CONTROL ENGINEERING
ELECTRONICALLY REPRINTED FROM MAY 7, 2019

Sustainable cybersecurity architecture for safety instrumented systems

Choosing a safety instrumented system (SIS) architecture for defensible operation across the product lifecycle is one of the first decisions an organization must make; know these applicable standards.

BY SERGIO DIAZ AND ALEXANDRE PEIXOTO

When an organization begins a safety instrumented systems (SIS) project, one of the first decisions stakeholders must make is a choice of architecture.

It is possible to deliver successful, hardened systems using an interfaced or integrated SIS architecture within the constraints of international cybersecurity standards such as International Electrochemical Commission (IEC) 62443 (ANSI/ISA 62443 family of standards) and/or local recommendations, such as the User Association of Automation Technology in Process Industries (NAMUR) guidelines.

Understanding the unique benefits and considerations behind each architecture is critical to making an informed decision on which will best serve the needs of the organization.

Cybersecurity standards provide guidelines for separating safety-critical and non-safety critical components. Under ISA guidelines, safety-critical assets *must* be grouped into zones logically or physically separated from non-safety-critical assets.

NAMUR offers a similar set of guidelines in worksheet NA 163, "Security Risk Assessment of SIS." The guideline defines three logical zones—core SIS, extended SIS, and control system architecture (referred to as "peripherals" by NAMUR)—that must be physically or logically separated (Figure 1).

A core SIS consists of the components required to execute the safety function (logic solver, input/output [I/O] components, sensors and final elements). The extended SIS contains components of the safety system that are not required to execute the safety function (such as engineering workstations). Peripherals are components and systems such as the basic process control system (BPCS), which are not directly or indirectly assigned to an SIS, but they may be used in the context of a safety function. Safety functions might include a resent request from the BPCS or visualization of the safety function in a human-machine interface.

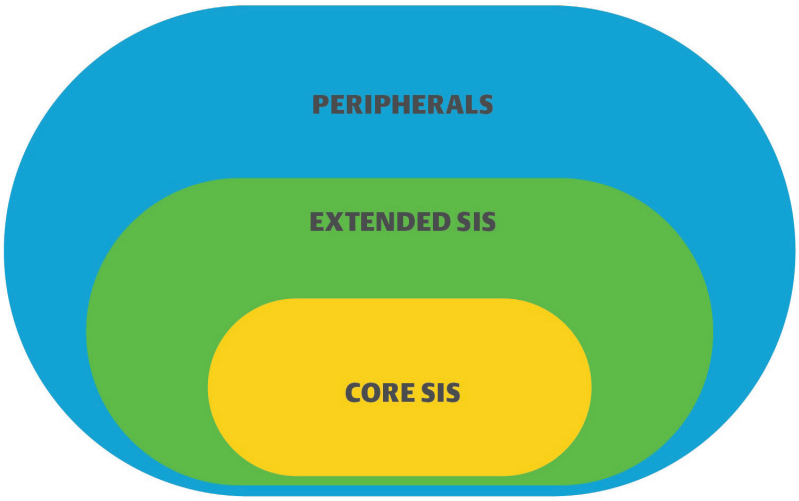

Figure 1: NAMUR offers a similar set of guidelines to ISA 62443 cybersecurity standard, with SIS functions grouped into three zones: Core SIS, extended SIS, and control system architecture (referred to as "Peripherals" by NAMUR). Courtesy: Emerson

Neither standard defines a required architecture. Users must decide how best to structure SIS networks and ensure the final design provides sufficient logical and physical separation between the BPCS and the SIS. This often leaves organizations with three choices for architecting SIS networks:

- A separated SIS completely disconnected and independent from the BPCS
- An interfaced SIS connected to a BPCS by means of industrial protocols (typically Modbus)
- An integrated SIS interconnected to a BPCS, but sufficiently isolated to meet cybersecurity standards.

Some may claim a separate SIS is more secure than any other SIS deployment type. However, all the architectures listed can deliver a hardened security posture as long as the posture is defined beforehand and enforced during safety system design, implementation and maintenance. While important, the SIS architecture is just one aspect of defining security for a safety system.

