Technical Article

Infrastructure & Cities Sector
Building Technologies Division

Zug (Switzerland), September 12, 2012

Effective protection of critical infrastructure through systems' coordination and communication

By Bernhard Voit, Head of Portfolio Command and Control, Siemens Building Technologies

Attempts to destroy power plants, cut off supplies of food and fresh water, disable communications or paralyze transport systems are, unfortunately, realities of modern life. The recent, politically-motivated, terrorist attacks in the USA, UK and Europe, have helped to illustrate how these threats can impact on a country's economy, public safety or environmental health. In many cases, critical infrastructure has historically been designed and built with the priorities of efficiency and cost, with protection given little regard. Security of critical infrastructure systems was sacrificed for economy and, subsequently, systems and installations are seen to be vulnerable to attack.

The four megatrends demographic change, urbanization, climate change and globalization are having an increasingly profound effect on people's everyday lives. Of these trends, the growing global population and the ever-increasing move towards city-living means that, everywhere throughout the world, people are becoming even more reliant on the critical infrastructures that support thriving mega-cities. There are basic physical and organizational structures that are needed for societies to carry on functioning efficiently and effectively. These include the generation, transmission and distribution of electricity; the production and supply of oil and gas; the water supply; the roads, rail networks and other transportation systems; airports and travel systems; telecommunications, finance and banking systems. They all play a substantial and vital role in the daily lives and continued well-being of citizens all around the world. The everyday services and benefits that these diverse and different elements of critical infrastructure bring to society are generally taken for granted but, whenever access to them is denied, they are sorely missed.

Terrorists and political activists worldwide are fully aware of the destabilizing effect of loss of infrastructure. Not surprisingly then, the need to install comprehensive protection systems to all critical infrastructure has become a priority and taken on much greater significance. This is true, not only when designing and building new facilities but also when attempting to safeguard existing installations and services. Especially in the Asia Pacific region, safety and security have traditionally been treated as stand-alone systems. However, awareness is growing that integrated and interactive systems will improve the existing safety and security processes substantially.

Protection of vital everyday facilities

Protection of the assets that are essential to the everyday functioning of society covers a wide range of disparate utilities. Incidents in recent years have proved that failure of individual power plants can destabilize the power distribution networks across countries and can cause blackouts for large geographical areas just as it happened in India recently. Power plants, whether they are based on the old technologies of burning coal or gas, or the comparatively new processes of solar-power, geothermal, or renewable, are all very different. Many different factors such as their design, age, legislation, fire regulations or the requirements of insurance providers influence the demands for their security. The one thing that they do have in common, however, is that they cover large and complex sites.

The same is true and even more visible for airports. By the very nature of modern air travel, airports cover long tracts of land for take-off and landing and necessitate the use of various buildings for the processing of large numbers of passengers and the maintenance of facilities. They are like self-contained cities that translate into a maze of security challenges for decision-makers charged with ensuring passenger and staff safety, safeguarding business processes and protecting valuable critical assets.

Data centers are significantly increasing in number and are likely to continue to do so as business becomes ever more reliant on them. They are so fundamental to everyday living that protection of the data they hold and the uninterrupted availability of business, communication but also security processes and service they host are crucial. Cyber crime covering data theft, malicious uploading, data corruption, political or commercial espionage, theft of intellectual property or the simple denial of service to vital systems is therefore a big issue which needs to be addressed.

Terrorists physically attacking or disabling vital data centers are also a potential threat. The increased use of hosted services, cloud computing and virtualized environments makes the total protection of data centers even more critical.

Protection of mining resources and data

Security is a major concern for mine operators too. All mining assets need to be protected to ensure continued profitability of operation. Theft and manipulation of resources, along with eavesdropping by unauthorized persons, must be prevented. Necessary security solutions can include components such as access control, biometric ID, video surveillance, perimeter protection, screening and danger management systems to help security personnel make the right decision in the event of a security breach. Data security solutions can help minimize the risks to mine owners and operators posed by hackers and other Internet-based security breaches.

A multi-layered approach to security

Prevention is undoubtedly the most important aspect of effective security. By anticipating, identifying and classifying potential threats, it should be possible to limit their impact. Then, should any incident take place, rapid detection combined with effective response through reliable communication and optimum coordination of resources should minimize the impact of the incident and facilitate a rapid recovery and return to normal operation. A multi-layered strategy which involves a range of physical and electronic systems and capabilities is the best way to keep facilities as secure as possible.

