tcgdigital

A Comprehensive Approach to **Surveillance of Critical Infrastructure**

May 19, 2023

tcgdigital

CONTENTS

Executive Summary

The protection of critical infrastructure belonging to enterprises or the government is of utmost importance to ensure the safety and security of citizens, the economy, and national security. Surveillance technologies play a critical role in enhancing the security of the critical infrastructure.

This whitepaper examines the use of surveillance technologies in critical infrastructure and provides an overview of the benefits associated with their implementation. Critical infrastructure comprises the vital systems and networks necessary for the proper functioning of society, such as water supplies, transportation systems, and power grids.

The paper highlights the potential threats that critical infrastructure faces, including physical attacks, cyber-attacks, and natural disasters. It also explores the various methods of surveillance that can be used to detect and prevent these threats, such as closed-circuit television (CCTV) cameras, motion sensors, and access control systems. Furthermore, the use of AI and digital transformation paving the pathway for effective surveillance of critical infrastructure is illustrated through vivid examples.

The whitepaper concludes by highlighting the need for continued investment in surveillance technology and infrastructure to ensure the protection of these critical infrastructure. It also encompasses a brief on the importance of a single end-to-end surveillance technology provider.

In a nutshell, it emphasizes the importance of collaboration between government agencies, private companies, and other stakeholders to create a comprehensive and effective surveillance strategy.

The Problem

Security

Security of both data and physical premises is becoming a matter of importance for most organizations in this digital age. The buzzword of “Digital Transformation”, even though at different definitions across people and organizations, has pushed itself into the center-stage of essential actionable activities. Furthermore, the pandemic has pushed people into an off-site mode of operations, thereby accentuating the requirement to ensure security across both digital and physical assets. Additionally, the pandemic has brought out the need to innovate and provide optimized solutions keeping in mind resource restraints.

Infrastructure

Security of both data and physical premises is becoming a matter of importance for most organizations in this digital age. The buzzword of “Digital Transformation”, even though at different definitions across people and organizations, has pushed itself into the center-stage of essential actionable activities. Furthermore, the pandemic has pushed people into an off-site mode of operations, thereby accentuating the requirement to ensure security across both digital and physical assets. Additionally, the pandemic has brought out the need to innovate and provide optimized solutions keeping in mind resource restraints.

Present-day Critical Infrastructure

Enterprises are leveraging digital surveillance to monitor key aspects like:

- Security of their premises and detecting breaches
- Detection of anomalies in their infrastructure
- Identifying potential hazards likely to happen
- Streamlining logistics
- Optimizing energy utilization and reducing the carbon footprint
- Generating early alerts to avert/minimize losses, and so on

Government is leveraging digital surveillance to provide:

- Security of citizens in public places
- Security of key infrastructural assets like Airports, Railway Stations, Government Offices & Buildings, Plants and Power Stations, Courts, and so on
- Protection of human rights at Police Stations
- Monitoring government transportation and optimizing essential services
- Identifying citizen emergencies in public places and expediting remedial actions, and so on

The Solution: Digital Surveillance

The key to successfully deliver digital surveillance lies in the ability to translate the information from end device feeds to identify anomalies and deploy remedial actions to mitigate the risk from the anomalies.

In this, there also lies the challenge. It is imperative for organizations to identify what exactly they need to monitored to meet their objectives for providing security of their critical infrastructure. Once that is done, they would need to prioritize the monitored metrics basis criticality of the breach/anomaly, and list the thresholds that would generate different levels of alerts based on the nature of the issue.

Once that is completed, it is equally important to create the workflows that will translate an alert to an action so that the risk can be mitigated. This usually involves coordination between different systems and departments. Both the technological aspects and administrative coordination become key to providing an end-to-end resolution to the issue on hand.

Digital Surveillance Architecture:

The basic architecture required for any infrastructural digital surveillance set-up includes

- **End devices for monitoring**
  - Cameras (CCTV, Thermal, etc.)
  - IoT Sensors
  - GPS devices
  - Thermal Sensors, etc.

- **Command Center running 24/7 operations**
  - Monitors where Camera feeds are viewed
  - Receive logs of IoT devices & screens monitoring locations from GPS devices on maps
  - Software with AI to analyze feeds from cameras and IoT/GPS devices, etc., and provide inferences as well as reduce 'false positives'
  - Monitor key metrics as may be designed by the specific organization and generate alerts (both physical by observers and system-driven by AI-driven programs) in instances where the set thresholds are breached
  - Provide operational support for coordinating remedial measures across departments/teams

Benefits of Digital Surveillance

There are innumerous use cases that are being deployed across organizations. Technology is being embraced to help deliver these with the sole intention of ensuring real-time information for assessing threats and issues and taking remedial measures in time. Some of the most common applications of digital surveillance are listed below:

Public-place Monitoring:

Monitoring public areas with CCTV Cameras is a common sight across the world. The challenge lies in processing all the images and identifying potential issues in time, every time. Command Centers run 24x7x365 operations to observe all the camera feeds to monitor various aspects like crowding, crime, citizen emergencies like person collapsing or pressing help buttons at public installations, and accidents. Monitoring other aspects also include identifying abandoned objects or suspicious packages left unattended and so on.

