, heavy vehicles are capable of carrying a large amount of explosive to pose a hazard as a VBIED especially on the flood regulator section, and need to be checked. The same is not feasible on a daily basis, however, in the eventuality of the hazard level and State of Readiness is increased to the highest, sufficient design features, technologies and procedures must be catered for to check such vehicles on the given occasion. Various Security hazard levels which can be considered are as mentioned below.

(1) **Level 1**: The minimum (baseline) level of security at the dyke to protect assets against anticipated incidents and ongoing hazards;

(2) **Level 2**: Enhanced security measures at the dyke in response to information received of a potential hazard that exists to national critical infrastructure, but that is not specific to the Dykes Sector;

(3) **Level 3**: Enhanced response, recovery, or security measures at the dyke where information has been received concerning a potential hazard to State- or local-level critical infrastructure, or when a national hazard to the Dykes Sector is communicated; and

(4) **Level 4**: The highest level of security, response, and recovery measures at the dyke to address a credible, specific hazard communicated directly to the Dyke officials that are specific to a state, local region, sector asset, or entity.

4.2 Project Security Design and Defence Plan

The project security and defence plan evolves from basic conceptual level requirements examined in the previous section. Each Zone has a set of critical assets which need to be protected based on their sensitivity. They all require corresponding levels of protection using technology as per the defined operational requirements. The Kalpasar Dyke Security Design and Defence Plan has been created Zone -Wise for risk and sensitivity-based implementation of technology. This will assist in ensuring that the overall zone sensitivity and commensurate protection / control measures cater for even the low risks, thereby minimising future security gaps and breaches. While Zones will lead the design basis, it is important to also consider that each zone will be impacted by various security components as described below and will greatly influence the security features and technology that needs to be incorporated.

The detailed Security Design and Defence Plan can only be evolved once all the project construction plans are frozen and are ready for implementation, during the PDR stage. However, in the interim to guide planners a broad plan with various components of security, design considerations and technologies, including key mitigation strategies have been articulated in this security DPR. As technologies are likely to evolve over time, the recommendations in this DPR will need to be reviewed at a date closer to project finalization and implementation in order to keep abreast with the technology advancements of the time.

4.2.1 Mitigation Strategies

Prior defining the Project Security Defence Plan Components, it is essential to consider mitigation strategy options that are available based on a detailed analysis of risks, TEFs and its evaluation undertaken in the preceding sections of the study. Mitigation strategies are applicable individually as well as collectively to various critical assets of the project, therefore they have been grouped as per applicability and comments offered as appended below.

(a) Mitigation of Risks - Dyke Structure Including Abutments, Irrigation Structure, Solar/ Wind Farm, Power Transmission and Distribution Network

The core mitigation strategy for the dyke structure and abutments needs to be aimed at achieving deterrence and early detection by way of robust surveillance and monitoring along with preventing hazards from gaining proximity to the structure by denial. These can be achieved by institutionalising procedures complimented with technology. Exclusion Zones, prohibited/ restricted areas, no man's land both marine and land coupled with barrier systems, smart fences, alarms together can achieve the above. The irrigation structures, solar/ wind farms, power transmission and distribution network which are likely to be geographically spread would need independent sensor based early warning systems with the capability of quick response in the event of an incident.

(b) Mitigation of Risks - Flood Gates, Control Rooms, Machinery Spaces, Maintenance Corridor

The critical assets grouped in this section are at highest risk, thus mitigation strategy should aim to first discern between friend and foe and then delay and deny, as far as possible, access to the flood regulator and the flood regulator mechanism. This can be achieved by use of multiple measures deployed together such as manned watchtowers, patrolling by boats, monitoring of the reservoir and seaward side by hi-definition CCTV cameras strategically placed on either side of the carriageway and overlooking the reservoir and the gulf, placement of radars and use of drones etc.

Exclusion zones of 1-2 nautical miles on seaward side and post construction as appropriate on reservoir side should ideally be established. Any boat or craft entering the exclusion zone should immediately be challenged and asked to proceed as per defined SOPs. Security patrols on top of the flood regulator can also augment monitoring efforts. Jetties on the reservoir as well as the gulf side to embark/disembark manpower for conduct of patrols and ensure quick response to defeat hazards will need to be provided for the marine force. Berthing and maintenance facilities also need to be factored to ensure operational functionality of the mitigation strategy.

Peacetime airborne drone hazards need to be mitigated with a robust CUAV solution appropriately designed to function in an integrated manner with the larger air defence plan. Today's unmanned technology in the underwater space needs to be mitigated with underwater diver/ AUV detection systems on the reservoir side around the flood regulator area.

Control Centres and vital machinery can be protected by providing a little spatial separation from the traffic flow. Although data has been worked out for large quantities, it is unlikely that explosives in such large quantities will be deployed, both due to difficulty in sourcing as well as the likelihood of detection. In smaller quantities, the hazardto personnel

will be far lesser while infrastructure would largely be impervious to any effect. The effect will be more of 'Optics' and uneven media coverage.

(c) Mitigation of Risks -Road and Rail Transportation Corridor

The two corridors are meant to reduce the travel distance between Saurashtra and South Gujarat and service a large population. The dyke which otherwise traditionally would have been restricted area, now needs to be open to public and allow the flow of large traffic. The quantum of traffic and mix of cargo and passenger vehicles will necessitate designing controls on the vehicular movement across the dyke. The mitigation strategy needs to be based on the expected hazard Level on a particular day and the availability of design features, technology available to implement the control. Although the vehicles, by themselves, will not pose a hazard to the infrastructure, however, if laden with explosive material and operated by people inimical to national security, they can cause disruptions in the dyke activity. Similarly, freight traffic will need to be monitored for content. This cannot be done on a daily basis, however whenever intelligence indicates a credible specific hazard and has been communicated to the operator, all elements of the D6 concept need to be applied as per design. Towards this a separate checking and sanitisation zone with full body scanners etc. needs to be available and diversion of traffic for checking should be well before entry over the dyke section.

The construction and robustness of the dyke infrastructure will most likely withstand explosions of very high orders but surface damage and temporary disruptions cannot be ruled out. Care will also have to be accorded to the pedestrian walkway since a person with small charges and weapon will have a larger potential to disrupt activity because of greater manoeuvrability coupled with the likelihood of slipping through security gaps. An individual on a 'Lone Wolf Attack' kind of mission or a group of people who arrive separately and congregate on the dyke will be able to inflict casualties, disrupt traffic and even damage to the flood regulator infrastructure and control rooms if they are able to infiltrate and commandeer resources. Robust monitoring of the areas and access control measures to detect and deny as well as mobile jammers to prevent activation of IEDs need to be implemented.

A site-specific security plan needs to be set in place to mitigate vehicle borne hazards. The need for vehicle access control may be necessary and should be addressed in the site security plan.

(d) Mitigation of Risks -Trained Operation and Maintenance Personnel

Trained operation and maintenance manpower remains the softest and weakest area and thus all elements of the D6 security design concept are applicable to create a robust mitigation strategy. The placement of smart technology, including cameras, sensors, alarms, access control devices together itself create sufficient deterrence value for perpetrators to stay away and discard targeting plans.

Well-designed SOPs that lay down methodologies to discern between authorised and unauthorised entries, along with zoning and physical barricades will delay and deny access to inimical elements posing a hazard. Safe rooms can be catered for shelter in case of major incidents.

(e) Mitigation of Risks - Master Control Room, Administrative Infra / Complex, Storage/ Stacking Yard, Project Site Admin Infra

Control Centres and vital machinery can be protected by providing a little spatial separation from the traffic flow. Although explosive impact data has been worked out for large quantities, it is unlikely that explosives in such large quantities will be deployed, both due to difficulty in sourcing as well as the likelihood of detection. In smaller quantities, the hazard to personnel will be far lesser while infrastructure would largely be impervious to any effect. The effect will be more of 'Optics' and uneven media coverage.

(f) Security Manning Strategy

A well established and trained Quick Response Team (QRT) comprising security forces involved with management of security at the facility, who can intervene to defeat hazards in real-time is mandatory. Both marine and landward QRTs need to be suitably equipped with protective gear, ballistic shielded vehicles/ boats, secure communications and robust command and control structures to be effective.

