whitepaper

Everything 'critical' secured with STL Sensron+

1. Executive summary

Critical infrastructure systems and facilities are fundamental to driving modern society, providing the necessary basic services that form a foundation for nearly all other activities.

This paper seeks to highlight the effectiveness that can be brought about by infusing technology into security setups around the world. As we proceed, we will look at an overview of critical infrastructure and challenges. We will elaborate on the foundational components of a successful critical infrastructure security strategy. We intend to use this as a "best practice" primer for securing critical infrastructure.

2. Critical infrastructure and why they must be protected

Before we embark on our journey to understand why critical infrastructure needs to be protected, let us try and understand what constitutes critical infrastructure.

Critical infrastructure, by definition, comprises "the assets, and systems", so vital to a nation that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

On a global scale, the following sectors are usually categorised as critical infrastructure

Sector	Critical Infrastructure
Energy	• Nuclear Reactor, Materials, and Waste • Chemical facilities • Oil and Gas pipelines • Off-shore rigs
Information and Communications Technology	• Research and development centres • Data centres • Communication network infrastructure
Manufacturing	• Critical manufacturing units
Defence	• Defence industrial bases • Military camps • Cantonments • Naval establishments • Air force bases • Border areas
Food and Agriculture	• National knowledge research centre • Research centres • Storage facilities
Transportation	• State wide transport networks
Healthcare	• Hospitals • Research and development centres
Government Facilities	• Critical government offices • Water and wastewater management systems • Dams

We live in an age with a significant increase in the number of disasters with natural and/or technological causes, which could have potentially serious consequences for critical infrastructures. Were these infrastructures to fail or be destroyed, the resulting cascade effect could lead to catastrophic damage and affect not only the plants, but also people, the environment and the economy. This rise in the number of disasters over the years is due to industrial and human activity as well as society's sensitivity to major hazardous events. The construction of industrial complexes brings with it stocks of hazardous substances, increased transport infrastructure (road, railways, shipping and pipelines), a rise in population and its concentration, malicious behaviour and human error.

With increasing political uncertainties, terrorist threats and unforeseen infrastructure security breaches, ensuring the safety of critical infrastructure is becoming more and more complex with time.

Although defence may be primarily focused on missions, defence installations, bases, and facilities are also supported by a variety of critical infrastructure and operational technology (OT), from power generation and utilities to building automation and safety systems. A successful attack against defence critical infrastructure can also jeopardise a vital response element to the safety of the entire country. Imagine the plight of our forces that protect our borders and coastlines from infringements, with what terrain they must cover manually to prevent malicious activity from across otherwise porous borders. Similarly in civilian society, incidents of disrupting critical infrastructure can result in loss of power, contaminated drinking water, exposure of confidential information, interruptions to operations, and threats to the safety of personnel. Similarly, critical establishments that run across international borders like air bases, army cantonments, oil pipelines and power stations also need the same level of protection.

3. Resources at our disposal

Human element

Today, security systems across the globe are designed in a way that emphasises the role of human involvement heavily in sensing, surveillance and monitoring. This comes as an additional responsibility to ensuring real-time "response to threat".

Technology

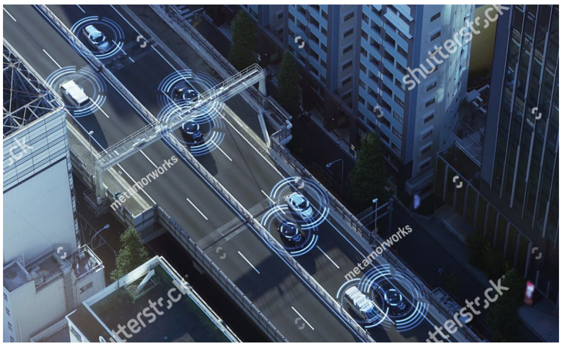
Technology exists, today, as an enabling arm to augment a security system's capability to sense & inspect access-related activities. Technology in security typically takes the form of high-tech products such as sensors, surveillance equipment and action mobilisation centres which are each aimed at performing their specific tasks respectively.