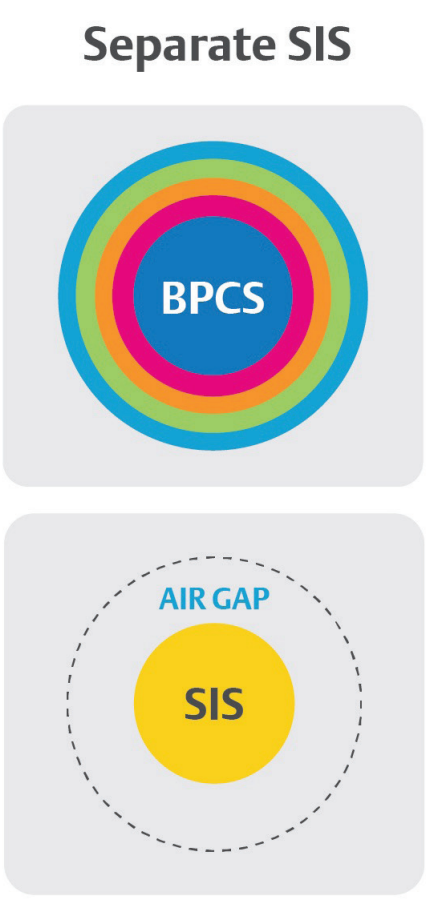

Figure 2: Air-gapped infrastructure separates safety-critical and non-safety-critical SIS but adds extra upkeep to maintain defense-in-depth safety layers on two different systems. Courtesy: Emerson

Maximizing defense-in-depth

Protecting an SIS requires a defense-in-depth approach. With cyber attacks rising every year, one layer of protection for safety-critical assets is not adequate. Network administrators are employing multiple layers of security—antivirus, user management, multi-factor authentication, intrusion detection/prevention, whitelisting, firewalls and more—to ensure unauthorized users face an insurmountable barrier to entry. The goal of a defense-in-depth strategy is to increase the access control protection mechanisms. This is done by adding layers of protection that complement each other.

Defense-in-depth – Separated systems

One of the most common methods for protecting an SIS is to separate the system entirely, creating an "air-gap" between the core SIS functions and the BPCS (Figure 2). The benefits of this approach seem obvious. If the SIS is separate from other systems, it is hardened against intrusions by default.

However, even separated systems are not immune to cyber attacks. Users eventually will require external access to the system for tasks such as extracting event records for sequence of event analysis, bypasses, overrides, proof test records or performing configuration changes and applying security updates. USB drives, which are often used to implement these updates, are not easy to protect.

External media dependency is one of the main reasons why a separated SIS still needs additional layers of protection like the ones used to protect the BPCS. Proper system hardening leaves users managing two separate sets of defense-in-depth architectures. This creates a high potential for more work hours, longer downtimes, and additional areas where oversights might leave holes in the protection layers.

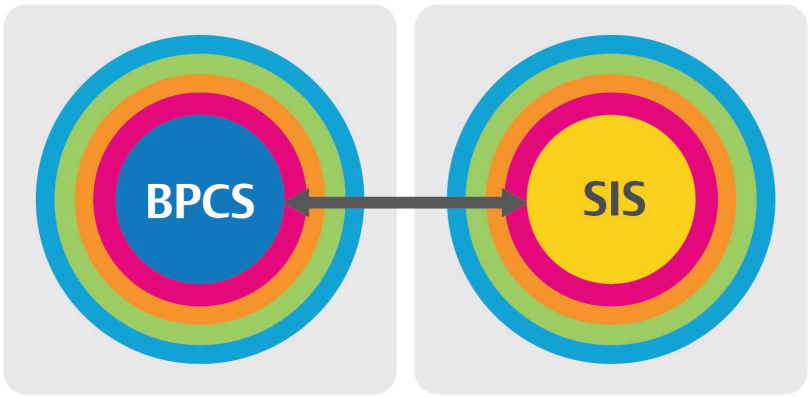

Figure 3: A cybersecurity vulnerability assessment also requires partitioning the system into zones and conduits.

Defense-in-depth – Interfaced systems

Interfaced systems function like separated systems in that safety-related functions are separated physically from non-safety-related functions (Figure 3). The difference is in interfaced systems; the BPCS elements and the core SIS functions are connected using engineered links with industrial open protocols. Typically, firewalls or other security hardware and software restrict traffic between the BPCS and SIS.

