INTEGRATED PROTECTION AND DETECTION

Frank Beyer, ILF Consulting Engineers, Germany, presents a holistic approach to protect critical infrastructure from the threat of danger.

The physical, information and operational security of critical infrastructure is subject to a wide range of threats. A significant increase in attempts to manipulate the related operation technology (OT) systems can be observed. The attacks against a Ukrainian power grid can be taken as an example of what such attempts look like. They are usually a combination of several co-ordinated activities, with the aim not only to provoke maximum damage to a system and to destroy the security of supply, but also to hinder response and recovery/restoration works as long as possible. Another example is the attack against a safety integrated system of a process plant using a tailor-made malware. This shows that not only the basic process control systems, but also the emergency shutdown systems are the subject of dedicated attacks.

Sophisticated attacks often bypass traditional security measures and have the potential to disrupt the production

process, cause spills or product contaminations, destroy process equipment and endanger human life. Isolated technological, administrative or organisational measures cannot stop such attacks. A holistic approach is required to protect assets, detect attacks and restore normal operation.

Such an approach to secure the facilities should cover at least the following aspects:

- Development of an integrated security management system.
- Provision of a robust system design.
- Definition of required physical security measures.
- Development of cyber security measures for information technology/operation technology systems.

The approach starts with an in-depth system evaluation of all assets belonging to the critical infrastructure and the physical, electronic and organisational measures in place or planned to protect these assets. Such a review, in addition to all the technical facets, also includes a verification of related policies, operation and maintenance procedures, administrative procedures, security rules, response plans and recovery procedures, as well as the business continuity plan.

The protection line will only be as strong as the weakest link in the chain. A sophisticated cyber security system would, for instance, be useless if clear access regulation to the critical infrastructure is not in place.

An up-to-date asset inventory and a complete system documentation are prerequisites for a risk assessment and the definition of required security measures. If no (up-to-date) asset inventory or system documentation exist, a dedicated internal project may be required to implement an asset inventory system and to update all relevant documents. If not yet available in digital format, this should be ideally combined with a document digitalisation project.

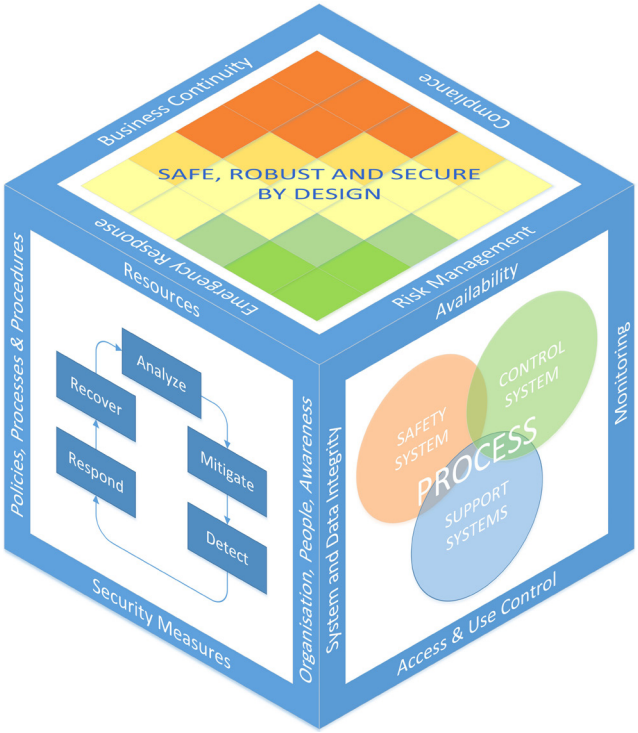

Figure 1. Aspects of a holistic approach.

Usually all political, environmental, socio-cultural, technical and economic risks are part of a safety risk assessment, for example: quantitative risk assessment (QRA), hazard identification (HAZID) studies and hazard and operability (HAZOP) studies, as well as security incident reports.

In light of protection of critical infrastructure, it is necessary to amend these standard approaches in order to tackle physical and cyber-physical attacks against it. Known attack goals, techniques, their impact on security and safety, as well as the probability of detecting the attack, should be considered in an attack-tree as a guideline for the system design. In particular, politically motivated and state supported attacks are often characterised by the availability of significant financial and human resources to cause substantial damage to a critical infrastructure.

