INTEGRATING SAFETY AND SECURITY IN PROCESS CONTROL

JOIN SAFETYBASE

RISK ASSESSMENT

INDUSTRY STANDARDS

OSHA

Home / Compliance / Articles / Integrating safety and security in process control

Safety Compliance, Assessments, Standards and OSHA.

In order to make sure that your plant or operation is compliant it is important that you know what compliance regulations and standards are in place. That's why at SafetyBase.com you'll find the latest compliance information and regulatory standards that can help you stay informed. Choose from the selections below to learn more.

Integrating safety and security in process control

2009-10-20

Traditionally, safety and security in process control adhered to a philosophy of separate but equal. Today, that approach is changing. Interest in integrating these two critical functions is accelerating and benefits are accruing—for a number of reasons:

- First and foremost, control systems engineers are recognizing that safety and security have common goals. In the end, both involve life safety. Whether the cause is an unsafe act or a security breach, the fear is the same—that a personnel safety incident might occur. "Avoiding production interruptions and downtime are important, but secondary," observes Exida's John Cusimano, director of cyber security. "From a control system standpoint, most companies are less concerned about data falling into the wrong hands than about somebody altering a system in a way that could cause danger to someone."

- Second, adopting a common methodology or lifecycle approach to safety and security is simply more efficient engineering. It avoids duplication of effort, minimizes the possibility of omissions, and helps develop a safer and more secure system overall. "Doing an automation system safety design, and then going back to see if it is secure enough wastes time and effort," explains Cusimano. "Doing the two concurrently is more efficient and makes it less likely to overlook something."

- Finally, security and safety are more readily integrated today because the differences that once separated them are disappearing. As industrial control systems adopt commercial technologies and operating systems, vulnerabilities increase. As networks and open systems proliferate and IT infrastructure is incorporated into control systems, the expertise of IT security professionals is required to help manage these unfamiliar technologies. "We can't always apply IT security practices to process control as they are applied in the IT environment," warns Cusimano. "They need to be tailored to the control system. This reality has created the need for an overlap between the two disciplines, fostering a team approach that is becoming critical to effective safety/security integration."

Disparate roots, converging goals

These recent trends toward successful convergence, however, belie the historically disparate roots of safety system engineering and control system security. Safety system engineering, the more mature of the two, has developed over the past 10 to 15 years, drawing upon the experiences of engineers who design, implement, and maintain automation systems safety. Its development was driven by industrial incidents and accidents and led to the promulgation of international standards—such as IEC 61508 (*Functional safety of electrical/electronic/programmable electronic safety-related systems*) and IEC 61511 (*Functional safety: Safety instrumented systems for the process industry sector*)—that have made it possible and practical for engineers to incorporate safety system methodologies into their designs in consistent fashion.

Control system security practices, on the other hand, have markedly different beginnings, with origins in the IT world. When control systems engineers sought security for the new IT technologies they were applying, they turned for help to those already experienced with methodologies proven to prevent unauthorized access and deal with unfamiliar standards such as ISO/IEC 15408: *Common criteria for computer security*. And from this diversity grew unprecedented cooperation, and an unquestionable awareness that safety and security practices in an industrial setting seek common ground: on the safety side to ensure that systems operate as intended and, if they fail, to do so safely; and on the security side to prevent outside influences from making these systems behave other than as intended.

Accelerating the integration

Given that the integration of these two disciplines is already under way in reaction to industry requirements, how should facilities best approach safety and security in their own process control systems? A good place to start is with a risk analysis. Cusimano recommends performing a HAZOP (HAZard and OPerability) analysis—most plants are familiar with this methodology—which employs a combined safety and security lifecycle. Analyze all four types of occurrences: internal, external, accidental, and intentional. Security incidents tend to be more external and intentional, while safety issues typically are internal and accidental, focused on equipment failure. "Note that studying accidental incidents," adds Cusimano, "often uncovers vulnerabilities that would allow the same hazards to occur should someone intentionally attack the system."

Process industry professionals should also be aware that a variety of forces are working to promote safety and security integration efforts. The ISA (International Society of Automation) S99 committee (*Industrial Automation and Control Systems Security*) is presently analyzing IT standards. Among the goals of its Working Group 7—which includes representatives from S99 and ISA S84: *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*—is to develop new standards

governing the integration of common safety and security practices that prevent dangerous situations and unwanted shutdowns in process control systems.

“We recognize that the efforts of both areas are to avoid the same consequences,” concludes Cusimano. “The safety system discipline is mature enough to provide a knowledge-base that can be applied to and help expedite security situations. We can’t afford to wait 10 to 15 years to gather a similar body of experience with security practices. We need to bring the existing experience of safety experts into the equation now, apply it to security practices, and together make the integration process work.”

For more information…
Additional information on safety and security products and solutions are available online from Exida at www.exida.com, and Siemens Industrial at www.siemens.com. Also visit the following two resources for a wealth of information on integrating safety and security in process control:

- *Repository of Industrial Security Incidents (www.securityincidents.org). RISI is a non-profit organization that maintains a database of cyber security incidents compiled over more than 20+ years. It focuses on incidents in process control systems, industrial automation environments, and SCADA systems in an objective, factual way.*

- *U.S. Department of Homeland Security (www.us-cert.gov/control_systems). The U.S. government offers abundant free resources and safety and security information from training to standards to technical information. Its Control System Security Program specifically addresses efforts to reduce industrial control system risks.*