We will now proceed to look some of the interesting products that are enabling technology-enabled security today

Sensing & Surveillance

Fibre optic sensors (FOS) among many other applications, can act as sensors covering long range distances, providing accuracy, and speed while being low on maintenance, which makes them ideal for intrusion detection sensing applications. Moreover, fibre based sensors are small in size and light weight and can be used in harsh environments.

Fibre based physical intrusion detection systems are broadly divided into four categories; speckle pattern, interferometry based, fibre Bragg grating (FBG) based and scattering based.



Fibre PIDS Technique	Max Range (km)	Location accuracy (m)	Cost	Advantages	Limitations/ Dis-advantages	Recommended installations
Speckle Pattern	2	-	Low	Low cost	Small range	Small perimeters
Interferometry	80	± 5 – 10	Low to Medium	Long range	Not cut-immune	Long range fence and buried installations; Drainage monitoring
FBG	2	± 1	Medium	Good location accuracy	Small range; Technology not matured yet	Small to Medium sized perimeters, Drainage monitoring
Scattering Based C-OFDR	80	± 5 – 10	High	Long range	Technology not matured yet	Long range fence and buried installations
Scattering Based C-OTDR	80	± 5 – 10	High	Long range; cut-immune	Large bandwidth and complex processing	Long range fence and buried installations, cut-immune configuration

Microwave sensor

Microwave sensor solution provides high probability of detection, low nuisance alarm rates and resistance to rain, fog, wind, dust, falling snow and temperature extremes. The microwave sensor provides a semi-conical detection area, referred to as a barrier curtain. Microwave security systems tend to be self-contained solutions that stand alone or can be integrated with existing facility and perimeter security systems.

Microwave technology is used as a complement to fence perimeter security such as a fibre sensor mounted to the fence or buried in gravel inside or outside the perimeter. Microwave relays can be tied into new or pre-existing alarm annunciation equipment to trigger incident response measures. Microwave integrated solutions can also support local guard and patrol services that can be notified through an auto-dialer enabled by the alarm output technology.

Sonars

Sonars provide detection, tracking and classification of information on underwater threats that could endanger property and lives. They are developed to provide underwater security for ports, coastal facilities, offshore installations, pipelines and ships. Due to the variety of life and objects that exist under the water, it is desirable that a system be capable of distinguishing between large sea mammals, shoals of fish; a ship's wake; a diver with an open circuit scuba set and a stealth diver with a breather.

Hydrophones

Hydrophones are based on a piezoelectric transducer that generates an electric potential when subjected to a pressure change, such as a sound wave. Some piezoelectric transducers can also serve as a sound projector, but not all have this capability, and some may be destroyed if used in such a manner.

Similar to SONARs, hydrophones are developed to be used underwater for recording or listening to underwater sound. A hydrophone can detect airborne sounds, but will be insensitive because it is designed to match the acoustic impedance of water, a denser fluid than air.

CCTV

CCTV surveillance systems have historically been used as deterrents. CCTV surveillance systems have evolved into a forensic tool — that is, collecting evidence after an event has occurred. become more easily integrated with monitoring devices, alarm systems and access control devices, a third use of CCTV is gaining momentum: Helping security personnel to identify and interrupt security breaches as they're occurring, or even before they take place. Intelligent video algorithms, such as sophisticated motion detection, can identify unusual walking patterns and alert a guard to watch a particular video screen.

Drone

Drone surveillance enables surreptitiously gathering information about a target as captured from a distance or altitude. Drones' flight capabilities, small size and ability to withstand harsh environments mean they can often survey subjects that might not be accessible otherwise

RADAR

RADAR technology for detection can reduce the number of false alarms and increase detection efficiency in conditions with poor visibility. Superior detection abilities in darkness or fog, a motion detector based on radar can be a cost efficient complement to other types of surveillance. Reliability; Minimised false alarm rate; Essential complement to other security tech.