It should be noted that the approach to protect critical infrastructure has to cover not only the operation period but also has to include all project phases, starting from first feasibility studies through to front-end engineering design (FEED), implementation and commissioning.

The approach shall be supported by a security master plan that addresses corporate social responsibility; co-operation with the intelligence community; risk and hazard management; and response planning (including public security forces). In addition, the master plan must consider the implementation of security measures that allow for detection of threats and the co-ordination of responses in time, disaster recovery and business continuity planning, as well as the training of all involved parties to assure a secure operation.

Integrated security management system

A security management system has to be implemented to co-ordinate all components, internal processes and all aspects of corporate security.

An integrated approach is required to manage the related risks, resources, policies, procedures, performance reviews, the continuous improvement process and interfaces with other (management) processes:

- Definition of roles and responsibilities, location, and technical installations to be covered.
- Definition of expectations, goals and frame conditions, integration with existing security systems and elements.
- Definition of scope and area of application, physical/technical as well as cyber security.
- Definition of policies, procedures, measures and work instructions.

- Performance review and continuous improvement.
- Training of employees, contractors, etc.

By conducting a business impact analysis, an alignment of the security management system with emergency response plans and business continuity plans has to be developed:

- Identify business- and safety-critical processes.
- Define priorities for system and data recovery.
- Identify resources required to operate a specific system/provide a specific service.
- Define minimum requirements for emergency operation.
- Select the most suitable response strategy.
- Define processes and technologies that a computer emergency response team can use to identify, categorise, investigate and remediate adverse security events.
- Document procedures, plans, measures, etc.
- Prepare test and training plans.

As a result, an integrated security management system will be developed and will come into force for the entire lifecycle of the critical infrastructure.

Robust system design

A safe and robust system design is key for certain resilience of the critical infrastructure against a wide range of threats. The review of an existing design, or the development of a new design, mainly relates to the:

- Geographical area/corridor and the relevant separation distances/zones and evaluated environmental impacts.

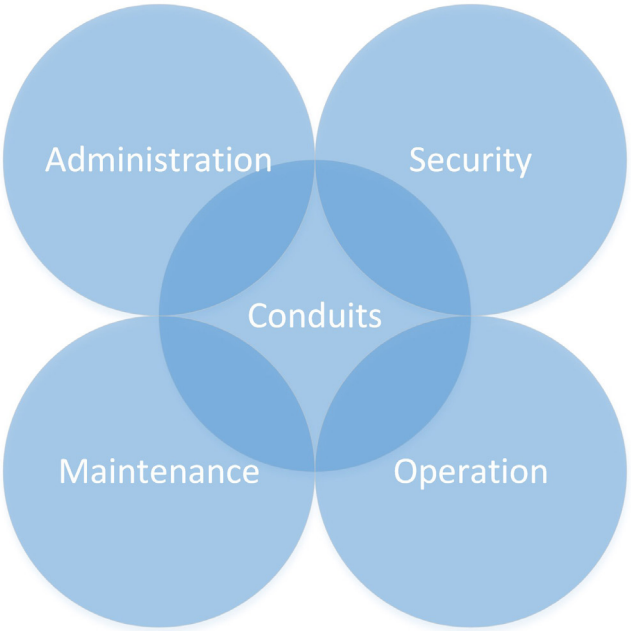

Figure 2. Security management system.

- Location of/distances between all facilities and achievable response times.
- All relevant protection systems, e.g. relief systems, fire and gas detection systems, firefighting systems.
- Alarm management system.
- Emergency response/recovery/fall-back strategies.

For the development of a robust system design it will be necessary to enhance the standard design guidelines by adding the following engineering guidelines:

- Defence in depth.
- Simplicity over flexibility.
- Redundancy, diversity and contingencies.
- Implementation principles.
- Secure supply chain.
- Staff security.
- Test requirements for the physical/cyber security systems, as part of the security management system.
- Configuration and operation principles, principle of least privilege, monitor systems and networks, response/recovery/fall-back definitions.

In light of the ever-growing risk of cyber and cyber-physical attacks, special attention shall be paid to the design of industrial control systems and safety instrumented systems, including associated networks.

