DeltaV SIS™ and Cybersecurity

Executive Summary

Safety Instrumented Systems (SIS) are designed to keep processes safe, especially during critical situations. With this concept in mind, it is paramount that the SIS components are not taken down due to cyber-threats. The purpose of this white paper is to explain, in detail, the Emerson approach for cybersecurity as well as the built-in security features available within the DeltaV SIS process safety system.

DeltaV SIS can be implemented either as an Integrated Control and Safety System (ICSS) with the DeltaV DCS or as interfaced system with any third-party system. An ICSS delivers faster and easier project execution, greatly simplifies FAT/SAT, reduces commissioning costs and improves operational efficiency. This white paper explains how a combination between product functionality and work practices leads to an SIS that fulfills the expectations, needs, and demands of current security context without sacrificing the benefits delivered by an ICSS. There is a misperception that an ICSS is not as secure as an interfaced SIS. Some people even consider that a completely isolated SIS is the most secure of all the SIS architectures. This paper clarifies that while the SIS architecture selection has some impact in the SIS cybersecurity robustness, the inherent cybersecurity posture of the ICSS itself is the most important protection against cyber-threats. Focusing only on the interface type between SIS and DCS is an oversimplification of the cybersecurity discussion. SIS security should rely on multiple layers of protection. A coordinated cybersecurity approach between SIS and the Basic Process Control System (BPCS) makes an ICSS as defendable or more than an interfaced SIS without such measures in place.

Security threats may come from a variety of sources: unauthorized access, inadvertent virus infection, intentional attacks, and accidental disruption due to equipment malfunction or improper maintenance activities.

A coordinated cybersecurity approach between SIS and BPCS enables proper countermeasures against cybersecurity threats:

- Network segmentation to isolate safety critical components from components not required for execution of the safety function (e.g. separate workstations from logic solvers)
- Multiple layers of protection against unauthorized access, including enforcing physical presence to prevent remote attacks
- Comprehensive approach to prevent inadvertent virus infections
- Automatic removal of maintenance bypasses to prevent both inadvertent or intentional defeat of safety logic
- Validation of messages between BPCS and SIS to reduce the risk of sending invalid messages to the SIS from workstation applications
- A fully integrated control and safety system that is easier to secure

Cybersecurity standards related to industrial control systems are still a work-in-progress. The last section of this white paper provides an overview of these emerging standards as they are also relevant to SIS. Emerson can deliver DeltaV SIS in compliance with these emerging cybersecurity standards with any of the supported SIS architectures.

Table of Contents

Emerson's Approach to Cybersecurity

Emerson's cybersecurity approach aligns with the Defense-in-Depth strategy described in the ISA/IEC 62443 series of standards.

The DeltaV SIS process safety system is comprised of safety logic solvers, workstations, and network components[1]. The built-in security features are customizable, and some are even optional. It is the user's decision whether to implement all or parts of the whole *Defense-in-Depth* strategy based on the level of security required.

The Defense-in-Depth strategy described in the DeltaV Security Manual[2] represents Emerson's approach when deploying DeltaV SIS either as:

- Separate SIS
- Integrated to DeltaV (also known as integrated but separate)
- Interfaced to any BPCS (including DeltaV) when a customer wishes to add a DeltaV SIS to a legacy BPCS, or has requirements for an interfaced SIS solution.

Network segmentation is one of the basic protection mechanisms of Emerson's Defense-in-Depth strategy and for DeltaV SIS this is taken into perspective for all supported safety systems' variations. A basic principle of DeltaV SIS is to isolate the safety-critical components (logic solvers, sensors and final elements) from components that are not necessary for executing the safety function (e.g. SIS engineering station, or SIS HMI).

