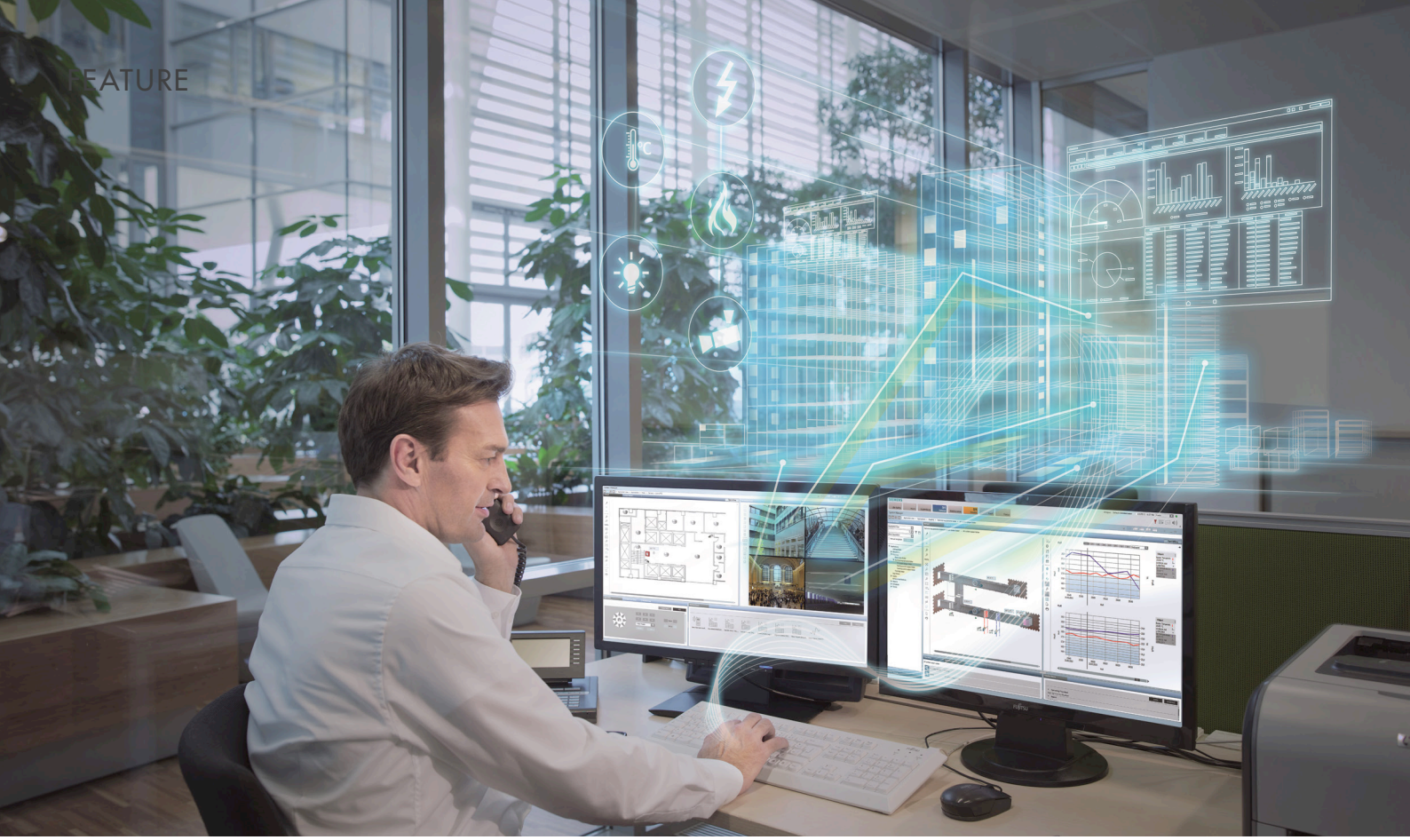

SAFEGUARDING SOCIETY

Damage or destruction to essential services by extremist groups has the potential to threaten public health, disrupt services and even cause loss of life. Siemens examines some of the challenges and solutions facing the nation's critical infrastructure.

Protection strategies

It is vital for organisations to drive a risk management strategy which should be supported by governance and implemented by the Board and senior management. All employees, contractors and suppliers should have a clear understanding of the risk management regime and be familiar with all related policies, practices and risk boundaries.

The best methodology for organisations to safeguard themselves against security threats is to use a fusion of protection measures encompassing physical, personnel and cyber security. A multi-layered approach will deliver the optimum combination of deterrence and detection, and assist in the delay of any attack.

It is imperative that procedures, measures and investments put in place are appropriate and proportionate for that specific situation. Even within the same organisation, the needs of different locations will vary considerably; therefore 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.

The role of technology

Critical national infrastructure faces many operational challenges, but these can be alleviated through the adoption of an integrated technology-based approach, harnessing the experience and knowledge of solution providers who understand the specific requirements of these complex industries and public sector agencies. 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.

High level security and safety

A typical project scope might encompass: command and control solutions; wide area surveillance; perimeter and site intrusion protection; access control for people, contractors and vehicles; alarm management; analytics and intelligence; fire detection and emergency evacuation systems. To achieve fully protected critical national infrastructure necessitates the installation of robust command and control platforms that improve protection across multiple sites, manage critical situations and enhance procedures.

These improve efficiency and enhance security and safety 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. 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.

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. 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 is automatically generated to provide a full incident report.

Minimising risk in the area of cyber security comprises both comprehensive security mechanisms and integrating security activities into the whole lifecycle. This means taking security considerations into account during development and engineering as well as service and operations activities. Comprehensive security mechanisms should combine physical and network security, and system and software integrity. Cyber security issues have been the subject of standardisation for some time, and Siemens plays an active role in all major organisations; among others, Siemens supports the work of ISA-99, IEC 62443, DHS, BSI, WIB NAMUR and CLSI AUTO11-A2 to make sure that common cyber security standards are developed.

A high knowledge base is required to address the technical complexities of critical national infrastructure, as well as the necessary capabilities to operate effectively in a hazardous environment with full compliance to

rigorous processes and procedures. Fundamental to this environment are robust health and safety policies and practices. These should focus on critical areas of the business where safe behaviours by managers, employees, contractors and agency staff are essential to safeguard all.

For high-level fire protection, fire safety systems should eliminate the potential for unwanted alarms and offer 100% reliability, particularly in critical locations where immediate and accurate fire detection is vital to life safety and business continuity. Working in tandem with high level security and fire safety solutions are voice alarm systems that enable both automatic and live messaging to alert all personnel to critical incidents. These assist in the phased and orderly evacuation to safe muster points, even from multi-level, multi-occupancy buildings. Research has proven that in an emergency, people will react without confusion or panic if they receive a clear, intelligible message informing them of the nature of the incident.

Conclusion

It is vital that life critical security and fire safety systems are fully supported by engineering teams who are trained to identify and interpret customer specifications, CDM requirements, relevant legislation and British Standards, and the impact on health, safety and the environment. High-level security and fire safety solutions save lives, and protect organisations and reputations; furthermore they ensure business continuity across the UK's vital services.

Command and control assists by adopting a systematic approach; one that includes the development of a clear technological roadmap to drive a coherent, joined-up and long-term investment strategy that includes safety and security at its core. Taking a wider view of how people and businesses can better prepare for threats to the nation's critical infrastructure is essential to avoid disruption, damage, loss of assets and severe economic loss.

www.siemens.co.uk/safe-secure-sustainable