Manpower requirements to cater for the security of the facility need to be worked out in detail once the detail designs have been made and the project is in the pre contract stage. Correct manning which commensurate with the technology/ hardware deployed is mandatory to ensure that systems are optimally exploited and do not remain unused for want of sufficient manpower qualified to technically exploit modern systems. The manning strategy needs to be established basis designation of roles, with uniformed security forces, private contracted security and technical support staff to man and maintain OEM equipment.

4.2.2 Overview of Project Security Defence Plan Components

Keeping in mind the overall risk assessment, evolved security concept, and mitigation strategies a project security defence plan with its components can now be evolved. The security defence plan would emerge keeping in mind various components that need to be looked into along with the individual elements, technologies as per the zones and a layered defence concept. The basic five KDSD components are as tabulated:

Table 30: Security Components

SNo	KDSD Component	Protection from
1	Landward Security	Local and internal land hazards
2	Marine Security	Waterborne surface and subsurface (AUV) hazards, reservoir side
3	Coastal Security	Sea side hazards originating within inland and territorial waters
4	Naval Defence	Seaward, surface and subsurface hazards beyond territorial waters
5	Air Defence	Long range airborne and local UAV hazards

(a) Landward Security

The land-based security systems generally consist of surveillance, monitoring, intrusion detection, entry control, electronic access control, and CCTV observation systems to name a few. Complementing these systems are trained manpower for the management,

control and response to security incidents on the dyke. The area to be protected includes all land sites and the areas adjoining the sites with the area detection systems extending beyond the physical perimeters of the sites. Apart for the security features and equipment that will be catered for as per the project plan, various security forces involved with landward security of the Kalpasar Dyke during peace and war time will additionally need to cater for resources as per their respective operational roles.

Table 31: Landward Security Components

Landward Security Components and D6 Function	Protection from
Perimeter Wall and Fencing *Deter, Delay, Deny*	Unauthorised access, Passive surveillance, Targeted Surveillance, High Power Microwave (HPM), Electro Magnetic Pulse (EMP), Attack on Communications, Theft of Stores and Equipment, Vehicle Borne Improvised Explosive device (VBIED), Personnel Borne Improvised Explosive Device (PBIED), Technical Attack, Disruption to Utilities and Services, Disruption to Fuel Supplies
Perimeter Clear Zones *Detect, Discern, Defeat*	Enable improved Detection and Response capabilities
Compartmentalization of Sensitive Facilities Within Facility *Deter, Delay, Discern*	Unauthorised Access, Theft of Stores and Equipment, PBIED, Technical Attack, Targeted Surveillance
Fence Detection Systems *Deter, Detect*	Assists Perimeter Wall and Fencing to prevent Unauthorised Access
Terrain Following Detection Systems *Deter, Detect*	Assists Perimeter Wall and Fencing to prevent Unauthorised Access
Heavy Vehicle Entry Gate and Search Area *Detect, Discern, Deny*	Unauthorised Access, VBIED, PBIED, Theft of Stores and Equipment
Vehicle Arresting Barriers *Deter, Delay, Deny*	Unauthorised Access, VBIED
Electronic Access Control and Attendance System *Deter, Detect, Discern, Deny*	Unauthorised Access
CCTV Observation System *Deter, Detect, Discern*	Supports Detection Technologies for Discrimination and response to Unauthorised Access
Area Lighting *Deter, Discern, Detect*	Supports Passive and CCTV Surveillance to Deter and Respond to Unauthorised Access
Watchtowers *Deter, Discern, Detect*	Manned and Unmanned Support Passive and CCTV Surveillance to Deter and Respond to Unauthorised Access, direct fire response capability
High Security Alarm System *Deter, Detect, Defeat*	Unauthorised Access, Sabotage, Espionage, Disclosure of Information, Technical Attack, Attack on Communications

Physical Security of Security Control Rooms *Deter, Detect, Delay*	Unauthorised Access, Sabotage, Disclosure of Information, Attack on Communications, Theft of Stores and Equipment
Physical Security of Communication Centre *Deter, Detect, Delay*	Unauthorised Access, Sabotage, Espionage, Disclosure of Information, Technical Attack, Attack on Communications
Mobile Phone Jammers *Defeat*	Activation of remote controlled IEDs
Mobile Phone Detection System for Speech Privacy Areas *Deter, Detect*	Disclosure of Information, Technical Attack
Facility-Wide Security Alert System *Defeat*	Supports Response Function
Dyke Security and Command and Control for Landward and Seaward Systems *Discern, Defeat*	Enables the Effective Coordination of D6 Layers. Note: This system must integrate into the Seaward Defence System
Mobile Ready Reaction Force *Deter, Detect, Discern, Delay, Defeat*	Response Function, Unauthorised Access, Sabotage, Attack on Communications, Theft of Stores and Equipment, VBIED, PBIED, Disruption of Utilities and Services, Disruption to Power Supply, Demonstrations and Blockades, Localised Harassing Fire, Lone Gunman or Sniper, Indirect Fire Area Weapons

(b) Marine Security

The proposed elements of the Marine Security and the primary hazards mitigated against are detailed below. Local security forces involved with marine security including surveillance and patrolling of the Kalpasar dyke reservoir during peace and war time will additionally need to cater for resources as per their respective operational roles.

Table 32: Maritime Security Components

Marine Security Components and D6 Function	Protection from
GIS-Geo Location Enabled Surface Radar *Deter, Detect, Discern*	Surface Vessel Improvised Explosive Device (SVIED), Subsurface Reconnaissance or Asset tagging, Subsurface Attack by Divers (assisted by surface craft), Mining of Marine Channels, Special Forces Surface Reconnaissance or Attack
Surface/Air Surveillance Radar *Deter, Detect, Discern*	Fast Coastal Attack Craft, Surface to Surface Missile Attack, Surface Ship Attack, SVIED, Low Altitude Air Attack, Light Aircraft Delivered IED
Integrated Observation System *Deter, Detect, Discern*	Subsurface Attack by Divers, Mining of Marine Channels, Subsurface Reconnaissance or Asset Tagging, SVIED, Special Forces Surface Reconnaissance or Attack

Subsurface Detection System *Deter, Detect, Discern*	Subsurface reconnaissance or Asset Tagging by Unmanned Vehicles, Subsurface Attack by Divers, Subsurface Attack by Unmanned vehicles, Mining of Marine Channels
Active Anti-Diver Devices *Deter, Deny, Defeat*	Subsurface Attack by Divers, Subsurface Reconnaissance or Asset Tagging
Marine Barrier System *Deter, Detect, Delay, Deny*	Surface vessel Improvised Explosive Device, Subsurface Attack by Divers, Surface Attack by Unmanned vehicles
Reservoir Marine Exclusion Zone *Detect, Delay*	Surface Vessel Improvised Explosive Device, Surface Reconnaissance or Attack
Long Range Acoustic Warning Devices *Deny, Defeat*	Enforcement of Reservoir Marine Exclusion Zone
Marine Response Force *Detect, Delay, Defeat*	Fast Costal Attack Craft, Surface vessel Improvised Explosive Device, Special Forces Surface Reconnaissance or Attack, Enforcement of Reservoir Marine Exclusion Zone
Integrated Command and Control for Marine Defence System *Discern, Defeat*	Enables the effective Coordination of D6 Layers. Note: This system must integrate into the Landward Defence System

(c) Coastal Defence System

The proposed elements of the Coastal Defence System and the primary hazards mitigated against are listed below.

Table 33: Coastal Defence System Components

Coastal Defence Components and D6 Function	Protection from
Sites identified for coastal and air defence radars *Deter, Detect, Discern*	Low altitude air attack, surface to surface missile attack, High altitude air attack, Light Aircraft Delivered IED, SVIED
Sites identified as Close-in Weapon System (CIWS) *Deter, Detect, Discern, Defeat*	Low altitude air attack, surface to surface missile attack, Fast Coastal Attack Craft, Surface ship attack, Light Aircraft Delivered IED, SVIED

(d) Naval Defence Operations

Blue Water Naval operations for the Defence of the Indian West Coast such as, antisubmarine warfare, air and sea patrols, submarine versus submarine operations, surface helicopter patrols, etc are not being considered in this DPR as it is assumed that Indian Navy will institute necessary measures concerning these separately. The likely hazards envisaged can be summarised below.