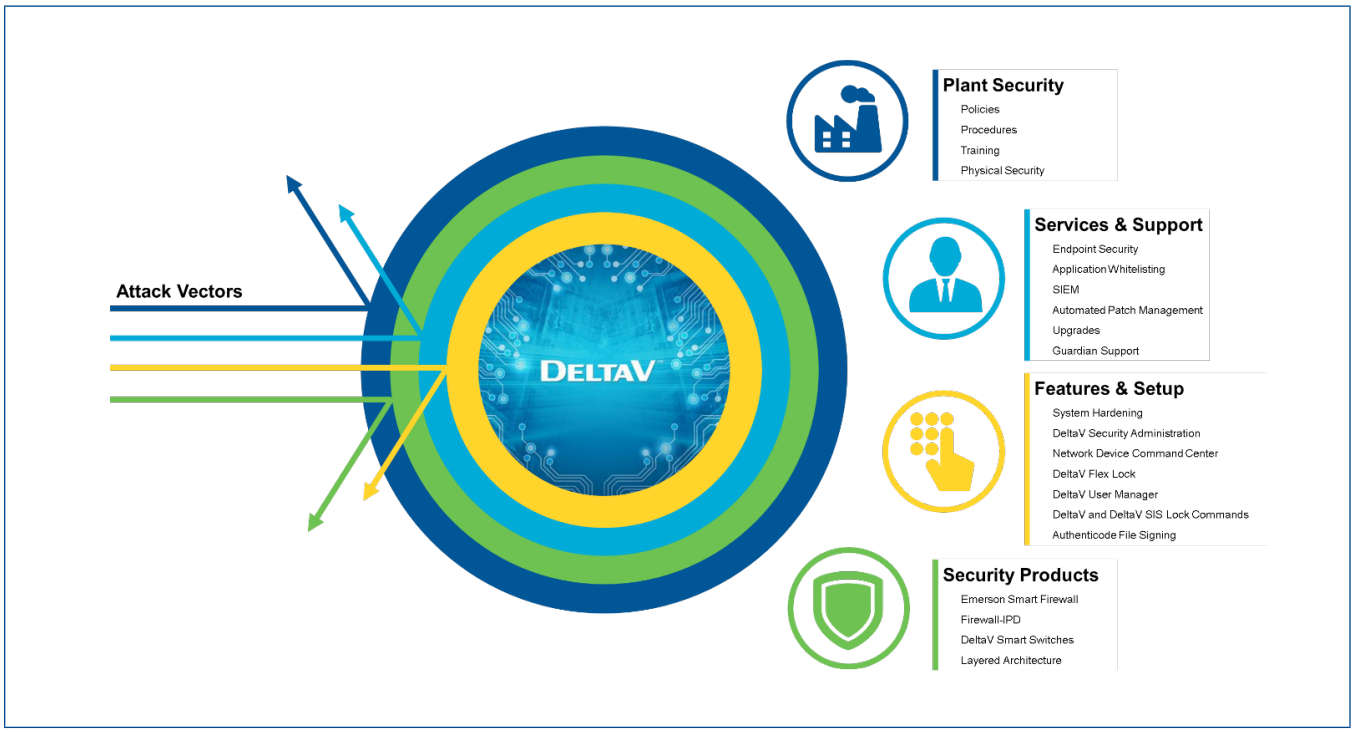

Figure 1 - Emerson's Defense-in-Depth strategy.

DeltaV SIS Architecture Overview

The DeltaV SIS process safety system uses a modular distributed architecture. Modularity brings flexibility and scalability, while distribution reduces single points of failure among other benefits. On the DeltaV SIS distributed architecture, each CHARMs Smart Logic Solver (CSLS) is a container for a reduced number of Safety Instrumented Functions (SIF). This is very different from the traditional centralized approach where hundreds of SIFs are all placed in a single safety PLC. Modularity and distribution also helps from a cybersecurity point of view, as will be explained later.

Safety rated communication among logic solvers occurs on dedicated safety networks with no direct connection to unauthorized nodes. All non-safety rated communications go through an isolation node that securely allows DeltaV SIS to exchange data with the BPCS (either a DeltaV system or a third-party BPCS).

The local safety network (LSN) is the communication backbone of the DeltaV SIS process safety system. The LSN is a standard Ethernet network dedicated to the DeltaV SIS that enables communication among CSLSs on the same LSN, as well as the CSLSs and the SZ Controller. A global safety network (GSN) enables safety-rated communication among CSLSs on different LSNs.

