Security of Key Infrastructures

By: Capt S B Tyagi, COAS'CC, FISM, CSC

What are the Key Infrastructures? Transport, communication and Energy sectors have great role in nation building and economical prosperity. Energy security draws attention of planners and saboteurs world over. Focus is on Energy Security which is core of Key Infrastructures and also very vulnerable.

US has defined the Key Infrastructures as -

> **"Systems and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."**
>
> **- US Patriot Act**

There is no definition of this term but broadly it is defined as

> **"Key infrastructures are those, damage to which will adversely affect Nation's Defense preparedness and Economy. "**

Following are the areas falling in the category of 'Key or Critical Infrastructure –

- Energy infrastructures – nuclear, hydro, coal and gas
- Information & communication infrastructures

- Water resources
- Financial institutions
- Transport infrastructures
- Space – development and research
- Food – supply chain
- Health infrastructures

Because of the private ownership of major elements of critical infrastructure any security and control measures will (almost by definition) require the involvement of both private and public interests. However the national authorities will often have sole competence in the area.

India's Economic Rise & Infrastructure

Best consideration for Indian economical development will require following steps:

- Development of infrastructures to cope with the growing demand;
- Policy for sustainable growth and up-gradation of existing assets.
- Ensuring availability of resources through domestic efforts or through long term supply agreements or through buying assets abroad;
- An elaborate network for easy availability for domestic stakeholders;
- Above all, institutional and policy mechanisms to ensure an equitable usages both in terms of reaching underdeveloped regions and in terms of the economically backward sections of the Indian society.

Major Areas of Security Concerns

The creation of any key-infrastructure is a major logistical operation from locating and investigating new sites to the movement of personnel and establishment of facilities. It takes an enormous amount of resources to establish such sites and all the operators have to rely on a sound cloak of security to prevent theft of equipment, extortion, sabotage and kidnapping of work force. There are following major areas of security concerns –

- Security of survey parties and their equipments (even explosives!)
- Land acquisition and establishing camp sites: Pre-camp: armed / static security
- Security during movement of essential equipments and key personnel
- Travel protection of executive and employees
- Transportation of heavy machinery and raw material - rail, air & sea
- Commencement of construction activities – labor unrest, law-and-order
- Establishing early oil / gas collection centers and security thereof
- Security of off-shore platforms, receiving terminals, dispatch terminals, compressor stations etc.

- Security of larger installations such as refineries, LPG plants and petrochemical complexes
- Security of supply chain – storage / warehouse, rail / road transportation
- Intelligence gathering and disaster planning
- Constitution of Emergency Response Teams

For the Key Infrastructures such as power, oil and gas, security is always a major concern as this sector world over has high probability and vulnerability from terrorist attacks and sabotage. Their operations also have high criticality.

Strategies for Reliable Security of Key Infrastructures

Following are the specifics of the security management of this sector -

Optimizing Assets through Centralized Command & Control

Integrated command and control systems must be positioned to provide an integrated solution, which captures and validates data that can be used throughout the organisation during normal operation, whilst providing relevant, useful information in difficult and emergency situations. This approach will enable operators of critical national infrastructure to optimise their assets whilst maintaining their investment in legacy systems. New developments in technology can improve the security of personnel and assets and provide enhanced operational capabilities.

Biometric Integrated Safe System of Work

Integrated Safe System of Work (ISSoW) is a key tool in ensuring the safe operation of Oil and Gas installations. However, such systems can only be truly effective if user identities can be quickly validated and definitively authenticated. For this to be implemented in practice in providing advanced authentication and identity management, the biometrics based access control solutions are found to be very reliable. There are many solutions available solution where worker identities can be positively and accurately registered, identified and managed securely throughout their lifecycle.

High Accuracy Real Time Personnel & Asset Location

There is need to have a system that improves the safety of workers in hazardous environments and helps to improve the effectiveness of emergency response measures. There are systems available which can locate an individual, or asset, to within 1 meter in 3D (e.g. in a multi-storey/multi-level facility) and it can do this up to 1km from a base station. The system provides a position update every second and, for example, could be used to track a lone worker or road tanker's progress through a plant or ensure that personnel are moving towards the correct muster points in an emergency. Such system do not require large amount of infrastructure or extensive cabling and is therefore easily installed in an existing plant at minimal cost.