LiDAR

LiDAR bounces out laser beams, measures how long it takes for the light to hit an object or surface, calculating the distance to the object the light just hit and forming data points, called "point clouds" are processed as a 3D visualization in seconds, rendering accurate object displays – all without video surveillance cameras. LiDAR does not dissipate as it travels back to its scanner. LiDAR can be easily affected by fog, rain, or even dust. Light waves have short wave lengths, less than one-millionth of a meter to be exact, meaning they are easily absorbed by water droplets in the air.

4. Is technology alone enough?

The ever-evolving technological landscape we all now live in throws up both benefits and challenges for those tasked with defending our most important utilities. As our means of protection evolve, so do the ways in which they could be vulnerable or used against us. Technology has been a constant factor supporting much of mankind's evolution from time unknown. Over the last decade, there has been a proliferation of destruction and damages to critical infrastructure. With all the incidents that have transpired around the technology that is equipped specifically to handle them, it begs the question 'is technology alone sufficient to ensure complete security of our critical infrastructure?' We will now look at the considerations that make a security system completely lapse-proof.

Piecemeal practices

So far, security setups across the world have largely been commissioned in pockets, often as a response to either a disaster or an intrusion event/attempt. An implementation here or one there is more focused on plugging a particular point of contention rather than an integrated and connected ecosystem. Such practices have resulted in suboptimal designs thereby leaving the door open to lapses in ensuring total awareness and security. One of the biggest challenges in protecting critical infrastructure is ensuring this doesn't make these systems any more vulnerable and that all connections are adequately secured.

Technology alignment

A key aspect of a holistic security system is seamless interactions among its constituent elements. This often presents us with the dilemma of choosing the best technology versus choosing the right technology. More often than not, it is the former that takes precedence. Thus we see an assortment of uncoordinated hi-tech security products, each with its own standard operating procedure and response mechanism making interfacing across the stack an extremely challenging and expensive affair.

Agility

We live in uncertain times and this can often be reflected both industrially and economically. With more and more devices, tools, equipment and now vehicles connecting to each other with the help of the Internet of Things (IoT), would-be attackers can now pick and choose from a plethora of entry points to critical infrastructure systems. Perhaps more important, the dynamic uncertainty due to adaptive predation by external entities makes it extremely difficult to measure the efficiency of any security measure.

Availability

One of the most important properties of any security setup is that it must be up and running 24x7 without rest, ensuring which is a daunting task. Unwavering availability of critical infrastructure is essential to the smooth functioning of each of the critical infrastructure sectors. A case in point would be the defence sector where different systems may be operating in different geographical areas, e.g. shipboard systems out at sea, mobile communications towers active in the field, or power generators operating at a remote firebase. Not only are they vital for the continued day-to-day operations, but losing the support of critical systems, even momentarily, may jeopardise mission success.

Real time reaction capability

A fragmented ecosystem poses another challenge concerning reaction time, something which should be as near real time as possible. Given the evolved nature of disasters and attacks on critical establishments, it is perhaps worthwhile to deliberate the swiftness with which such events are responded to.

“The best time to prepare for tomorrow was yesterday.”

Today’s security systems are, at best, prompted into action through a sequence of information relays involving human intervention and multiple time lapses at each rallying point. Thus, action orchestration ends up being behind right from the start.

Public-Private collaboration

In both public/private and private/private partnerships, the tension between organizational autonomy and the independence of the constituent units of the large-scale system makes communication and coordination critical. Actions in one unit can have unintended and perhaps serious consequences elsewhere. Providing sufficient slack, encouraging constant and clear communications, and creating a consistent belief structure and safety embracing culture help reduce this problem. Large-scale systems need to be flexible in adapting to rapidly changing situations.

5. 5-point formula for enhanced security

The challenge of critical infrastructure protection is a multifaceted one requiring a variety of responses. Market mechanisms and engineering design both have roles, but neither is sufficient. Beyond infrastructure vulnerability assessments, continuity of operations planning, and deliberate investment in a small set of obviously cost-effective technologies, the following structural, organizational, and financial strategies should be considered to improve the capacity of the critical infrastructure service providers and public authorities to perform their functions.