Sites that are complex and cover a large area with extended perimeters need constant surveillance and monitoring. Physical motion detectors used in tandem with integrated intelligent video surveillance solutions offer reliability and effectiveness, even in harsh external operating conditions, triggering an alarm and allowing real-time verification and response before access to critical areas is gained. Data centers are often located in newly-constructed, prestigious buildings or science parks where – rather than high, chain-link fences – 'virtual' perimeters are established. The video sensory analysis of state-of-the-art video systems, possibly even in combination with radar systems, provides classification and localization of detected objects along with custom policies that enable a single operator to handle and manage the data from a large and complex perimeter without fatigue. Operators who just try to watch signals from hundreds of cameras on a video wall would miss most of the incidents.

Fully integrated access control systems can provide high levels of security and convenience for the buildings and storage areas on any site, offering controlled yet efficient movement for workers, management, contractors and visitors whilst maintaining a secure environment. Intelligent fire solutions for the protection of the site – particularly potential problem areas of power plants, airports, chemical or pharmaceutical plants, oil and gas facilities and data centers – are able to detect the smoke, heat and pre-combustion particles in the very earliest stages of a fire. Building systems too, with the appropriate tailoring during planning and installation, are able to integrate devices with common open protocols into a single robust control system, able to regulate airflow, monitor energy use and integrate with fire detection, access control, security lighting and other security and life safety relevant systems.

Intelligent response through integration

Providing a safety and security solution that integrates different systems into a single, multi-modal, administrative solution is not just about merging equipment, devices or systems. It is about putting into place a solution to support clearly defined normal working routines whilst ensuring rapid, compliant and efficient response to emergency situations along with the mandatory, post-incident reporting analysis.

Today’s security solutions for critical infrastructure combine intelligent video capabilities with command and control features. They can be customized according to specific corporate set-ups, policies and processes. Specifically designed for critical infrastructure sites such as power plants, airports, oil and gas facilities, and industrial complexes, these solutions give more than just a display of video images and alarm incidents on an intuitive graphical interface. Signals received can be associated with predefined actions giving a complete decision-management workflow, helping the operator to assign priorities and determine emergency procedure based on specific, pre-configured guidelines for that site. Continuous and dedicated communication between the infrastructures’ security command and control center and the on-site responders ensures that coordination of the response operation, escalation or de-escalation of a critical situation, can be managed. Records can then be archived and used for the continuous improvement of the site’s security operations.

Using open and flexible architecture, these solutions are able to integrate a broad variety of subsystems. These include perimeter protection, intruder detection, video and wide-area surveillance, access control, fire detection, alarming and extinguishing along with building automation systems, emergency call systems, telephone and radio communication systems. This consolidation onto a single platform gives operators and managers real situational awareness and represents it graphically in a user-friendly way. The platform supports the roles typically found in a control center and offers the kind of real time functions and information needed in complex situations. It streamlines operations, unifying all data needed to coordinate effectively and quickly any incident response. It provides workflow-based support of efficient decision-making in real time for routine operations as well as emergency situations, thus increasing effectiveness whilst minimizing the possibility of errors.

For larger sites, the implementation of wide-area intelligent video analytics will enable the facility to track and classify moving objects automatically, triggering alarms when pre-determined limits such as prohibited areas, policy zones, virtual tripwires etc. are broken – even across water. This makes it possible to provide the continuous and effective, around-the-clock monitoring of critical areas not only of airports, industrial facilities, transportation hubs and power plants but also of water treatment facilities, docks or seaports.

The integration of generations of systems installed and provided by different vendors is a very challenging and demanding task. It involves many aspects, not only the technical issues. The processes being introduced, along with a state-of-the-art command and control system that integrates multiple subsystems, impact customers’ security organizations and qualification of personnel. Allowing for more efficient organizations, the introduction of command and control solutions implies a change process on multiple levels of the organization.

Standardization in the area of command and control

The introduction of the European standard EN50518 – monitoring and alarm receiving center – gives directions specifically for control centers that respond to incidents with a potentially criminal or terrorist background. The standard describes location and construction requirements, technical requirements as well as the procedures and issues relating to the operation of a command and control center. Thus it is designed to ensure highest availability of the control center against technical or personnel failures and to protect the control center itself against attacks.