Table 34: Naval Defence Operation Components

Naval DefenceOperations D6 Function	Protection from
Provides a high-level long-range function of: *Deter, Detect, Discern, Defeat*	Surface ship attack, Low altitude air attack, Surface to air missile attack, Surface to surface missile attack, Subsurface attack by submarine, Fast Coastal Attack Craft, Mining of sea channels, Subsurface attack by unmanned vehicles, SVIED

(e) Air Defence Systems

Indicative, air borne hazards to the Kalpasar dyke are as listed below. The air defence plan as per Indian Air Force for national level critical infrastructure is not being discussed in this DPR as it is assumed that this requirement will be addressed separately by the concerned agencies, if required in coordination with their other sister services. However, suggestions for Counter UAV system requirements during peace time have been articulated at Appendix A.

Table 35: Air Defence Components

Air Defence D6 Function	Protection from
Provides a high-level long-range function of: *Deter, Detect, Discern, Defeat*	High altitude air attack, Low altitude air attack, Surface to air missile attack, Air to Air missile attack, Surface ship attack, Ballistic missile attack, High altitude magnetic pulse

4.2.3 Summary

Towards the above hazards the Armed Forces, Coast Guard, various Paramilitary and Police forces in the region were corresponded with (example of RRU letters sent to stakeholders placed at Appendix B and preliminary interactions were carried out appraising them of the project. During interactions it was suggested that additional assets, resources that may be required for the defence of the Kalpasar Dyke during peace and war time as may be envisaged by them as per their operational role may be catered for by them. It would also be advisable that the National Committee overseeing the preparation of the DPR may separately correspond with these authorities and officially intimate them regarding planning and catering for their envisaged project related security requirements in the coming years.

4.3 Rough Estimation of Master Plan Measures & Application During and Post-Construction

Prior developing the Master Plan and working on measures of the various security elements, technologies and their location and application during and post construction a site visit and discussions with site engineers was undertaken to understand the ground reality**.** Zone wise security measures and their application is described below:

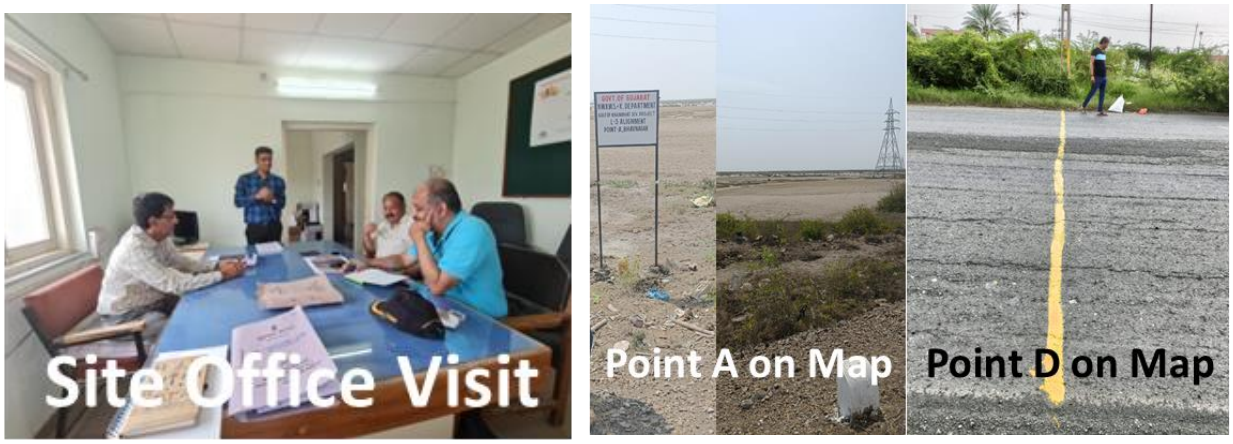


Figure 25 : Site Visit

4.3.1 Zone 1

(a) Security Measures and Application

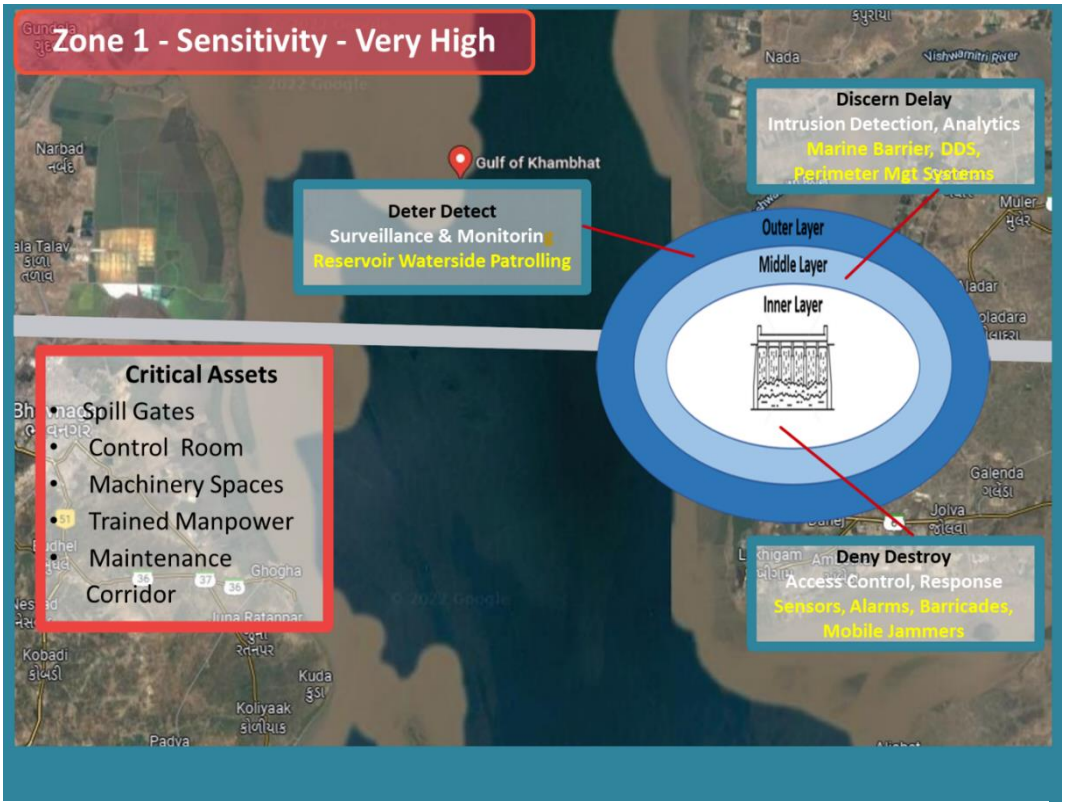


Figure 26 : Zone 1 Measures

(b) Sub Facility and Layer Wise Measures

Table 36: Zone 1 Sub Facility ad Layer Wise Measures

Sub Facility	Layer	Security Measures	Deployment Location
(1) Flood Gates (2) Control Room (3) Machinery Spaces (4) Trained Manpower (5) Maintenance Corridor	**Outer Layer**	Perimeter Wall	Control Rooms, Machinery Spaces and others as applicable.
		Marine Barrier	Reservoir side
		Watch Towers	Dyke reservoir and sea side
		Power Fence	Around Very High Sensitive zones/ areas as applicable eg. control room, machinery spaces etc
		Buried Ground Pressure Sensor Cable	Around Very High Sensitive zones/ areas as applicable eg. control room, machinery spaces etc
		Flood Lights	Across the facility as applicable
		CCTV System (Thermal/ IP cameras with IR Illumination)	Across the facility as applicable
		Revolving Search Lights	Across the facility as applicable
		Water Security Lights	Reservoir and sea side
		View Cutters	On the flood regulator section along road and rail corridor, and as applicable
		Drainage Intrusion Detection System	Entry of stoplog gate reservoir side
		LRADS	On reservoir side/ Patrol Boats
	Middle Layer	Fibre Optic Fence Sensor Cable	Around assets in Very High risk category, control room
		Biometric Access Control at Entry Points	Control room, machinery spaces, adm infra complex, and all areas requiring restricted access
		12' Anti Climb Fence with Concertina Coil above `Y' Beams	Around assets in Very High risk category, control room, storage yards, project site offices
	Inner Layer	Fibre Optic Fence Sensor Cable	Around Command and control Centre/ Sensitive areas