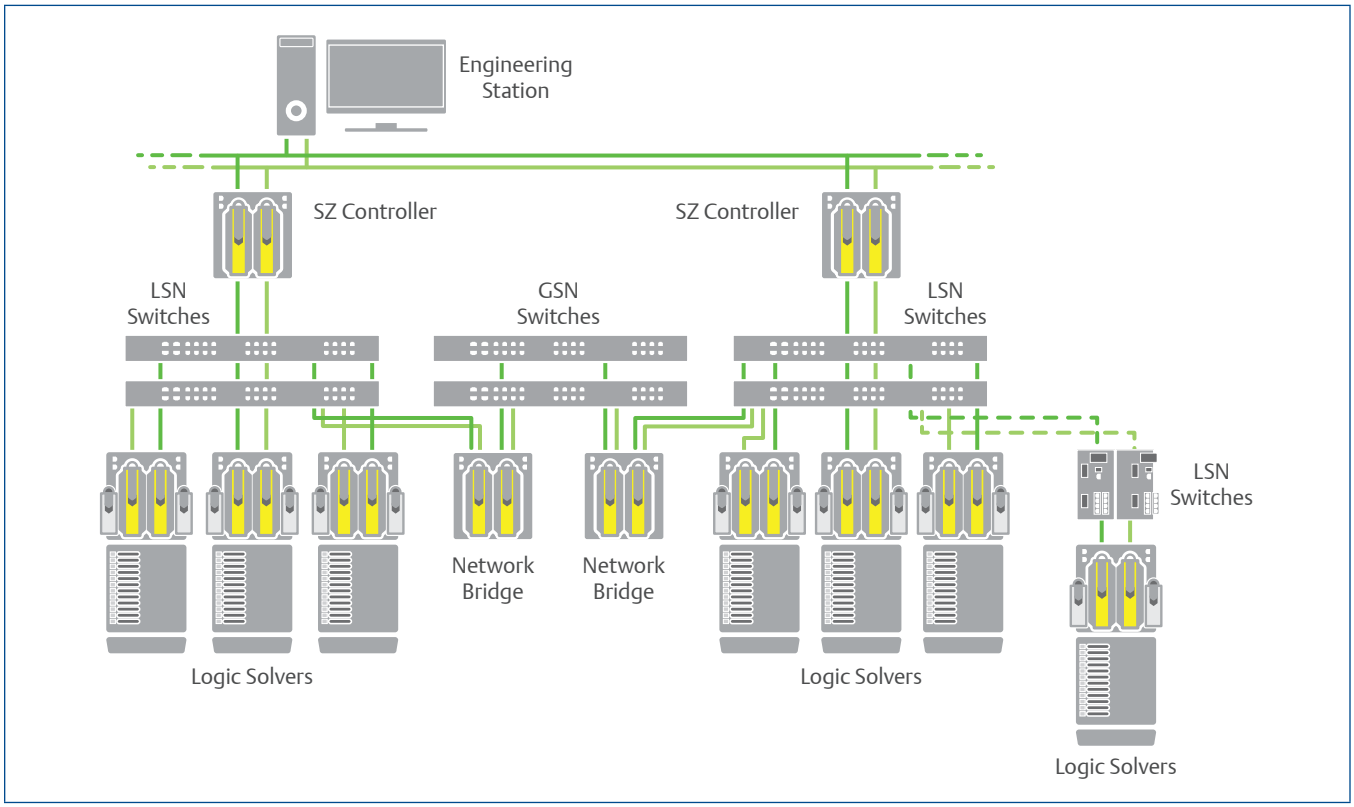

Figure 2 - DeltaV SIS safety network architecture diagram.

Architecture Options for Safety Instrumented Systems

While SIS can be deployed completely separate from the BPCS, generally the SIS has some levels of connectivity to the BPCS. The ARC Advisory Group 2016 report, *Process Safety Systems Global Market Research Study* provides three classifications for the SIS in terms of the connectivity with the BPCS:

- **Interfaced:** The SIS is interfaced to the BPCS using standard protocols such as Modbus TCP or OPC.
- **Integrated but separate:** The SIS can share the same engineering tools and operator environment with the BPCS, but the safety logic runs on separate hardware.
- **Common:** This approach uses common hardware for both SIS and BPCS.

DeltaV SIS can be deployed either as a completely separate (no connection to BPCS), an interfaced, or an integrated (a.k.a. “integrated but separate”) SIS. Emerson does not use common or shared logic solver hardware for SIS and BPCS which means that a common architecture is not utilized. This white paper focuses on the cybersecurity aspects for each architecture with emphasis on the integrated architecture.

Completely Separate SIS

In this architecture, the SIS does not share data with the BPCS and it is either completely isolated from the BPCS or deployed without a BPCS. It can have either a permanent engineering station, or be configured and maintained using a laptop computer. It can have a local Human-Machine Interface (HMI) or not. While complete isolation might be perceived as the ultimate security option, the reality is that it is still subjected to cyber-threats. Removable media access is a potential source for virus infections, and the laptop needs to be maintained up-to-date to minimize zero-day vulnerability exploitation. Isolation itself does not guarantee security. Monitoring must also be in place. Since most users require some type of data exchange between the SIS and the BPCS, this architecture is declining in use. Still, DeltaV SIS can be deployed as a completely separate SIS and still provide the means to maintain an appropriate level of security, if this is required.

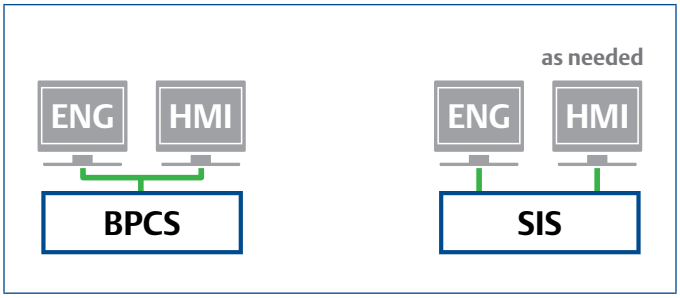

Figure 3 - Separate Safety Instrumented System.

Interfaced SIS

In the interfaced architecture, there is some integration between the SIS and the BPCS, and the most common protocols used are Modbus (RTU or TCP) and OPC. This communication is restricted to operations only. Typically, one vendor provides the SIS and another the BPCS, but the same vendor could provide both. This architecture tends to be perceived as more secure than an integrated architecture, and one of the assumptions is that an attacker would need to compromise multiple systems to affect the SIS instead of just one. However, depending on how the SIS is interfaced, an attacker would not even need to affect the SIS at all to perform a cyber-attack.

For example, if the SIS does not have a solid management of bypasses/overrides and it simply relies on the BPCS configuration for setting/removing those bypasses, then a malicious attacker would only need to set multiple bypasses to disable the SIS. Once the SIS is disabled due to the presence of maintenance bypasses, then the attacker just needs to create a demand or wait for a demand to occur to affect the process safety. The key SIS features to avoid this type of scenario are the ability to prevent, at the logic solver level, multiple bypasses and even the ability to automatically remove bypasses. Since this functionality is inherent to the DeltaV SIS logic solver, it is available for both interfaced and integrated architectures.

The design of the Modbus interface also plays a role in an interfaced architecture. DeltaV SIS does not use Modbus directly and writes from a Modbus master are not allowed. The logic solvers pull information from Modbus registers explicitly configured by the user. Since there is no predefined table, the user will need to download the logic solver to modify how the information pulled via Modbus is being used. Preventing authorized downloads provides a means to prevent modification on the information being exchanged via Modbus.

The architecture selection alone, does not make an SIS more defendable, but a comprehensive approach to security would have a better chance to succeed on this strategy.