Identification Purposes:

In advanced cases, CCTV feeds are also used to identify if any person on a watchlist is noticed in any of the monitored areas. The same can also be used to find missing persons at public venues, e.g. a lost person in a fair or station, etc.

Controlling Access:

Camera feeds can also be used for access control to premises and attendance. During the pandemic, many organizations used feeds from their CCTV cameras to identify violations of mask rules or identify people coughing. Camera feeds along with thermal signatures from thermal sensing cameras were then used to identify persons with fever.

Breach Identification:

Camera feeds along with IoT sensor readings are used at plants, airports, stations, secure premises, etc. to identify breaches.

Performance Monitoring:

IoT sensors to identify anomalies like sensors on key machines giving suboptimal readings of the performance so that remedial maintenance measures are taken up prior to failure.

Asset Maintenance:
IoT sensors along with cameras are used to determine leakage/rust etc. of critical assets in plants – e.g. If the flow of fluids in pipelines is showing less pressure then it implies either leakage or weak supply, etc.

Resource Planning & Inventory Management:
Resource Planning & Inventory Management: IoT sensors identify the utilized capacity of resources to trigger workflows that ensure replacement prior to overflow. Solid waste management/mobile toilets etc. are monitored and appropriate actions are planned basis these insights.

Supply Chain Optimization:
GPS/IoT can also be used to plot the location of public transport/school buses/containers in logistics at ports, etc. so as to optimize their movement and also optimize the supply chain thereof.

Green Digital Transformation:
IOT sensors to measure luminosity, temperature, and pollutants in air/water, etc. for efficient energy utilization (lights and air-conditioning/heating only when certain luminosity/temp levels go below a threshold). Identifying areas of contamination to trigger remedial actions by alerting teams of such situations so they can then do investigations to identify sources and try and reverse the situation. Smart building solutions depend on these for energy optimization and in countries that give credits for carbon footprint reduction, organizations benefit from such initiatives.

There are many use cases being deployed in the current scenario and this is only growing. More and more organizations are embracing digital surveillance solutions to secure their assets. There are many organizations providing solutions in the market as well.

Partner Requisites

Finding the right partner to deploy a solution for digital surveillance is very important as it involves having multiple skill-sets, either in-house or through collaboration from their partner eco-system to deliver an end-to-end digital solution for infrastructural security. The “One neck to hold” theory is of paramount importance as the solution includes multiple-point solutions, which are essential to cater to the ask, and this means managing multiple vendors. Having a partner who will be able to provide all the pieces without compromising on quality and manage the consortium of the point solution vendors while being a single point of contact to the end customer is usually the key to a successful delivery of such solutions.

It is important to note that digital surveillance is a full time on-going project running 24x7x365. Given the trend for organizations to focus on core and outsource everything else is another factor that demands the organizations to ensure the partner selected is able to provide quality service continually. The systems deployed also need to provide both scalability and flexibility to evolve to accommodate the constantly changing environment of threats, flexibility, and growth.

AI is also a key player in this arena as it is the AI engines that rationalize all the feeds to ensure only those actually requiring attention are flagged. Also, AI plays a key role in the face recognition scenarios. Having a strong team with AI experience will become the backbone once the core infrastructure is in place.

As use cases grow, rapidly analyzing the humungous amounts of data from the feeds will become increasingly important to providing timely insights. More complex programs will need to be written to address the needs as more and more information will become relevant to provide meaningful recommendations (e.g. Just the feed from a thermal sensor of a presence in a restricted zone or IOT feed of a breach on a fence may not necessarily be reason to raise an alarm if the breach is by a bird on a restricted fence or in a marked zone.)

Conclusion

The key objective remains for customers to:

- Ensure they clearly identify what they want monitored
- What are the thresholds that define an issue of the monitored object
- Ensure they have the resources/means to address the alerts that are generated to mitigate the risk.

Additionally, the other key aspect for customers is to find the partner who will provide an end-to-end solution, which has a reasonable amount of flexibity to scale and evolve in keeping updated with the changing realities at the customer workplace.

As an industry thought leader, TCG Digital blends deep domain surveillance knowledge with continuous end-to-end technology investment to partner in the real-time protection of critical infrastructure, and ensures smooth functioning. This is achieved by providing a flexible and scalable ecosystem that is future-ready to Engage, Innovate, Accelerate, and Optimize continuously – driving Velocity to Value. For over two decades, TCG Digital has been empowering enterprises worldwide with actionable intelligence through AI and Emerging Technologies, having successfully handled complex projects like the Surveillance of Critical Infrastructure.

Author

Supratik Banerjee
VP - India,TCG Digital

TCG Digital is the flagship data science and technology solutions company of 'The Chatterjee Group' (TCG), a multi-billion dollar conglomerate. We leverage hyper-contemporary technologies and deep domain expertise to engage enterprises with full-spectrum digital transformation initiatives in operational support systems, enterprise mobility, app development and testing, cloud and microservices, automation, security, big data, AI/ML, and advanced analytics.

In addition to our digital transformation practices, by using our end-to-end AI and advanced analytics platform, **tcgmcube**, enterprises are extracting highly actionable insights from their invaluable data assets, and achieving Velocity to Value. **tcgmcube** democratizes data science with scalability, performance, and flexibility. For more information, please visit our website at www.tcgdigital.com