		12' Anti Climb Fence with Concertina Coil above `Y' Beams	Around Command and control Centre/ Sensitive areas
	Main Entry	Sanitization Zone	Separate vehicle checking corridor
		UVSS	Entry of vehicle checking corridor on both ends of the dyke and other entry point of critical assets where vehicles are permitted
		DFMD	Building entrances
		HHMD/ Baggage Scanner	Building entrances
		Full Vehicle Scanner	Entry of vehicle checking corridor on both ends of the dyke
		HH Vapour Detector	Entry of vehicle checking corridor on both ends of the dyke
		VMS	Building entrances
		RFID Tag	Building entrances
		Biometric Access Control	Building and sensitive area entrances
		Bollards/ Road Blockers	Entry of vehicle checking corridor on both ends of the dyke and other entry point of critical assets where vehicles are permitted
		Tyre Shredder	Entry of vehicle checking corridor on both ends of the dyke and other entry point of critical assets where vehicles are permitted
		Crash Rated Sliding Gate	Entry of vehicle checking corridor on both ends of the dyke and other entry point of critical assets where vehicles are permitted
		BP Sentry Post	Across the facility as applicable
	Misc.	Micro UAVs	Located as required for surveillance
		Counter UAV System	On the dyke and other key sensitive areas
		PSIM	Control room
		Centralised Alarm System	Control room and all sensitive locations

4.3.2 Zone 2

(a) Security Measures and Application

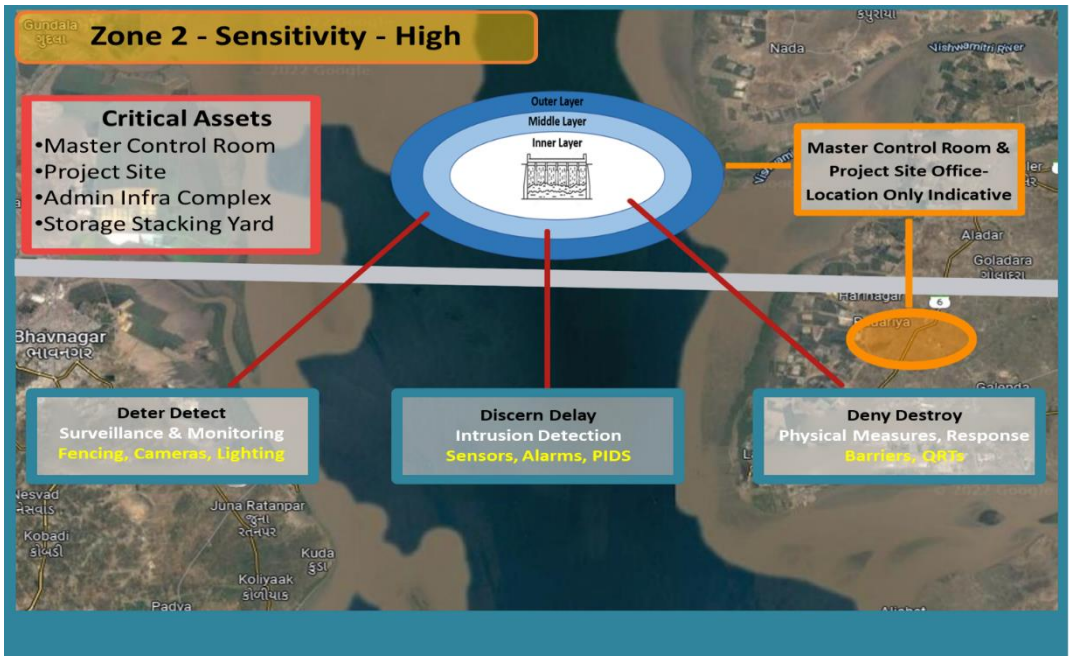


Figure 27 : Zone 2 Measures

(b) Sub Facility and Layer Wise Measures

Table 37: Zone 2 Sub Facility and Layer Wise Measures

Sub Facility	Layer	Security Measures	Deployment Location
(1) Master Control Room (2) Admin Infra Complex (3) Storage Stacking Yard (4) Project Site	**Outer Layer**	Perimeter Wall	Across the facility as applicable
		Watch Towers	Across the facility as applicable
		Buried Ground Pressure Sensor Cable	Around Very High Sensitive zones/ areas as applicable eg. Master Control Room etc
		CCTV System (Thermal/ IP cameras with IR illumination)	Across the facility as applicable
		Flood Lights	Across the facility as applicable
		Revolving Search Lights	Across the facility as applicable
		Power Fence	Across the facility as applicable

		Perimeter Road	Across the facility as applicable
	Middle Layer	Fibre Optic Fence Sensor Cable	Around Master Control Room/ Sensitive areas
		Biometric Access Control	Building and sensitive area entrances
		12' Anti Climb Fence with Concertina Coil above `Y' Beams	Across the facility as applicable
	Inner Layer	Ground Laid Concertina Barrier	Around Master Control Room/ Sensitive areas
		12' Anti Climb Fence with Concertina Coil above `Y' Beams Around C&C Centre/ Sensitive areas	Around Master Control Room/ Sensitive areas
	Main Entry	Sanitization Zone	No mans land around the facility
		UVSS	Entry point where vehicles are permitted in the facility
		DFMD	Building entrances
		HHMD Baggage Scanner	Building entrances
		HH Vapour Detector	Entry point where vehicles are permitted in the facility
		VMS	Building entrances
		RFID Tag	Building entrances
		Biometric Access Control	Building and sensitive area entrances
		Bollards/ Road Blockers	Entry point where vehicles are permitted in the facility
		Tyre Shredder	Entry point where vehicles are permitted in the facility
		Crash Rated Sliding Gate	Entry point where vehicles are permitted in the facility
		BP Sentry Post	Across the facility as applicable
	Misc	Counter UAV System	Master Control room and all sensitive locations
		Centralised Alarm System	Across the facility as applicable
		PA System	Across the facility as applicable