Ecosystem mind-set over technology approach

The need of the hour, as we must have realised by now, is constant vigilance. One of the most future looking ways to achieving this is by conceptualizing solutions from an ecosystem standpoint as opposed to from a purely technology orientation. We must always bear in mind that technology is one of the enabling arms of an ecosystem. Technology alone, in the absence of seamless integration across constituent elements will hardly be effective.

Design-led planning

Following closely on the heels of the ecosystem mind-set is the design aspect, something which is equally essential to ensuring the right mapping between problems and their solutions. Optimal designs equip us with the right choices to lay down a robust security solution that is impervious to the threats it is meant to protect against. Security monitoring and control systems that provide comprehensive and intelligent integration of industry-leading technologies are an important part of any design.

Custom-make and custom-build

Given the wide variety of infrastructure that can be characterised as critical infrastructure, it should not come as a surprise that there can be no ‘on size fits all’ solution. One of the great things about modern advances in both physical and cyber security is that, in certain situations, the same solution can be applied to different industries or circumstances and be just as successful.

Facial recognition in modern surveillance cameras, for example, has multiple uses and roles with a wide variety of sectors. While some technologies may seem to fit on paper, slight differences in operation, management or installation can result in disastrous consequences. As an example, a pipeline transport infrastructure might find much use of pressure and temperature sensors, an establishment such as a parliament building might find video-enabled and light based surveillance equipment. Bespoke requirements will need to be met in order to guarantee the highest levels of protection for critical infrastructure.

Next-generation readiness

Another key factor in determining the efficacy of a security ecosystem is the ease with which new-age technologies such as IoT, Robotics, AI/ML, AR/VR, Blockchain and Bigdata can be integrated. An augmented security ecosystem is able to capture and process information in real-time and provide recommendations on the mobilisation of resources in order to neutralize threats based on their categorisation. The utilities that these new technologies offer not only pave the way for real time reaction to threats but also pre-emptive measures to be put in place which can be used to predict future incidents and plan accordingly.

Layered action orchestration mechanism

In light of the above, an ideal critical infrastructure security solution must be conceptualized & planned holistically and must consist of:

- Command & control centre with computer monitoring, controls and alert notifications
- Alarm processing components with alarm priority coding to aid appropriate decision making
- Sensors with continuous tamper/fault detection, with nuisance alarm discrimination
- High data processing and analysing capability

- Long-range lighting to deter intruders & supports camera image resolution
- Video & camera infrastructure
- Secure digital network to enable real time information exchange between the command centre and other constituent entities
- Action orchestration to ensure timely and appropriate threat response

6. Looking ahead

We believe that integrating cutting edge technology across layers with the variables that constitute the ecosystem is key to ensuring invulnerability of critical infrastructure from threats.

The critical infrastructure protection market size is expected to grow to $150 billion by 2022, at a Compound Annual Growth Rate (CAGR) of 6.8%

during the forecast period. The major growth drivers of the CIP market include the rise in security breaches, stringent government regulations and increasing adoption of best practices, and high investment in smart grid technologies. Emerging countries from the APAC and MEA regions are also poised to offer several untapped and unexplored opportunities in the CIP market.

STL's Sensron+ is a first of its kind end to end solution for critical infrastructure security that leverages the power of hybrid sensing technologies, combined with big data & analytics, and the most advanced command & control centre to deliver a 360^0 situational awareness and an unparalleled "threat-to-response" mechanism. By giving you instantaneous visibility into every bit of coverage, Sensron+ offers you control over who—or what—attempts to access your environment.

As a pioneer and leader in innovative network solutions, STL provides you access to cutting edge technology with unprecedented transparency—simply and cost-effectively. We enable continuous monitoring to detect rogue or unsafe access attempts. And because we believe that collaboration and openness keeps us all safer, we work with other leading security vendors to keep your technology investments intact and your business compliant and secure. Today, STL has partnered with numerous private and government service providers across 100 countries, delivering cutting-edge technology solutions to enhance life experiences as we stand at the threshold of digital revolution.

STL beyond tomorrow

for more details visit www.stl.tech