This standard is expected to change the design and setup of command and control centers and security organizations, not just in Europe but also in the Middle East and Asia Pacific regions, particularly in low cost countries in which typically a high number of personnel guards are deployed. Enterprises operating internationally will require compliance towards the same standardized processes throughout all of their locations.

Dispatch of response teams in an emergency

Some of today's command and control solutions that connect the various subsystems of critical infrastructure sites that would otherwise run in isolation, can also manage the deployment of security personnel throughout the site. The status and location of all available resources are clearly displayed via a Geographic Information System (GIS) on maps and site plans in two or three dimensions and proposals providing the most appropriate use and deployment of personnel are given clearly and effectively to operators as computer aided dispatch.

Other system features might include automatic or semi-automatic alarming and the transmission of task-relevant information, along with the logging of operational progress. Such solutions can help security operators and rescue and emergency services to optimize operational processes including the management of complex coordination and communication requirements. They fully support the dispatch of security guards, the emergency services, or service engineers and also support the different means of communication between the control center and the responding forces.

Also for incidents reported via telephone, integrated functions ensure fast and easy communication in an emergency situation. When an incoming call is received, the system recognizes and displays the caller number, name and location in the GIS or in a building's floor plan and can be configured to route it automatically to a dedicated team of operators. These systems also offer integrated control for communication with on-site resources via analog radio or TETRA digital radio (Terrestrial Trunked Radio) communication. A two-way dialogue between the control center and all resources via regular e-mail communication through standard PDAs (Personal Digital Assistants), ‘palmtop’ computers or, more commonly, today’s smartphones also ensures seamless and uninterrupted communication.

Communication in a crisis

Software recently developed by security solutions provider Siemens provides an integrated communications solution suitable for the operators of critical infrastructures such as airports, chemical plants and power plants as well as for the control centers of fire brigades, police departments and search and rescue organizations. Siveillance Vantage Connect combines and processes normal phone calls, emergency calls, radio calls and other notifications, allowing all communications to be consolidated and displayed clearly on a touch-screen, regardless of whether the information is transmitted over analog or digital landlines, cellular networks, IP-based channels (Internet Protocol) or by fax. This provides control center personnel with an accurate and concise overview of all current information arriving over different communications channels and allows them to take the necessary actions. In the future, additional media channels such as text messaging, instant messaging and social media will be added to the system.

Highest safety and security for sites

In summary, the more diverse and complex the risks of any site, the more important it is to have an intelligent, integrated system that can manage all aspects of safety and security. Command and control solutions have been developed by security providers to enable centralized alarm management and supervision of a wide range of different safety and security subsystems, allowing interaction between the disciplines to enhance overall safety and security, even for multi-site applications. Regardless of how many subsystems are connected, they can all be displayed in a uniform and clearly structured manner, allowing operators to manage the system easily and safely, even under the most stressful emergency conditions.

With user-friendly engineering tools, security solutions for critical infrastructure can be configured quickly and easily. Powerful graphics engines support existing AutoCAD type building drawings or floor plans and thus offer the operator a comprehensive system overview. Icons within the graphic displays show the current state of equipment and alarms and messages are clearly listed according to security-relevant priorities, so operators have all relevant information at a glance. In the case of an emergency situation, operators are again guided step by step through pre-defined procedures.

Long-term disruption to critical infrastructure, whether it is natural, accidental or deliberate, will have a devastating effect on the lives of millions of people. Powerplants, petro-chemical and heavy industries, roads and rail networks, airports, transportation systems and communication and computer networks all need to be protected. As the importance of their role increases as mega cities continue to develop, innovative solutions need to be applied to ensure even the most complex sites are given real security and protection.

The **Siemens Infrastructure & Cities Sector** (Munich, Germany), with approximately 87,000 employees, offers sustainable technologies for metropolitan areas and their infrastructures. Its offerings include integrated mobility solutions, building and security technology, power distribution, smart grid applications, and low- and medium-voltage products. The Sector comprises the Divisions Rail Systems, Mobility and Logistics, Low and Medium Voltage, Smart Grid, and Building Technologies. For more information, visit www.siemens.com/infrastructure-cities

The **Siemens Building Technologies Division** (Zug, Switzerland) is the world leader in the market for safe and energy-efficient buildings ("green buildings") and infrastructures. As a service provider, system integrator, and product vendor, Building Technologies has offerings for building automation, heating, ventilation and air conditioning (HVAC), fire protection and security. For more information, visit www.siemens.com/buildingtechnologies