4.3.3 Zone 3

(a) Security Measures and Application

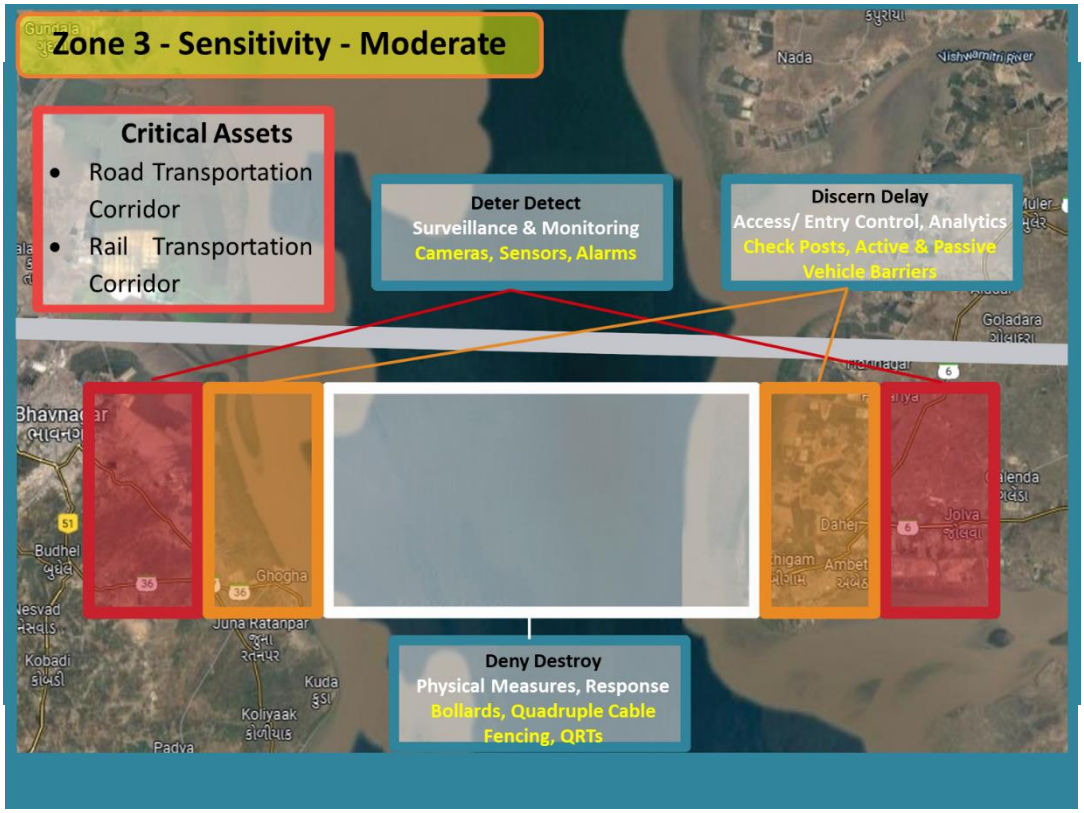


Figure 28 : Zone 3 Dyke Measures

(b) Sub Facility and Layer Wise Measures

Table 38: Zone 3 Sub Facility and Layer Wise Measures

Sub Facility	Layer	Security Measures	Deployment Location
(1) Dyke Structure (2) Abutments (3) Road/ Rail Corridor (4) Power transmission and Distribution network	**Outer Layer**	Concertina Coil on `Y' Beams	Power transmission and Distribution facilities
		Audio Warning System	Across the facility as applicable
		OFC based Vibration Detection System	Power transmission and Distribution facilities
		CCTV System (Thermal/ IP cameras with IR illumination)	Across the facility as applicable

Figure 29 : Zone 3 Transport Corridor Measures

		Flood Lights	Across the facility as applicable
		Revolving Search Lights	Across the facility as applicable
		Perimeter Road	Across the facility as applicable
	Middle Layer	NA	
	Inner Layer	NA	
	Main Entry	Sanitization Zone	Separate vehicle checking corridor
		UVSS	Entry of vehicle checking corridor on both ends of the dyke and other entry point of critical assets where vehicles are permitted
		DFMD	Building entrances
		HHMD	Building entrances
		Baggage Scanner	Building entrances
		VMS	Building entrances
		RFID Tag	Building entrances
		Bollards/ Road Blockers	Building and sensitive area entrances
		Tyre Shredder	Entry of vehicle checking corridor on both ends of the dyke and other entry point of critical assets where vehicles are permitted
		Crash Rated Sliding Gate	Entry of vehicle checking corridor on both ends of the dyke and other entry point of critical assets where vehicles are permitted
		BP Sentry Post	Across the facility as applicable

4.4 Surveillance Strategies

4.4.1 Waterways Surveillance Strategies

Surveillance of waterways is critical for the safety and security of the Dyke. Exploitation of the waterways is highly feasible as it provides relatively easy access to various critical sites of the project. Further, water is not the traditional medium to permanently position or accommodate administrative or security staff, thus monitoring and undertaking surveillance of this space from security perspective becomes essential. In order to achieve domination of the water body adjoining the Kalpasar dyke certain measures that can be put in place are as follows:

(1) Areas of the water body which are close to the structure need to be demarcated and entry prohibited to deny access to intruders. Exclusion zones of 1-2 nautical miles on seaward side and post construction as appropriate on reservoir side should ideally be established;
(2) Waterborne QRTs need to be positioned at suitable points from where they can undertake patrolling, act swiftly in case of incident, and be administered easily;
(3) Electronic systems like sonars, diver detection systems, marine barrier systems need to be integrated with the overall command, control and response mechanism to ensure cohesion of effort;
(4) Sensitization and compliance of the local population to avoid breeching laid down security guidelines while pursuing livelihood related activities will reduce surveillance and monitoring effort;
(5) Utilise the local population operating on the waterbody to be the first line of surveillance and monitoring, as their local knowledge of friend and foe will be most reliable; and
(6) Existing Naval and Coast Guard surveillance and monitoring capabilities need to be integrated to provide early warning to local security teams.

4.4.2 Junction Point Surveillance

Surveillance systems possess the capacity and competence to promptly record occurrences and happenings, activate notifications and warnings, monitor, trace, and avert potential issues before they materialize. Surveillance systems like electronic equipment, software, or hardware that can gather, capture, document, store, manipulate, intercept audio, visual, biometric, or comparable information will be necessary to be deployed at the Junction Points leading to the main transportation corridor passing over the project site as they are the first point of monitoring the transportation corridor. To ensure an effective system the following is necessary.
(1) All Surveillance Systems being deployed for traffic monitoring requirement should to be integrated for security purpose as the CCTVs, Video Incident Detection Systems (VIDS), Automatic Traffic Counter and Classifier (ATCC) etc will feed into the security monitoring system at the control room;
(2) Vehicles should be equipped with a sensing device, which is having the unique identity of the vehicle to enable smooth uninterrupted flow of traffic. Those vehicles that do not have such devices should be segregated to a separate lane;
(3) Every entry and exit points of the junction should be equipped with a transceiver which performs identification of the vehicles and aggregates the information about several inbound and outbound vehicles;
(4) A controller system with specific traffic commands needs to be present in every junction point in order to implement the automated and intelligent traffic management; and
(5) Apart from electronic monitoring, deployment of trained manpower including reactionary teams with mobility will be essential to be placed at the junction points to ensure early detection and mitigation of any eventuality.

4.4.3 Security Measures During Operations

Robust security can be fundamentally achieved through good understanding and training, latest and appropriate electronic systems, and finally correct SoPs and practices. The third element ie. security processes often gets missed and intruders exploit the

situation in the absence of integration of process with technology. Towards that certain essential best practices that should be kept in mind during operations are as listed:

(1) Develop SOPs and check lists for various contingencies and for every stakeholder keeping in mind existing/planned security systems and their planned exploitation;

(2) Develop SOPs for integration of external response agencies and joint handling of situation, including command and control structures at scene of action;

(3) Develop SOPs for localising threat aimed at containment and location wise response mechanisms including lock down procedures in the event of Active Shooter threat;

(4) Ensure perimeter lighting and search lights do not blind the sentries, patrols and other surveillance equipment;

(5) Implement more stringent access control measures in non-technical and residential areas;

(6) Update database of vehicles belonging to the organisation and staff;

(7) Verification of antecedents of all personnel employed by various contractors, especially those have access to sensitive areas;

(8) All common areas such as maintenance corridors should be kept locked and after hours, access should be strictly controlled. Key offices should be checked periodically after hours;

(9) Develop counter intelligence capability in conjunction with local police to monitor activities in adjoining localities; and

(10) Establish Controls by integrating locals from populated areas in the neighbourhood to report unidentified/ unlawful movements/ activities aimed at `neighbourhood watch'.

4.5 Technology Solutions

Security Technology Solutions come in a wide variety of forms and types for different applications and it is important to establish their necessity and relevance prior committing expenditure. Technology should be deployed to support mitigation of gaps, weak areas and critical sensitive points in a facility. Technology by itself is not the answer or the solution. It needs to be integrated with the facility design and plan, along with the security processes and SOPs, to be relevant. Identification of the right technology is an important part of the final solution and should be formalised at the stage when final project designs have been prepared. In this way the most suitable technology available at that time to meet the correct design requirement will get incorporated and prevent wasteful expenditure. Further, since technology is continuously advancing, requirements should be frozen at the time of detailed designing and project implementation stage. Accordingly, this section list only indicative technology solutions that can be incorporated, while detailed identification of the same needs to be a subsequent project activity.

4.5.1 Landward Security

Without sufficient surveillance, intruders with malicious intent can cause significant damage to national assets. Security therefore requires an elevated and comprehensive land surveillance system that is efficient and affordable, offers continuous, wide-area observation and delivers target information quickly and reliably. Comprehensive land-based security systems consist of entry control, electronic access control, time of attendance and CCTV observation systems.

(a) Perimeter Walls and Fences

Perimeter walls and fencing should be maintained to define property boundaries, prevent encroachment and deny passive and targeted surveillance of assets. Security walls are the first line of defence to prevent trespassing, theft, vandalism, and assault. Security walls and fences can also protect against High Power Microwave (HPM), Electro Magnetic Pulse (EMP), attack on communications, Vehicle Borne Improvised Explosive Device (VBIED), Personnel Borne Improvised Explosive Device (PBIED), Technical Attack, Disruption to Utilities and Services, Disruption to Supplies. Security fences can be made from a variety of materials, including chain link, wrought iron, concrete and precast concrete and can be of different types based on their purpose.