Physical security measures

The physical security of critical infrastructure is a prerequisite for protecting it against various threats. Based on the results of the system evaluation and the risk and hazard assessments, it might be required to implement protective structures, third-party intervention, access control and intrusion detection systems. These systems shall be designed to ensure that all aspects – including the requirements of the response teams – are properly considered in the physical design. Additional technical security systems (like video surveillance systems) shall be designed and implemented as another measure to support the overall security concept.

By using distributed fibre optic sensing systems for third-party interference (TPI) detection, even the entire pipeline corridors can be covered. The TPI detection system informs the operator and the security team about any relevant event and indicates the location on a map (e.g. based on GIS data) with an accuracy of a few meters.

Cyber security measures for IT and OT systems

A cyberattack will try to use any vulnerabilities in the OT system, as well as in the communication and IT systems,

to manipulate process and safety components in order to disrupt the operation process or destroy equipment.

Attack goals, well known from the common office environment (IT system) are extended by further items related to the OT equipment. The possibility of an injection of malicious code, already on firmware level or with the shared library used for the compiling of the machine code, must be eliminated. A possible sending of fake sensor data or process control commands to controllers and OT applications, or a decalibration of sensors, need to be excluded. The protection of OT against tampering, unauthorised reconfiguration or disabling must be ensured.

Servers and workstations within control systems run standard operating systems like Windows or Linux. Normally these common operating systems have standard security programmes and services like host based/ built-in firewalls. However, manufacturers of control systems and applications often fear possible performance degradation, which leads them to deactivate these functions. Patching of operating systems in industrial environments cannot be carried out easily during normal operation, compared to the patching of operating systems in office environments.

Unlike IT networks with a component lifetime of no more than five years, requested lifetimes of OT components are in the range of decades, varying from 15 to 25 years. OT software and hardware will therefore be outdated after a certain time, e.g. due to the end of maintenance support. In combination with discontinuous patching, these systems become an easy target for cyberattacks because of the vulnerabilities and 'holes' in such outdated software and hardware.

Any cyber security measure shall be part of the security management system and shall support the requirements of the permanent adaptation/improvement of security with appropriate tools. The focus will be on the prevention and detection of cyberattacks, as well as on the support of initiation of countermeasures. Also, a recording of all activities, regardless if an attack is successful or not, is required.

In order to achieve a reasonable level of cyber security, both organisational and technical measures need to be implemented in order to ensure the integrity and availability of all (passive and active) components that are part of safety, instrumentation, control and automation, communication and IT systems. It also includes measures and technologies required to monitor support systems.

The technical measures shall also cover: the requirements for the network design (network separation, data flow control, network devices, time synchronisation, security management); the hardening of all relevant IT and OT components (asset and configuration management, vulnerability management, patch management, user authentication and authorisation, intrusion detection systems, log management system, security incident and event management); the definition of all interfaces between the internal zones as well as to external networks (secure remote access); and the detailed back-up and recovery concept.

All organisational measures resulting from the risk assessments as well as being part of the integrated security management system, need to be implemented in the IT/ OT systems. These measures are very similar to the known requirements of a common office environment. The relevant policies are to be defined, a security officer needs to be nominated, and security checks on personnel are required.

The entire supply chain has to be secured in order to ensure that no counterfeit hardware and software is procured, and that the hardware and software is not contaminated by malware during production and manufacturing.

Basic principles include:

- Software development lifecycle programme in place.
- Only personnel involved in the software development have access to the information, rooms, hardware and software.
- Applications are executed with least privileges.
- Applications process and store only information relevant to the task.
- Strong input validation is implemented.
- Static and dynamic code analysis is performed by developers regularly.
- Application captures all data about abnormal conditions.
- Application fails in a secure or safe way.

Verification of the holistic approach

All security system parameters and functionalities should be verified on a regular basis during the engineering phases by design review meetings, and during the implementation phases by predefined test procedures. The test procedures need to be extended accordingly and shall cover all components of the security system, the organisational measures, plans and work instructions defined in the security management system, the emergency response plans and the physical and IT/OT security measures. In each of these tests the effectiveness and practicability of the implemented measures shall be demonstrated (e.g. by a penetration test). Already during a factory acceptance test, an integrated security test procedure shall be established to verify the performance of the entire security solution. The physical protection measures will be subject to the commissioning and the site acceptance test.

Prior to the start of operation, training programmes tailored to the specific installation and the security management systems are required. Only after this training can the final verification of the security management systems be completed.