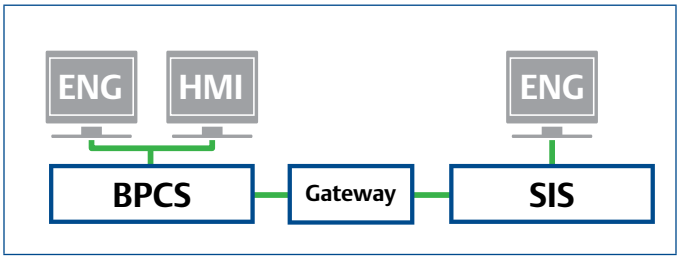

Figure 4 - Interfaced Safety Instrumented System.

An interfaced SIS system must be properly protected against cybersecurity threats, especially related to system access. The use of an HMI for bypass/overrides operations, the need to gather system records for compliance purposes, the desire to use system and device diagnostics to improve safety and availability, as well as the initiatives for digital transformation all increase the need for interacting with the SIS.

Integrated-but-Separate SIS

In this architecture, the SIS shares engineering tools and the operator environment with the BPCS. An integrated SIS delivers major benefits over an interfaced SIS. During the engineering and implementation phase, an ICSS delivers faster and easier project execution by using a common engineering environment, eliminating data mapping and handshaking logic. All of these features greatly simplify integrated FAT/SAT. Commissioning costs are optimized by reducing coordination among different teams. Operational benefits come from integrated diagnostics. For example, HART device alerts can be easily sent to maintenance personnel as early warnings of potential issues. For final control elements, non-disruptive partial stroke testing can be initiated directly from the operator graphics. An ICSS can provide the appropriate level of cybersecurity protection by separation of functions and segmentation of networks. Full integration is rather a cybersecurity strength rather than a liability since it does not rely on engineered interfaces between BPCS and SIS.

> *"While all three integration approaches have their merits, ARC believes the integrated-but-separate approach will ultimately become the architecture of choice for many end users, since it offers the most potential to minimize common cybersecurity threats between the systems"*
>
> *Source: ARC 2016 report for Process Safety Systems Global Market Research Study*

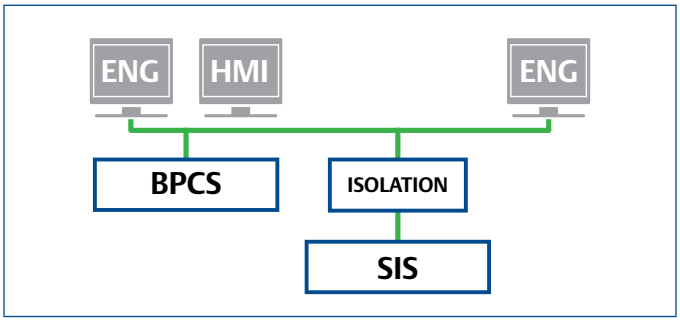

Figure 5 - Integrated Safety Instrumented System.

Instead of duplicating cybersecurity protections for SIS, an integrated approach uses the DCS as integrated but separate cyber-protection layers for the SIS. A simplistic view of integrated approach leads to the incorrect conclusion that compromising the DCS automatically compromises the SIS when the reality is that both SIS and BPCS have their own cyber-protection layers that work together to provide a more defendable system. The advantage of this approach is a cybersecurity strategy that is easier to maintain. Cybersecurity protections are not something done once. Those protections need to be maintained overtime.

