« Back | Print

Pursuing the discipline of control system cyber security

By John Cusimano -- Plant Engineering, September 1, 2009

As a relative newbie to the world of control system cyber security (who isn't?) but an old-timer to control system functional safety, there are two things I have noticed. One, the best performing companies approach safety and security as an engineering discipline. Two, they maintain discipline by having a deeply embedded safety and security corporate culture.

What does it mean to approach safety and security as an engineering discipline? It's easier to answer that today by looking at functional safety, because that field is far more mature than "functional security," which, as a term, is just beginning to be defined and adopted by industry. About 15 years ago, there were no broadly accepted standards on how to design and implement a safety system. In fact, there was not even consensus on what these systems were called.

Names ranged from emergency shutdown system to Safety Instrumented System (SIS) with about a dozen names in between. With a lack of standards and very little published material on how to design these systems, most control system engineers avoided safety system design like the plague. Those that dared work on these systems were revered in the same way ancient cultures revered the medicine man.

The situation started to change around 1996 with the first release of ISA's Standard S84, and subsequently acceptance of the international standard IEC 61511 in 2004. The standards defined a safety lifecycle and the underlying methodologies that enabled engineers to apply the same kind of engineering rigor and discipline to designing safety systems that they were used to applying in other aspects of control system design. An international engineering standard enabled industry to respond with training, textbooks, services and even professional certification for functional safety experts through independent, non-profit organizations such as the Certified Functional Safety Expert (CFSE) Governance Board (**www.cfse.org**).

This revolution has yet to occur within the field of functional security but, based on history, I predict we are on the brink of a similar revolution in that field. ISA has released several parts of ANSI/ISA S99 Standard, and the ISA Security Compliance Institute (**www.isa.org**) indicates they will have an Embedded Controller Certification Program operational in the fall of 2009.

The other discipline I spoke of is the discipline of a safety and security corporate culture. What does it mean to have a safety and security culture? First, it means management commitment originating from the highest levels of the organization. Second, it means management demonstrates that commitment by establishing, implementing, operating, monitoring, reviewing, maintaining and improving process safety and process security management systems. Finally, it means enforcing these systems and holding individuals accountable for failure to follow them.

Recent process safety incidents and the fact that they are still occurring after more than 15 years of progress on the engineering side, indicate that there is still a long way to go in establishing a safety and security culture in many corporations. For example, according to data provided by the Repository of Industrial Security Incidents (**www.securityincidents.org**), two serious control system-related process safety incidents occurred at the same chemical facility in Institute, WV. In August 1985 the facility, then owned by Union Carbide, leaked methylene chloride and aldicarb oxime. The leak resulted from a computer program that was not yet programmed to recognize aldicarb oxime, compounded by human error when the operator misinterpreted the results of the program to imply the presence of methyl isocyanate.

More than 20 years later, on Aug. 28, 2008, an explosion and fire occurred at the same plant, now owned by Bayer CropScience. The explosion ruptured the residue treater and launched it 50 feet in the air. Two operators died. Reports indicate there were significant lapses in the plant's process safety management including overrides on the SIS to accommodate long-standing heater problems, plus failure to provide adequate operator training on the same SIS.

William Feather said, "If we don't discipline ourselves, the world will do it for us." The discipline of control system cyber security needs to become part of the corporate culture, as does safety.

« Back | **Print**