Because the core SIS and extended SIS physically are separated from peripherals, interfaced systems offer adequate protection to meet ISA and NAMUR standards. However, just as in separated systems, SIS hardware and software need to be protected. Users must ensure the core SIS is not compromised via connections to the extended SIS.

To achieve this protection, interfaced systems require that defense-in-depth security layers be duplicated on multiple systems. In some cases, the multiple cybersecurity instances that must be monitored can increase the workload necessary to sustain adequate security. It is also up to the end user to ensure the link between the BPCS and SIS is configured so the system is not exposed to risk.

Defense-in-depth – Integrated systems

Another option for engineering separated systems is integrated SIS (Figure 4). In this approach, the SIS is integrated to the BPCS, but there is a logical and

Figure 4: In an integrated SIS architecture, safety-critical functions logically and physically are separated—still complying with ISA and NAMUR standards—yet located on the same system. This eliminates the need to maintain multiple defense-in-depth designs. Courtesy: Emerson

physical separation between the core SIS and extended SIS. Typically, this separation comes with proprietary protocols using embedded cybersecurity out of the box. This eliminates many of the security risks that come from manually engineering a connection between the SIS and BPCS.

Integrated SIS requires the same levels of defense-in-depth protection as separated systems, but because some of the security layers protect both the BPCS and SIS, an integrated SIS can reduce the time and effort spent monitoring, updating and maintaining security layers. This approach offers protection that goes beyond common security layers. Integrated SIS also has additional and specific security layers designed to protect the core SIS.

Eliminating complicated engineered interfaces between core and extended SIS with an integrated environment can lead to simpler and faster factory acceptance testing (FAT), helping to bring projects online faster and with less rework.

Managing entry points

Carefully considering defense-in-depth layers is critical to delivering a cybersecure SIS, but it's not enough. To ensure adequate security for an SIS network, organizations also must limit entry points into the safety-critical functions and provide mitigations for any risks that impact said entry points.

The more entry points available into an SIS' safety-critical functions, the more opportunities exist for cyber attacks to exploit possible vulnerabilities in the security layers. While it may be possible to adequately defend five entry points against intrusion, it is much easier and less resource-intensive to defend only one.

Entry points – Interfaced systems

NAMUR offers clear guidance for zoned SIS architecture in an interfaced format (Figure 1). In the diagram, the core SIS, extended SIS and control system architecture are isolated properly in their own zones. The engineered connections between architecture elements in the three zones—engineering stations, BPCS, plant information management systems, asset management systems and more—can create multiple potential connection points to the core SIS.

These connection points do not inherently present a security risk; the assumption is they will be secured with adequate defense-in-depth. Each door needs to be secured, potentially resulting in five or more sets of security hardware and software to manage.

Entry points – Integrated systems

Integrated SIS architectures can offer a design that limits entry points. The best integrated safety instrumented systems feature one component acting as a gatekeeper/proxy for all traffic going to and from the safety-critical functions. The result is one entry point that needs to be defended, likely using the same defense-in-depth layers that protect the BPCS and some additional protection layers more specific to the core SIS. Such a design can reduce maintenance and monitoring while providing the same or even greater level of standard SIS separation than other architectures.

There is often an assumption that more physical separation between SIS and BPCS means more inherent security. However, as in the case of air-gapped systems, more physical separation may lead to increased maintenance and monitoring overhead to ensure adequate defense-in-depth. The added overhead limits air-gapping's value for organizations looking to optimize performance and production while trying to achieve cybersecurity standards.

Integrated and interfaced systems can achieve high levels of connectivity, while offering flexibility in implementation of defense-in-depth cybersecurity structures. Because both architectures offer the highest levels of security, implementation teams looking to maintain a defensible SIS over the lifecycle of the system often discover they have more choices for a BPCS and SIS that fit unique organizational goals.

Sergio Diaz *and* ***Alexandre Peixoto*** *are DeltaV product managers, Emerson. Edited by Chris Vavra, production editor, Control Engineering, CFE Media, cvavra@cfemedia.com.*