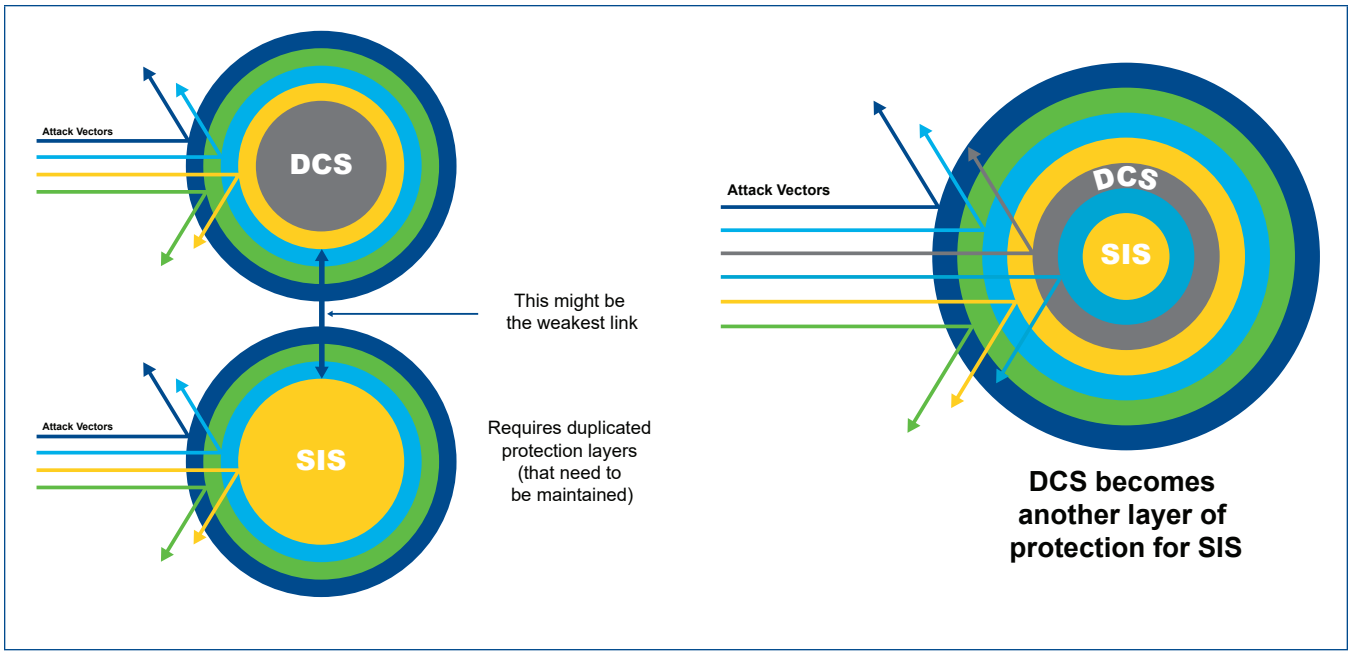

Figure 6 – Protections in both Interfaced and Integrated Systems

Cybersecurity Threats to SIS and Countermeasures

Security threats (aka. cyber-threats) are any cybersecurity related action that can generate, or lead to, an adverse impact on a system. Threats can be intentional or accidental and may come from a variety of sources. Cybersecurity threats can be classified in different ways. For this white paper, cybersecurity threats were classified in four types based on the white paper[3] from the *Cyber Security Working Group* from the 61508 Association (a cross-industry group of organizations with a common interest in functional safety):

1. Unauthorized access including:
   a. Trusted insider.
   b. Competitors (interested in stealing intellectual property or commercial intelligence rather than process disruption).
   c. Casual hacker whose only purpose is to try to break in without intending harm.
2. Inadvertent virus infection (e.g. through infected removable storage devices).
3. Intentional attacks. While intentional attacks could include unauthorized access, this category includes other types of threats such as a Denial-of-Service (DoS) attacks targeting plant operations disruption.
   a. Social activists (“hacktivists”) who perceive that a company does not operate in accordance with their perspective.
   b. Malicious attacker including terrorists or state-sponsored attackers.
4. Accidental disruption due to equipment malfunction or improper maintenance activities.

As indicated in both Figure 1 and Figure 6, each layer of the Defense-in-Depth strategy represents a list of protection mechanisms that together help mitigate the cyber-threats that could potentially disrupt the DeltaV system's operation. In the next sections of this white paper, the cybersecurity features and functions in Table 1 will be described; some of them are optional and some must be enabled/configured to deliver the protection that is expected. Please consult with your local Emerson sales office for information on how to implement these features in your DeltaV system.

Cybersecurity Threat	Countermeasures
Unauthorized Access	■ User account management ■ Two-factor authentication
Attacks from a trusted insider	■ Authorization from other users before critical actions can be performed ■ Notification and information awareness ■ User account management
Remote attacker who has compromised user credentials	Enforcing physical presence before allowing potentially disruptive actions: ■ Lock functionality paired with intrusion protection (Firewall-IPD) ■ Lock functionality paired with built-in key switch
Inadvertent virus infection	■ Control access to removable media ■ Antivirus and application whitelisting ■ Patch management
Cybersecurity Threat	**Countermeasures**
Disabling safety system by preventing system access to remove bypasses	■ Automatic removal of bypasses
Malicious logic solver firmware updates	■ Enforcing physical presence for firmware updates
Invalid (corrupted) messages	■ Messages validation (secure write mechanism)

Table 1 - Countermeasures summary

Unauthorized Access

Access to BPCS and SIS is based on the system privileges set at the operating system and DeltaV system levels. Unauthorized access happens when the permitted ways to use the system are somehow bypassed, brute-forced, wrongly manipulated, etc. Unauthorized access can be intentional or not, but it is the simplest approach attackers use to compromise systems especially when remote connectivity is allowed.

Preventing unauthorized access is a key element to maintain security. The DeltaV SIS provides different mechanisms to prevent unauthorized users from accessing the system.

User Accounts Management

The first layer of protection against unauthorized access is user accounts management. Security information in DeltaV systems is defined in terms of users, groups, locks, keys, and areas (scope for user privileges):

- Locks prevent users from either changing specific information or executing certain actions within the system.
- Locked objects or locked functions can only be accessed by users who have the appropriate key.
- DeltaV systems segregate BPCS and SIS privileges by specific SIS locks and the associated SIS keys.

Assigning the correct privileges to the right users is the first step. The second step is to have sufficient management of user accounts.

The DeltaV system also requires user authentication for monitoring and configuration of DeltaV SIS. Emerson recommends that ICSS systems are deployed in a Domain environment for added security and simplified user management. The Windows domain controller functionality can be decoupled from the DeltaV Engineering functionality which provide greater separation of roles as well as additional network segmentation. For more details consult the Independent DeltaV Domain Controller whitepaper.[13]

Two-factor Authentication

Since user passwords can be discovered, the additional protection of two-factor authentication is available when required. Two-factor authentication is based on smart cards that can be applied to DeltaV systems[4]. This type of solution provides an extra layer of protection for the user's authentication since it is not only based on usernames and passwords. Instead, it requires the user to have a pre-configured smart card (first level of authentication where the loaded digital certificate represents the username for the system), and a user's PIN – Personal Identification Number (second level of authentication based on a sequence of numbers usually less complex than a password). Without both authentication levels/factors, the user cannot be authenticated to the system.

Using Two-Factor Authentication to Restrict SIS Users to Specific Workstations

With the proper implementation, two-factor authentication can be used to restrict SIS users to specific workstations. All SIS actions including configuration and operation (e.g. setting a maintenance bypass) will require SIS users to log into specific workstations in the DeltaV network defined as SIS workstations. With this approach the following separation of roles will be enforced:

- SIS users can only login to specific workstations (aka SIS workstations). An SIS user cannot login to a non-SIS workstation.
- DCS users can only login to non-SIS workstations. A DCS user cannot login to an SIS workstation
- The separation of roles by workstations and users is illustrated in figure 7.