Fencing is generally used for the protection of assets within the boundary wall in areas which are not accessible by the public or of complex terrain not suitable for masonry wall construction. Fence heights are measured from the attack side of the fence or wall which generally is the side is facing away from the asset. Both walls and fences can be fitted with detection systems to detect breach of the defined line.

Type A: Masonry Wall

Type B: Masonry wall with razor wire topper

Type C: Masonry wall with Power Fence topper

Type D: Power fence

Type E: Chain link fence

Type F: Chain link fence with razor wire topper

Type G: Chain link fence with Fence Detection System and razor wire topper

(b) Storm water drainage

Storm water drainage across compound walls need to be provided with openings at the bottom to allow storm water to pass from one side of the wall to the other. Barred grills are to be used to secure openings to ensure they provide the same level of security as the wall or fence structure.

Storm Water Drains

(c) Perimeter Clear Zones

Walls and fences require a clear zone to be established on both sides so that they remain free from vegetation (this will require clearing of trees), are accessible for inspection and maintenance, provide clear lines of observation and enable security patrols. In locations on the

property line where clear zones cannot be maintained on both sides external patrolling by the security force should be maintained.

Perimeter Clear Zones:
General clear zones should be applied to all perimeter fences and walls and all internal security fences where practicable. Further compartmentalisation of areas within Sites is required to restrict access to assets and functional areas.

(d) Terrain Following Detection Systems

Terrain-following detection systems are recommended for the detection of intrusion onto site and internal perimeters. Terrain-following detection systems are designed to initiate an alert which is either visually discriminated by an operator through the observation system or responded to by the response force.

Terrain Following Detection Systems

(e) Entry Gates

The purpose of entry gates and vehicle search areas is the containment of vehicles whilst they are searched prior to entering and exiting the Dyke Maintenance Areas, personnel screening and entry administration. Entry gates have been categorised into 5 types for ease of classification. Each gate shall be designed to meet the needs and requirements of its purpose.

Type 1 Gates

Type 1 gates are main entry gates which will be continuously manned and are the primary entry point for personnel and light vehicles through the perimeter. Type 1 gates include: electronic access control points, boom gates, vehicle arresting barriers, security check facilities, pass issue and search facilities, a security office and guard force amenities for a security section.

Type 1-HV Gates

Type 1-HV gates are Type 1 gates with Heavy Vehicle marshalling, handling and search facilities (VOS), electronic access control points, boom gates, vehicle arresting barriers, security check facilities, pass issue, security office and guard force amenities for a security section.

Type 2 Gates

Type 2 gates are secondary entry gates which will be continuously manned and are the secondary entry points through for personnel and light vehicles on to the Dyke Maintenance Areas. Type 2 gates are also located on selected internal perimeters. Type 2 gates include: electronic access control points, boom gates, vehicle arresting barriers, security check facilities, search facilities, a security office and guard force amenities for up to 3 guards.

Type 3 Gates

Type 3 gates are internal perimeter entry gates which are manned either continuously or during hours of site operation and are the primary entry point for personnel and vehicles through internal perimeters. Type 3 gates include: electronic access control points, boom gates, security check facilities and guard force amenities for up to 3 guards. These gates include secondary security gates which can be closed outside of operational hours and at times of heightened hazard levels. These gates can be fitted with detections systems to compliment systems on adjoining fences and walls.

Type 4 Gates

Type 4 gates are internal movement gates which are manned during hours of site operation and are points for internal movement control for personnel and vehicles through internal perimeters. Type 4 gates include: a guard post for up to 3 guards with optional electronic access control. These gates can be closed outside of operational hours and at times of heightened hazard levels. These gates can be fitted with detections systems to compliment systems on adjoining fences and walls.

Type 5 Gates

Type 5 gates are access gates which are normally closed. The gates are used primarily to gain access through fences and detection lines for maintenance and to shorten response times for security forces.

(f) Communications Systems

Security communications systems are fundamental in order to enable security personnel to effectively communicate with their teams in the field and respond to a hazard.

Security Communications

(g) Electronic Access Control and Attendance System

The purpose of the Electronic Access Control System (EACS) is to provide an automated credential base system for the management of access onto and within the Dyke Maintenance Areas.

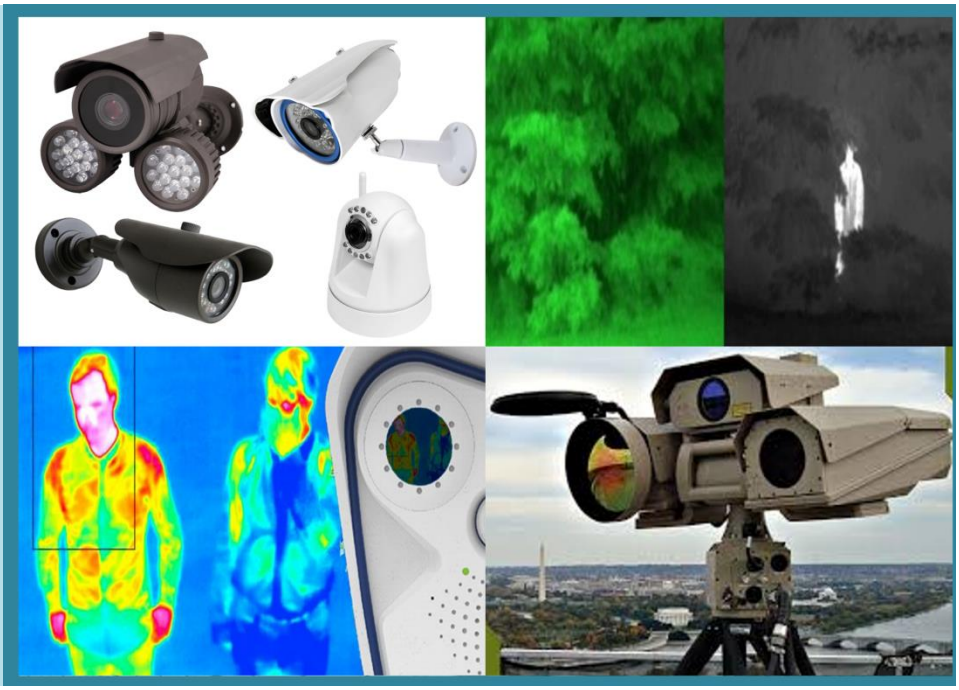
Electrnic Access Control Systems

(h) CCTV Observation System

CCTV observation system should provide surveillance of critical areas through enhancements such as; low light capability, the use of Video Motion Detection (VMD), detection device activation alerts, Access Control System event recording and number plate recognition. The CCTV surveillance system requires integration into the Dyke Security and Defence System as an observation and surveillance system capable of responding to location data provided by detection devices as a key detection and response management tool. Infra-Red (IR) laser illuminated active system, IR passive Thermal Imagery, low light and High-Definition Mega Pixel systems have be recommended. Further camera geo-fencing capabilities are useful tools.

CCTV surveillance system

CCTV Types



(i) Area Lighting

Area lighting is essential to enhance the effectiveness of targeted, passive and CCTV observation and is required in identified high hazard areas. Area security lighting has varied types for varied requirements which should be considered in the overall dyke security design.

Area Lighting

(j) Watchtowers

Watchtowers are positioned to provide elevated positions to achieve extended Fields of View (FOV) for the observation of the areas extending beyond perimeter walls and to monitor activity in close proximity to the perimeter. Watchtowers are designed so that they can be manned with up to 3 guards, however technology can be positioned in these locations to minimise the manpower requirements during low hazard periods. The technologies installed in watch towers varies from location to location but generally consists of an observations system such as either IR Laser Illuminated, or Low Light CCTV cameras that respond to alarm outputs from detection systems such as Powered Fence Toppers, Fence Detection Systems or In-ground Detection Systems. Long Range Acoustic Warning devices may be located to initiate an audible warning to deter accidental intrusion.

