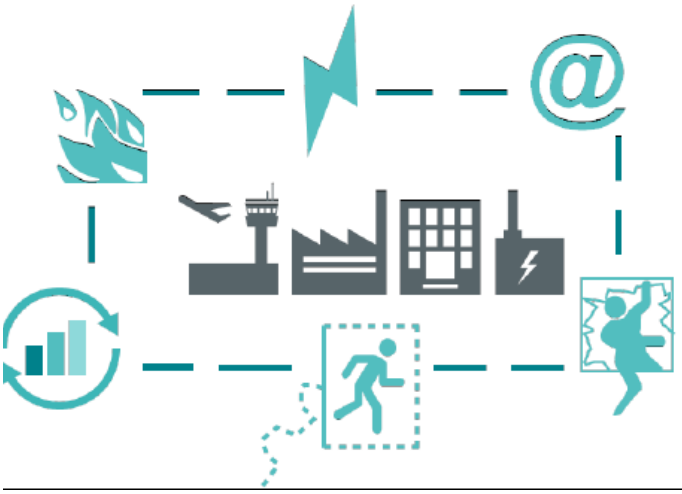
COMMAND AND CONTROL

The challenges facing high-risk facilities are becoming ever more complex. Even low-level intrusions can cause disruption, damage and loss of assets. Siemens examines how businesses can tackle this issue and deliver a safe and automated working environment.

A security attack on your facility can happen at any time. There is a significant probability that it will result in an interruption of vital services for extended periods, leading to the potential loss of reputation and public confidence. Many organisations therefore, face the issue of how to upgrade existing viable security technologies to a new IP management platform so they can deliver a greater level of intelligence and system functionality. Furthermore, there is the management of the cyber threat to network security as well as the system and software integrity.



Even within the same organisation, the needs of different locations will vary considerably and priority must be given to ensure the security measures taken are relevant to the threat, rather than a 'blanket approach'. A full risk assessment should be undertaken across individual locations to uncover potential vulnerabilities, understand the impact of intrusion or attack, and identify the optimum security response.

Developing and implementing security measures and best practices is known as 'hardening'. Hardening is a continuous process of identifying and understanding security risks, and taking appropriate steps to counter them. The process is dynamic because threats, and the systems they target, are continuously evolving. It is also vital to establish a formal security policy and response plan that describes how an organisation addresses security issues, in terms of practical procedures and guidelines.

The role of technology

The key purpose of every security system should be to deter, detect, delay and deny unauthorised intrusion and to communicate and control any security or hazardous incident:

Deter unauthorised intrusion by showing visible and effective security measures.

Detect activity across multiple sites.

Delay intruder attempts to defeat or bypass access control measures

Deny access to restricted areas.

Communicate incidents to designated personnel and provide the technical means for effective control of critical incidents.

Centralised command and control platforms manage critical situations and enhance security operations, whilst reducing risks. Operators are immediately prompted to take the correct action and the software will automatically set in motion a sequence of pre-agreed activities to ensure the right procedures are adhered to, as well as distributing essential information across multiple agencies.

A typical project scope might encompass the integration of wide-area surveillance; automatic number plate recognition; perimeter and site intrusion protection; access control for people, contractors and vehicles; alarm management; video analytics; fire detection and extinguishing; phased evacuation systems; lone worker monitoring and asset tracking.

This integration of many disciplines provides centralised situational awareness, improved information and intelligence, effective response to critical events and the proper co-ordination of resources. Security operatives are able to accelerate their response to alerts and manage risk before it escalates to a more serious incident.

Incidents can emanate from multiple sources such as system analytics or intruder devices, and an automated workflow or rules engine will prioritise the importance of these and alert operators in a number of ways. Deep integration enables identification and analysis of unusual behaviour and anomalies to facilitate proactive, rather

than reactive, decision-making. By combining a wide variety of building and infrastructure systems, and creating a logical sequence, it is possible to limit the escalation of damage.

Alarm rules will also assist operatives in managing response times, actions and feedback. Exported video can be combined from multiple cameras into one cohesive flow of evidence for analysis and importantly, a full audit of all activity can be generated automatically to provide a full incident report.

The centralisation of activities can also reduce cost and improve user efficiency as the command platform synchronises inputs from multiple disciplines, enabling operators to quickly master each situation, and to mitigate human error, decision making is more automated and systematic.

The software delivers a decision management workflow that assigns priorities, determines activities and allows them to allocate the appropriate actions and resources. This high level of transparency, complete with detailed reporting and audit trails, provides vital information to senior management to enable a better understanding of their site operations, leading to future improvements and cost efficiencies.

Integrating legacy systems

Existing systems and technologies often need to be integrated into a new control system. This will necessitate the creation of 'soft' interfaces, making it easier to integrate and reconfigure to adapt to change in the future, and operate from one single platform. To address key operational, protection, safety, future planning and compliance issues, organisations need to develop technology migration strategies that enable upgrades and improvements, whilst sustaining original system elements. Critical to success is the migration path which ensures high system availability throughout the change-out programme and is designed to incorporate interoperability between the existing and new technology portfolios. This enables both security and video system availability and low disruption during system change-out.

Cyber security

To counter the cyber threat, companies must establish risk-based rules that ensure adequate protection, with clearly defined and mandatory requirements. Baseline standards include:

Identity and access management: connected devices must have secure identities and safeguarding measures must allow only authorised users and devices.

Encryption: connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate.

Continuous protection: companies must offer updates, upgrades, and patches for their products, systems and services via a secure update mechanism.

Conclusion

High-level security solutions save lives, protect organisations and reputations and ensure business continuity across the UK's vital services.

The improved assessment, management and transparency of safety and security disciplines and the protection of vital assets are provided through improved automated decision-making, more efficient workflow procedures and greater convergence of technologies.

In line with the need for both the public and private sectors to lower costs, these software platforms enable superior operational performance, improved shared services, greater efficiencies and cost reductions, enhanced energy management, and a safer and more sustainable organisation. In short, they improve the protection of people, communities and assets.

www.siemens.com