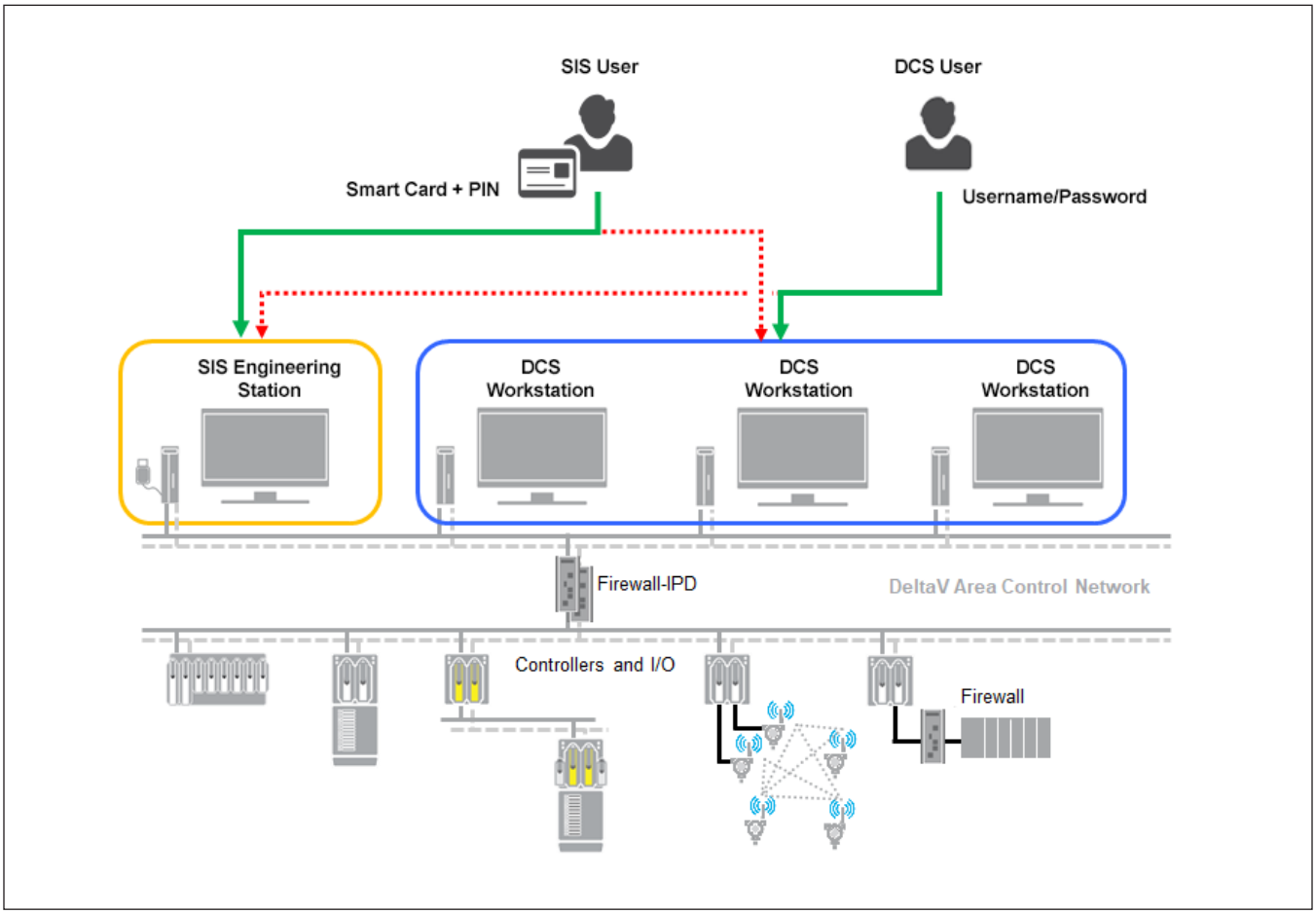

Figure 7 – Implementation of Two-Factor Authentication for Separation of SIS Roles.

In this example, all SIS users are required to have a smart card and all SIS workstations must have a smart card reader. Since DCS workstations will not have a smart card reader in this case, SIS users cannot login to those workstations. In the other hand, DCS users cannot login to SIS workstations by means of security policies since they are not required to have smart cards to log in. On the SIS workstations, the DeltaV authentication should enforce/require smart cards as well for added protection.

Smart cards provide an additional level of access authorization in addition to the DeltaV privileges that further separate SIS and DCS roles by default in any DeltaV system.

Note: The recommendation is to use two-factor authentication applied to all workstations and servers in a system so that the protection is applied to all users who have access to the DeltaV system. Partial two-factor authentication, as described in this section of the white paper, is a best effort to segment DCS and SIS functions given to specific workstations in the system by means of access authorization that is comprised of smart cards where applicable. Within a DeltaV system, there are three main types of workstations: ProfessionalPLUS, Application and Operator stations, and the system privileges on these stations are given to each user by means of licenses and authentication. By no means, this engineered solution using two-factor authentication is meant to change the DeltaV system functionality within DeltaV Explorer and other tools by creating, somehow, a new station type called "SIS workstation". The term SIS workstations is used in this section to describe a regular DeltaV workstations where users with the proper privileges can perform SIS tasks. The term DCS workstation is used to describe a regular DeltaV workstation where SIS tasks are prevented since SIS users cannot login to them.