Situational Awareness - Securely Integrating Site Data

This aspect deals with the need to simply and securely integrate data from a wide variety of systems to show site leaders and managers the overall condition of their site - and what is happening on it. This capability brings together data from operational, security and work management systems and merges this private data with public information from the internet to provide a complete picture. By using underlying open data architecture together with security protection system, it can bring these data sources together and share them securely among multiple disparate user groups, and at different locations, whilst ensuring data validity, security, and privacy. As well as the complete picture, it can also provide custom views for users such as maintenance teams, emergency services and even the media and general public in the event of a major incident.

Air traffic

Rogue aircraft can endanger the security of any flights in its vicinity of the flight path! Due to loose security controls at the take-off points unscreened passengers can board it with unimaginable explosives and ammunition! Even this is not needed as aircraft in collision path itself is big danger to other aircraft. Security of Aircraft in the future environment therefore must begin with the aim of improving security on commercial aircraft. It must address classic hijacking situations, September 11-type scenarios and futuristic scenarios involving electronic jamming and hacking of computer systems. Additionally it must address technical issues such as onboard-threat detection, threat assessment and response management plus flight protection.

Security of Offshore Platforms

Off-shore platforms are highly vulnerable, high risk installations having high probability of attacks of terrorist which may be equipped with some of the best technical capabilities. Somalian sea-pirates have well demonstrated that now-a-days any one can get any thing provided they have sufficient funds! It is therefore very important that beside sturdy infrastructure security and the security risk management mechanism including airborne, maritime and ground surveillance, these platforms have very reliable and impregnable communication and cyber security measures. Tracking and positioning of manpower and material is equally important.

To devise an action plan to combat attacks on its offshore installations, potential terrorist-related crisis situations should be incorporated in the CMP (Crisis Management Plan) along with the response mechanisms/capacity building required to handle such situations.

The Maritime Sector

The International Ship and Port Facility Security, **ISPS code**, was introduced in July 2004. It requires ports and vessels to show that they have put adequate security systems in place -

and vessels to show that they have been calling only at certified ports. The purpose of the code is to provide a standardized, consistent framework for evaluating risk.

Vessel Automatic Tracking and Monitoring System for the security of large oil infrastructures in high sea areas assume greater importance to rule out attack capabilities of Somalian like outfits which might draw their attention to the vulnerabilities of these assets.

Cyberspace

The EU has set up a task force to explore what its 25 member states are doing to combat cyber-threats against critical infrastructure. As part of the EU's Critical Information Infrastructure Research Coordination, CI2RCO project, the task force aims to identify research groups and programs focused on IT security in critical infrastructures, such as telecommunications networks and power grids. The scope of the cooperation goes beyond the EU; the task force also wants to include USA, Canada, Australia and Russia. India with its strong IT workforce, known world-over for its prowess must join such cooperative and collaborative efforts!

Robust, Secure, Global Communication Solutions

This capability calls for seamlessly connecting all oil & gas installations of an organization and on more higher level , of the Nation by providing highly available, robust, secure, integrated communication networks for critical operational systems. A number of communication solutions are available which provide robust connectivity and communication helpful for protection of assets and personnel in environments where a high standard of inherent safety is a mandatory requirement. There are resilient telecommunications networks such as Broadband Global Area Network (BGAN), which allow for simultaneous voice & data communications and secure access to applications from almost anywhere in the world.