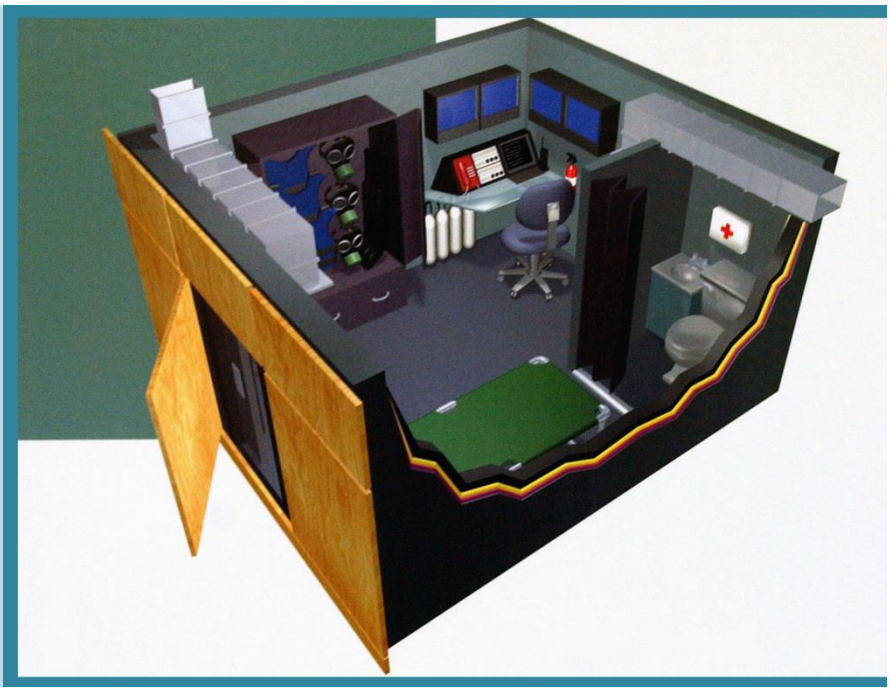
.

Watchtowers

(k) Safe Rooms

Critical spaces with trained manpower require safehouses to take protection against attacks from inimical elements. The idea behind a safe room is to provide limited duration shelter with basic provisions and essentials for personnel to sustain until hazard is neutralised by security forces. Elements of an ideal safehouse vary as per situational requirements.

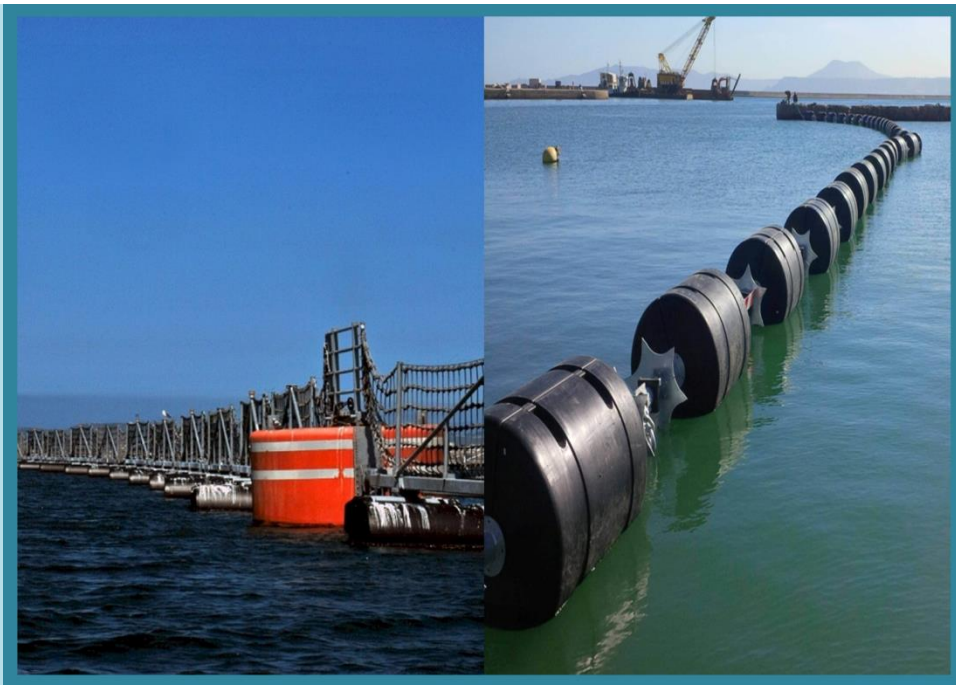
Safe Room



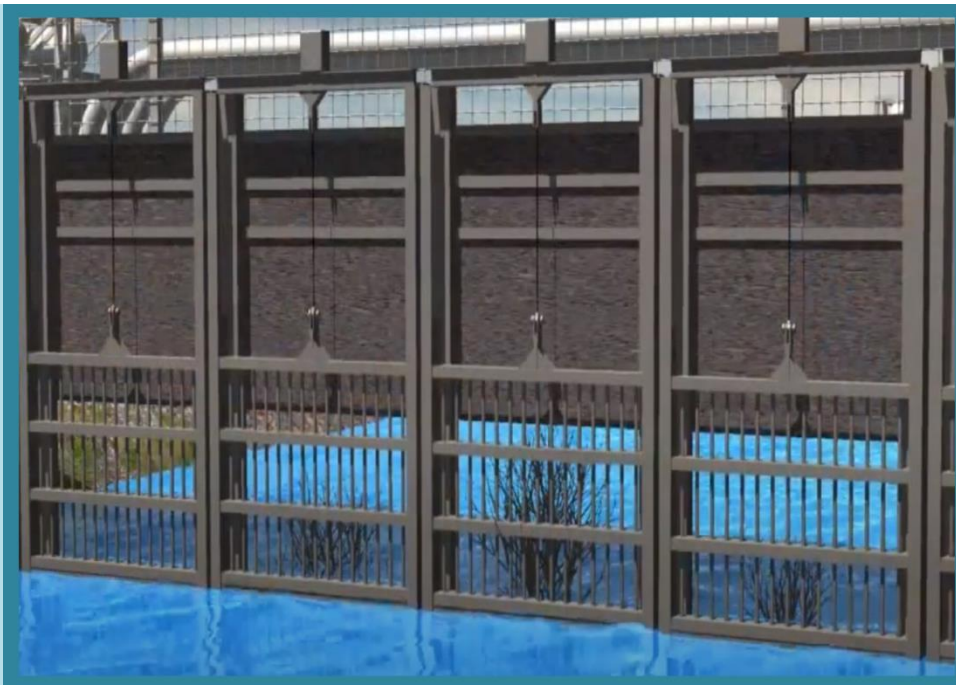
4.5.2 Marine Based Security

Access to vital assets from the reservoir side of the dyke can be restricted by waterway barriers and detection devices. Marine barriers can be categorised into two groups based upon the amount of delay they cause attackers. The first provide minimal delay and need to be paired with rapid detection and mitigation against the intruder. The second are designed to incapacitate an aggressor to such a degree that slower detection is acceptable. Other security systems include Magal Bars to secure underwater openings, Diver Detection Sonar (DDS) and Pneumatic barriers which need to be incorporated into the overall dyke security design.

Marine Barriers



Magal Bars



Intruder Detection Sonar

Diver Detection Units

4.5.3 Air Based Systems

(a) UAV Technologies

UAV systems for surveillance and monitoring with day and night capable cameras are essential. A range of 15-20 kilometres and endurance of 90-120 minutes is recommended.

UAV for Surveillance	

(b) Counter UAV System

A counter UAV system for UAV detection and mitigation is an essential security component for the overall dyke security system. The system should comprise of RF and GNSS detection and identification capabilities. It should have both hard and soft kill measures integrated for real-time neutralization of UAV hazards.

Counter UAV Systems	

4.6 Budget

In line with the D6 security design concept, and the planned layered security configuration for the dyke, as described in the preceding sections there will be a requirement to cater for security systems for flood control mechanism, transportation and maintenance corridors, machinery spaces and other allied infrastructure like office spaces, electrical substations, storage and maintenance yards, security holds, control room etc.

Quantification of numbers of each equipment would evolve at the final design stage at the time plans are frozen prior implementation. The project cost for security would thus emerge accordingly. The list of equipment envisaged for the security of the entire project during and construction and post completion periods is placed at the end of the summary. For the purpose of budgeting approximate costs have been arrived at based on fair assessment of the cost of listed security equipment vis a vis the project cost as enumerate in the succeeding paragraphs.