Segregation of Administrative Privileges

The use of Independent DeltaV Domain Controllers enables further segregation of duties. Windows administrators and DeltaV administrators can be much easily decoupled for increased security in a much simpler manner when the Independent DeltaV Domain Controller functionality (DeltaV v14.3 and higher) is implemented in your system.

Preventing Attacks from Trusted Insider

Preventing attacks from a trusted insider is quite challenging because the insider may have been trusted with higher privileges in the system, and therefore may be able to perform critical tasks that can affect the overall system's operations. DeltaV SIS records all user actions in event logs and while this could discourage insider misbehavior, DeltaV SIS has some additional mechanisms to provide enough checks and balances before certain tasks are performed.

One of the most disruptive actions a trusted insider could perform is changing the safety logic. In DeltaV SIS this would require a logic solver download. Each DeltaV SIS module (modular component for SIS configuration typically associated to one or more SIFs) could be associated with a SIL level (up to SIL3). Optionally, for each SIL level it is possible to assign up to five approvers (signers) who must approve the logic before a SIS module with an assigned SIL can be downloaded. When this functionality is enabled, all signers must approve the module before it can be downloaded (SIS modules with no assigned SIL do not require any approvals). Changing the offline configuration of a previously authorized SIS module changes the module's authorization state to Not Authorized, and only authorized modules can be downloaded.

Another disruptive action a trusted insider could attempt is to bypass the safety system. Some of the mechanisms within DeltaV SIS to mitigate this type of action are:

- Providing an alarm whenever a bypass is active so other operators are aware of the situation.
- Enforcing not more than one bypass per voter, SIF, SIS module or units. DeltaV SIS has out-of-the-box functionality to enforce that only one bypass is present per function block and it is possible to add logic to enforce the same at a higher level.
- Requiring a bypass permit that could only be set by a user with higher privileges.

Preventing Access from Trusted Insider

When temporary users no longer need access to the control system, or when individuals are terminated from the companies, their respective control system user accounts must be immediately disabled. Intentional unauthorized access to the control system on those specific circumstances can be interpreted as targeted cyber-threats and must be prevented.

There should be controls to immediately disable user accounts for recently terminated employees including any type of remote access (Emerson does not recommend remote access to SIS Engineering Stations).

Enforcing Physical Presence Before Allowing Potentially Disruptive Actions

One of the best lines of defense to prevent attacks that target credential theft is the enforcement of physical presence (something that a remote user could not have). DeltaV SIS provides different mechanisms to enforce physical presence before certain SIS changes are performed as described below:

DeltaV SIS Lock Functionality for Logic Solvers

Configuration manipulation is critical on SIS and the DeltaV SIS Smart Logic Solvers are provided with a built-in write protection. When enabled, the write protection mechanism (lock functionality) will not allow users to change the configuration that is running within the SLS1508 or the CHARM Smart Logic Solver (CSLS), if the logic solvers are locked.

When a logic solver is locked, the system prevents the following operations:

- Entering debug mode which prevents overrides
- Decommissioning the logic solvers
- Downloading the logic solvers
- Issuing Diagnostic Commands:
  - Manual Switchover
  - Force Reset on Active
  - Force Reset on Standby
- Issuing HART write commands

Starting with DeltaV v14, certain function block parameters in the CSLS can only be modified on-line if the CSLS is unlocked. There are three levels of access for user-defined parameters: writeable, not writeable, or only writeable when unlocked. Parameters classified as not writeable can only be modified via a CSLS download

Distributing the application program in multiple logic solvers enables the ability to only unlock a reduced section of the application program which reduces exposure during authorized changes. In a centralized approach, where a single hardware key protects a large centralized logic solver, the whole application program would need to be unprotected before any modification is performed. In a distributed approach where the lock is applied to individual logic solvers, only the specific logic solver being modified needs to be unlocked, leaving the rest of the logic solver protected.

For additional protection, it is possible to enforce physical presence before a user is able to unlock a logic solver. When physical presence is enforced, unlocking a logic solver becomes a two-step process. First, a user at site needs to set the system to allow an unlock command. Second, a user with proper privileges within the engineering tools needs to send an unlock command. This two-step approach has the following advantages:

- A trusted insider having physical presence but insufficient privileges will not be able to unlock a logic solver.
- A remote attacker without physical presence will not be able unlock the logic solver even if system credentials were compromised.
- It is possible to automatically lock the logic solver via software. If a hardware key is the only mechanism for locking a logic solver, as in some centralized logic logic solvers, the user could easily forget to return the key to the proper position.

DeltaV v14 introduced features to minimize the probability of leaving a logic solver unlocked. The user can send a timed unlock command so the logic solver is automatically locked after a user-defined time period.

There are two mechansims to enforce physical presence before an unlock command is sent to logic solvers:

1) Using a intrusion protection device (IPD)

2) Using a hardware key either on the logic solver, the SZ controller or both

Enforcing physical presence using Intrusion Protection Device

Privileged users can send the SIS-unlock command from DeltaV Explorer, and to further protect this mechanism, the DeltaV Firewall-IPD can be added to the network. The Firewall-IPD (formerly DeltaV SIS-IPD) is a firewall that inhibits the SIS-unlock command from reaching the SLS1508 or CSLS. The Firewall-IPD can only be put in bypass when the user accesses its local pushbutton (or the discrete input) – requiring physical local presence. It is only possible to unlock the SLS1508 or CSLS if the Firewall-IPD is in bypass mode.