Securing Supervisory Control Systems

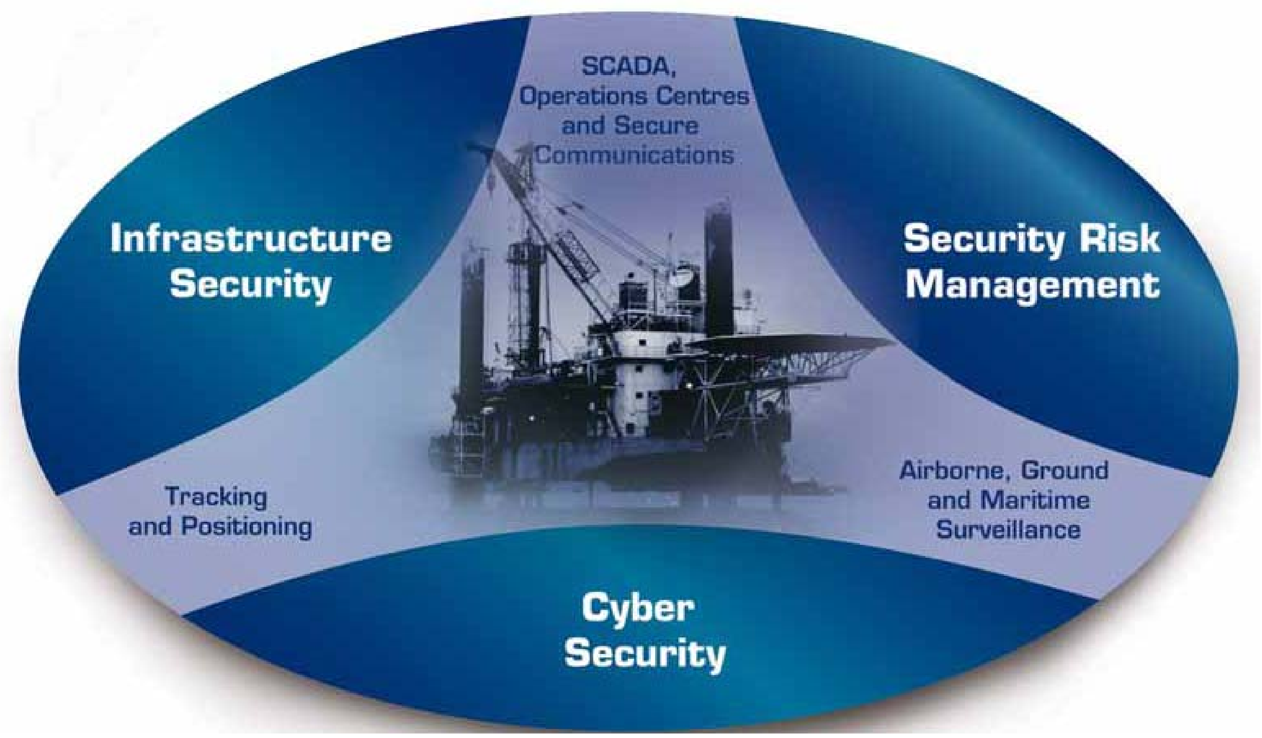
Supervisory Control and Data Acquisition (SCADA) systems and other similar control systems are widely used by utilities and industries that are considered critical to the functioning of countries around the world. The Operations, Safety, Security, and IT decision-makers of Key Infrastructures, specially oil & gas, power generation and transmission and nuclear energy are well advised to pay attention to following aspects –

- More and more reliability on Local Area Network (LAN), Wide Area Network (WAN) and Broadband Global Area Network (BGAN) brings increased threats to operations of organizations using them. Threats to SCADA are Malware, Insider, Hacker and Terrorists.

- The networks are suseptible to attacks aimed to disrupt and destroy them. Such an attack by viruses, worms or other forms of cyber-terrorism on nuclear, oil and gas industry process control networks and related systems could destabilize the national economy and defense preparedness.

- We need to keep control systems safe and secure, and to help minimize the chance that a cyber attack could severely damage or cripple infrastructures. We need to identify ways to reduce cyber vulnerabilities in process control and SCADA (Supervisory Control and Data Acquisition) Systems: to identify new types of security sensors for process control networks.

- There is real threat to SCADA from mischief mongers prowling in the web-world and the tech-savvy terrorist and Stuxnet is the most lethal combination!


SCADA, Operations Centres and Secure Communications
Infrastructure Security
Security Risk Management
Tracking and Positioning
Airborne, Ground and Maritime Surveillance
Cyber Security

Conclusion

While above are the main strategies for securing the assets of key infrastructure, constant improvement and improvisation need to be carried out to make security measures reliable as well as cost effective, as in present phase of economic melt-down no organization will take decision with out working out the ROI (Return on investment).

Dedicated manpower ready to face the disaster would always be central consideration for any security and disaster response plan. To keep them constantly motivated and updated is also another prime responsibility of the Management as otherwise even the best plans are doomed to fail. Only those will succeed in this sector who foresee and fore-plan and rehearse thereafter their security and emergency response plans!