4.6.1 Capital Expenditure

(a) Physical Measures (Infrastructure) and Surveillance

A large part of infrastructure and equipment in this category would be performing dual functions like road safety monitoring, traffic management etc. Additionally, the numbers required and the technology to be used cannot be frozen at the moment. Therefore, for the purpose of budgeting, an approximate cost of 1.5% (One and a half percent) of the project cost may be budgeted for the security infrastructure and surveillance equipment.

(b) Special Equipment

Special equipment listed above are unique to this project and the quantities can be estimated reasonably. Going by the estimated quantities and the approximate costs a total of INR 200 crore may be budgeted for these equipment.

(c) Allied Equipment

These form part of the project infrastructure and hence may not be catered for separately in the security infrastructure.

(d) Security Manpower

For the provision of security during the construction phase, the responsibility of security is normally with that of the individual contractors. For the purpose of budgeting expenditure by contractors over a five-year period on security manpower, an approximate cost of 1.0 % (one percent) of the contracted amount is estimated based on current manpower costs.

(e) Additional Equipment/ Systems

Any additional equipment/ systems, required by the Army, Indian Navy, Indian Air Force, Indian Coast Guard or CAPF as envisaged by them as per their operational plans for defence of a national level strategic asset would need to be projected and catered for by these organisations as per their budget plans.

4.6.2 Revenue Expenditure

(a) AMC and Maintenance

Revenue expenditure of 10% of the equipment cost may be budgeted per year for operational maintenance of the installed equipment.

(b) Security Manpower

The security manpower would ideally be provided through state forces and revenue expenditure on these would therefore be borne by the state.

5 Conclusion

5.1 Summary

Kalpasar Dyke is a national level strategic asset with large benefits to the nation and its population. Keeping it secure becomes the collective mandate of all stakeholders and towards that first identifying the core principles, concept and design of security becomes imperative. This study has systematically approached developing a security master plan using proven methodologies, for future implementation of security based on the current information available at the time of the study.

An in-depth analysis of the national as well as local environment of Gujarat was undertaken to establish the foundation of this study. Developing a conceptual level security design framework it was felt essential that the local conditions and present day challenges are kept in mind to make it realistic in its outcome. A variety of stakeholders were approached as well as inputs of other studies related to the project were evaluated to arrive at meaningful factors and criteria to drive the study in achieving appropriate conclusions and recommendations.

A detailed and methodical risk assessment using quantification has been undertaken to further develop a security concept and master plan. This has led to making sure that project resources and security budgets are disbursed toward mitigating the right gaps and also expenditures are towards the right technology which is needed and not just procured because it is available. The risk assessment answers the ***Why*** behind the security master plan and design.

As the environment is dynamic, a review would be essential and remain an ongoing process and at every stage of the project implementation. While there are a variety of recommendations that need to be implemented, the recommendations based on the study undertaken are elucidated in the succeeding paragraphs.

5.2 Recommendations

5.2.1 Recommendations for DPR

This study has systematically approached assessing risks and developing a security master plan based on the current information available at the time, and detailed description of the analysis, outcomes and strategies are enunciated in the main document. Major recommendations for successful implementation of security aspects are enumerated below:

(1) The Armed Forces along with the Paramilitary and the Police will play an important role in security of this critical national level infrastructure. Additional assets, resources that may be required for the defence of the Kalpasar project during peace and war time as may

be envisaged by these organisations as per their operational role needs to be catered by them;

(2) Manpower requirements for security will need to be catered for by Central and State security forces, as per their Standard Operating Procedures (SOPs). In addition, private security for manning control room and other security systems along with OEMs security equipment operators, maintainers will be required and revenue budgets for the same needs to be catered for after the design and equipment quantities have been finally frozen;

(3) The security concept and components designed are holistic in nature, however, technology advancements will influence the security design over a period of time. Keeping this in mind a review would be essential to keep pace with technology;

(4) Mitigating security risks is a combination of developing right processes along with technology solutions. The user's or security manager's designated to oversee security of the Kalpasar Dyke should be kept in the decision loop at the time of finalisation, prior implementation;

(5) Cyber threats which form an independent aspect of another study need to be separately addressed to ensure mitigation of project security risks from such threats; and

(6) As the environment is dynamic, assessments will remain an ongoing process and at every stage of the project implementation a review would be essential. The value of the study lies in its correct implementation on ground in letter and spirit during subsequent phases of the project and is recommended that a similar approach of involving domain expertise be continued for the subsequent phases of the project to ensure overall national security objectives of this critical asset.

5.2.2 Recommendations for Final Design Implementation

(a) Recommendation for Infrastructure (Hard)

As the project progresses to and the final design implementation stage there are a variety of issues that would need to be kept in mind. The outcome of this study brings to the fore certain recommendations for consideration. These are enumerated below:

(1) The NIAS social impact study, traffic study, flood regulator design, inputs from engineers at the Kalpasar site need to be continuously updated and integrated the final design prior implementation to ensure any changes or new outcomes are factored correctly;

(2) IB inputs should be obtained during the project implementation phase as well as later;

(3) Counter Drone solutions are required to be deployed in advance to ensure protection from drone threat during construction phase;

(4) Drone should be used for surveillance during the construction phase to fill the gap of permanent security manpower. They would be essential to the process even after implementation phase;

(5) SOPs and processes need to be developed keeping in mind the basic Security concept and master plan articulated in this study;

(6) Access to public at large for transportation needs to be vigorously monitored through surveillance and needs to be in cohesion with the anticipated security situation at the time;

(7) Deterrence needs to be achieved through promulgating exclusion zones, prohibited/restricted areas, both marine and land coupled with smart use of technology like barrier systems, smart fences, alarms placed at suitable points as per the security design;

(8) Exclusion zones of 1-2 nautical miles on seaward side and post construction as appropriate on reservoir side should ideally be established;

(9) Jetties on the reservoir as well as the gulf side to embark/disembark manpower for conduct of patrols and ensure quick response to defeat hazards need to be provided for the marine force;
(10) Control Centres and vital machinery can be protected by providing a spatial separation from the traffic flow;
(11) Safe rooms to be catered for shelter for trained operation and maintenance manpower in case of major incidents;
(12) Cyber threats which form an independent aspect of another study need to be separately addressed to ensure mitigation of project security risks from such threats;
(13) Review of this assessments will be essential at every stage of the project implementation;
(14) Utilisation of domain expertise be continued for the subsequent phases of the project to ensure overall national security objectives of this critical asset; and
(15) Additional assets, resources that may be required for the defence of the Kalpasar project during peace and war time as may be envisaged by the Armed Forces along with the Paramilitary and the Police as per their operational role needs to be catered by them.

(b) Recommendation for Manpower (Soft)

Recommendations related to manpower are enumerated below:
(1) Manpower requirements to cater for the security of the facility need to be worked out in detail once the detail designs have been made and the project is in the pre contract stage;
(2) Manpower requirements for security will need to be catered for by Central and State security forces, as per their Standard Operating Procedures (SOPs);
(3) Private security for manning control room and other security systems along with OEMs security equipment operators, maintainers will be required;
(4) Revenue budgets for manpower costs needs to be catered for after the design and equipment quantities have been finally frozen;
(5) Qualified manpower to technically exploit modern systems in commensuration with the technology/ hardware deployed needs to be made available to ensure that systems are optimally exploited and do not remain unused for want of sufficient staff;
(6) The manning strategy needs to be established basis designation of roles, with uniformed security forces; private contracted security and technical support staff to man and maintain OEM equipment;
(7) A well established and trained Quick Response Team (QRT) comprising security forces involved with management of security at the facility, who can intervene to defeat hazards in real-time needs to be made available both during project implementation stage as well as later; and
(8) Marine and landward QRTs need to be suitably equipped with protective gear, ballistic shielded vehicles/ boats, secure communications and robust command and control structures to be effective.

Rashtriya Raksha University (RRU)

Security and Scientific Technical Research Association (SASTRA)
RashtriyaRaksha University
Phone No: 079-68126800, Ext: 266

Arista Risk and Corporate Solutions
Phone No: 9850520516