SIEMENS

Technical Article

Zug, December 18, 2014

Security management for critical infrastructures

Critical infrastructures ensure the survival of a functioning community. At the same time, they are exposed to any number of hazards. Experts around the globe are working on organizational as well as technical responses to these challenges. At the core is the implementation of systematic security management for critical infrastructures.

By Ralph Müller, Market Manager Utilities, Siemens Building Technologies

Critical infrastructures are institutions and facilities that are vital to the functioning of a public community. If they fail partially or even completely, major supply bottlenecks and serious disruptions to public safety and security can result. Because critical infrastructures are increasingly interwoven and interdependent, serious incidents can set in motion cascade or avalanche effects. Last but not least, terrorist threat scenarios are bringing the security of critical infrastructures to the fore in national and private-sector security policy. Institutions and facilities that need safeguarding include energy supply, information technology, telecommunications as well as transportation and traffic, e.g. airports.

The mutual interdependence of critical infrastructures is not limited to individual sectors but, because of globalization, is increasingly transnational in nature. For example, countries purchase energy from neighboring nations to ensure a continuous supply. If the energy supply in one country is compromised, bottlenecks arise in neighboring countries. Because protecting critical infrastructures is not just a national issue, higher-level organizations such as the European Union have started to focus on it as well.

Safeguards are growing in importance

A recent incident highlights how dire the need for action is when it comes to critical infrastructures. In the spring of 2013, a transmission substation near California’s third largest city of San Jose was the target of a night-time attack. Unknown gunmen opened fire on the facility and destroyed 17 out of 21 major Silicon Valley transformers valued at several million dollars each. With a minimum of effort, the culprits took down the entire facility. The attack immediately raised fears in the U.S. that the national power grid could become a terrorist target. These fears were not unfounded, considering it took 27 days to restore operations. Similar cases of intentional sabotage of substations have also occurred in Europe, such as in Great Britain.

Even less dramatic incidents can have serious consequences for critical infrastructures. Remote substations, railway tracks and power transmission lines are not only vulnerable to vandalism and sabotage, but also at risk of theft of valuable metal cables. Rising metal prices worldwide have substantially driven up the number of thefts in recent years. The methods used by thieves, who primarily target copper and nickel, are becoming more professional and aggressive; even armed attacks are no longer rare. The damage total amounts to several hundred million euros annually. Even more serious, however, are the associated disruptions in businesses and public rail traffic.

The introduction of smart grids, intended to optimize the balance between energy supply and demand, will make the overall energy supply network even more complex. Electronic security solutions can minimize the potential threats in this network infrastructure, thanks to technology such as access control and video surveillance systems.

Research programs on critical infrastructures

Because of this growing risk, government agencies worldwide have begun to define minimum security standards for critical infrastructures. The North American Electric Reliability Corporation (NERC), for instance, is currently working on a security standard for substations. Large-scale security exercises, such as GridEx II in

November 2013, produced valuable insights. This effort simulated cyber and physical attacks on U.S. energy supply facilities and tested emergency measures.

In the European Union, numerous research programs are focusing on the protection of critical infrastructures, with cross-border infrastructures of particular interest. The European Reference Network for Critical Infrastructure Protection (ERN-CIP) established by the European Commission aims to strengthen relations between public institutions responsible for protecting critical infrastructures and the private sector. The ERN-CIP project launched in 2011 uses models and simulations to map cross-linked dependencies so sensitivity analyses can be performed. The design and processes of European energy, information and transportation infrastructures are being reviewed to determine if they are adequate for protecting critical infrastructures. The goal of these efforts is to ensure the uninterrupted availability of critical infrastructures.

Siemens study defines security management requirements

From a strategic point of view, it is absolutely essential that risk analysis, planning, communications and coordination of security measures for critical infrastructures be performed centrally. Siemens has been intensely engaged in security management issues for some time. In a recent study, the Building Technologies Division investigated how operators of critical infrastructures manage risk and what they expect from software solutions for security management designed to support them in their tasks. Four areas particularly at risk were studied: energy production and transmission facilities, airports, chemical and pharmaceutical plants, and campus-like environments such as universities.

The vast majority of those surveyed want security management software that first and foremost ensures the safety of individuals. In addition to protecting people, energy suppliers want to ensure a continuous supply of energy to the public as well as to fulfill official compliance regulations. Airport operators, on the other hand, see maintaining air traffic in accordance with official regulations and guidelines as especially important.

What special requirements do the study respondents have for security management software? Modular design that can be customized as needed is at the top of the list.

The software also needs to accommodate the growing need for technical consolidation of command and control stations. This is particularly true for air traffic as well as energy supply.

Siveillance Vantage as a central security solution for critical infrastructures
Over many years Siemens has gained a wealth of experience managing the security of critical infrastructures. This knowledge of precise customer needs was built into the Siveillance Vantage command and control solution. This software is specifically designed to support security management in critical infrastructures such as energy supply, airports, seaports, transportation, industrial complexes and campus environments. Whether for daily routine processes or in crises and emergencies, the solution provides real-time, targeted support for a reliable, scalable and efficient response to security incidents. The software solution is designed for installation in existing IT infrastructures. Open interfaces and integration technologies support the integration of a wide range of security systems. By consolidating these subsystems on one platform and combining all the data in one control point, security officers can quickly assess the current situation, make informed decisions and coordinate the necessary measures. This integrated communication approach saves critical minutes and seconds, thereby ensuring very quick response times to keep the situation under control.

A Geographical Information System (GIS) shows the incident location and the current position of security and safety resources on overview maps. Security and safety personnel and vital equipment can be pinpointed within a building using floor plans. In addition to displaying the status, availability and current position of resources, the system suggests the best available intervention forces for the task at hand.

Siveillance Vantage offers integrated phone and emergency call handling on a failsafe and networked platform. The software not only sets up connections to the police and fire departments, but also supports radio communication with internal company security personnel. It also offers individual interfaces to internal telephone, communication, alarm, access control, video surveillance and fire detection systems.

In addition, Siveillance Vantage can display messages from the various alarm systems with defined priorities to ensure that the most critical incidents are addressed first. Each alarm and incident can be associated with defined actions, which are then suggested to the operator as the situation warrants or carried out automatically. The software can be adapted to internal security policies, and appropriate measures for daily routines, time-critical procedures, and emergency and crisis situations can be defined.

Conclusion

More than ever before, critical infrastructures are tied to a multitude of security-related challenges. Intelligent software-based command and control solutions like Siveillance Vantage help infrastructure operators face these challenges.

A press picture is available at http://www.siemens.com/download?PR00350

For further information on the Building Technologies Division, please see
www.siemens.com/buildingtechnologies

Contact for journalists

Catharina Bujnoch
Phone: +41 41 724-5677; E-mail: catharina.bujnoch@siemens.com