JOHN CUSIMANO
DIRECTOR EXIDA
SECURITY SERVICES DIVISION
jcusimano@exida.coml
ERIC BYRES
CHIEF TECHNOLOGY OFFICER,
BYRES SECURITY
eric@byressecurity.com

# Safety and Security: Two Sides of the Same Coin

According to Merriam-Webster, the primary definition of safety is, "the condition of being free from harm or risk." This is essentially the same as the primary definition of security, which is, "the quality or state of being free from danger." However, another definition for security is, "measures taken to guard against espionage or sabotage, crime, attack or escape." This is the definition we are using when we refer to industrial security.

Using these definitions, we can better understand the relationship between safety and security. The relationship is such that a weakness in security creates increased risk, which in turn creates a decrease in safety. As a result, safety and security are directly proportional, but both are inversely proportional to risk.

In the context of industrial automation and control systems, safety systems are special control systems whose function is to detect a hazardous condition and take action (shut down the process) to prevent a hazard. They are one of many layers of defense in an overall protection scheme for the facility. Control system security refers to the capability of a control system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data, nor gain access to the system functions, and yet ensure that this is not denied to authorized persons and systems.

Safety standards and associated engineering work practices are mature and well-established, based on decades of learning. However, control system security is a much newer field and has its roots in information system or IT security.

So why the sudden interest in integrating the two? First, safety-integrated systems (SIS), are increasingly connected to or integrated with process control systems connected to the outside world. This raises significant concerns about the possibility of a common security vulnerability affecting both systems.

Another reason is a growing recognition of the many similarities between the safety and security lifecycles, and that there are improvements and efficiencies to be gained by combining the two approaches.

Let's take a look at the safety and control system security lifecycle models. The safety lifecycle model from IEC 61511 (also ANSI/ISA S84) has three main phases: Analysis, Realization and Operation. The security lifecycle model from ANSI/ISA S99.00.01-2007 also has three main phases: Assess, Develop and Implement and Maintain.

The safety analysis and security assess phases have the most similarity by far because in both cases, the purpose is to determine the amount of risk present, and decide if it is within tolerable limits for the facility. Determining the amount of risk involves identifying consequences (what could happen and how bad would it be?) and the likelihood of their occurring (how it could happen and how likely it is to happen?).

A first step in this process is the hazard and operability analysis (HAZOP), which is a method for identifying and dealing with potential problems in processes, particularly those which would create a hazardous situation or severe impairment of the process. The industrial automation and control system (IACS) should be listed as a cause if its failure or unauthorized access could initiate a deviation.

Unfortunately, other than identifying the IACS as a potential cause, a HAZOP doesn't study the details of IACS deviations, which is an important step, given the size and complexity of modern control systems. This is where a control hazards and operability analysis (CHAZOP), the next step in understanding the details of IACS hazards, comes in.

Another technique is a failure modes and effect analysis (FMEA). Both techniques identify causes and consequences of control system failures. The CHAZOP technique extends the concept of deviations and guidewords from HAZOP, extending the list of guide words for IACS-specific types of deviations. The FMEA process takes a more hardware-centric approach by systematically studying the failure

Weakness in security increases risk, decreasing safety. Safety and security are directly proportional, but are inversely proportional to risk.

modes of each component and the effects on the system. Either technique is acceptable. However, regardless of the technique selected, it is important to include security deviations or failure modes in the analysis.

Using these metods, we should have identified all of the causes of IACS failure, including security failures, and their consequences. However, we still have not determined the likelihood of these events occurring.

Estimating likelihood, particularly for security, is hard because it can be very difficult to estimate the skill and determination of an attacker. We can simplify the task by filtering the list to include only those with intolerable consequences (e.g., have the potential to cause injury, death, significant downtime, environmental equipment damage).

In safety, one of the most popular techniques for estimating likelihood is layer-of-protection analysis (LOPA). The security field uses the term defense-in-depth to describe a very similar concept. Even though the terminology is different, the LOPA technique can definitely apply to security threats.

The final step in the front-end of the combined safety-and-security lifecycle is to compare the results with facility or corporate tolerable-risk guidelines and document the results. Whenever the estimated risk exceeds the tolerable risk there is work to be done.

The following case study from a major U.S. refinery illustrates the analysis phase and subsequent develop/implement phase.

This refinery was concerned about the safety, security and reliability of its safety systems. To start, management conducted a security risk analysis of all control systems, expanding on existing safety HAZOP studies. This information was used to drive a FMEA that clearly showed possible common-mode failures of the control and safety systems due to either accidental network traffic storms or deliberate denial-of-service (DoS) attacks. While the safety systems would fail in a "safe" manner, even under attack, the consequences would be a significant (and costly) plant outage. The probability of occurrence was estimated to be high because the skill level needed to drive such an attack was close to zero (and in fact could be caused accidentally), the attractiveness of the site to criminals or terrorists was high, and the layers of protection were limited.

The lack of clearly defined security layers drove the decision to adopt a zone-and-conduit model as defined in ANSI/ISA99.02.01 as the solution to the realization/addressing phase. The plant business network, the management network, the basic control system, the supervisory (operator) system and the safety system were each defined as a separate security zone. Between these, approved "conduits" were defined for inter-zone communications. (For additional information on the use zone and conduit models see http://www.tofinosecurity.com/ansi-isa99).

Next, the engineering team defined appropriate safety/security controls on each of the conduits to regulate inter-zone traffic.

An extended version of this article, including charts, is at www.control-global.com/1004OtherVoices.html.

While it is easy to get caught up in an IT view of security, and think only of hackers and viruses. For the operator of a hydrocarbon processing facility, security is is about maintaining the reliability and safety of the entire system. As a result, the security of process systems can be significantly improved with a coordinated approach to both safety and security, starting with the initial analysis. By following a well-defined process, this analysis phase can be both cost-effective and significantly improve the reliability of the entire processing facility, providing an excellent return on investment. ■