In DeltaV version 13.3.1, an additional lock command was introduced to protect DeltaV embedded nodes which can be locked to prevent unauthorized downloads, decommissioning, access for troubleshooting, and firmware upgrades. This new feature applies to all DeltaV embedded nodes including the SZ Controller. Similarly, the Firewall-IPD must be put in bypass mode to allow the new unlock command to reach the specific embedded node being unlocked.

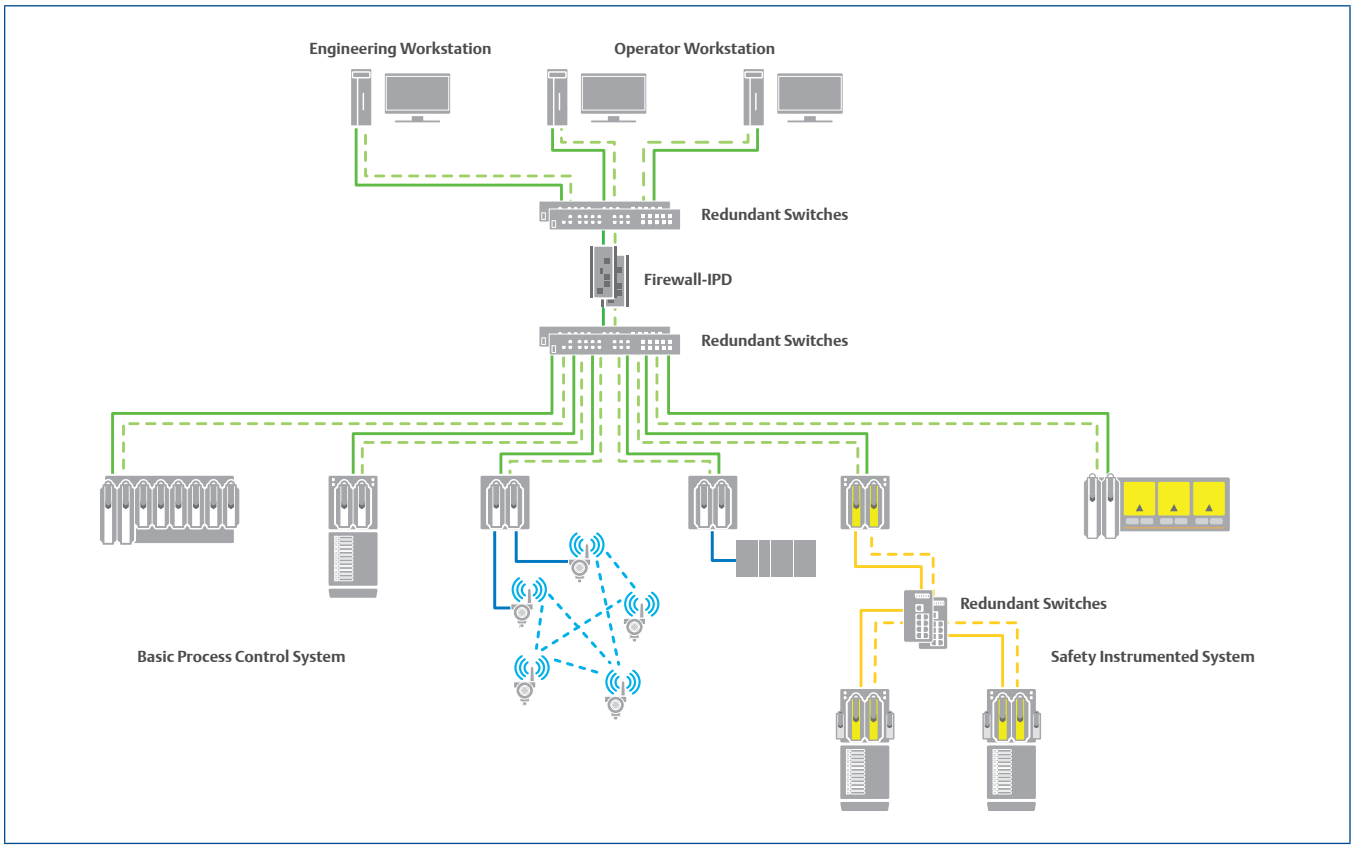

Figure 8 - Example illustrating the Firewall-IPD in the ACN.

Enforcing Physical Presence Via a Key Switch

The CSLS has a physical key that prevents unlocking the CSLS from the engineering tools unless the physical key is in the allowed position. The use of the physical key can be enabled or disabled on a logic solver by logic solver basis, and it is not possible to disable the key remotely (this must be done locally).

The SZ controller also has a physical key. Starting in DeltaV v14, the SZ controller key can be enabled to prevent unlocking of any CSLS within the local safety network. Enabling the physical key on the SZ controller requires the use of specific communication ports. Once enabled, there is no way to disable the use of the physical key without replacing the communication ports (which requires physical presence). To minimize the probability of leaving the physical key switch in the unprotected position, DeltaV v14 introduced the feature of single unlock behavior. After a executing a defined sequence at the physical key switch, the single unlock behavior is engaged so user can a unlock command even if the hardware key is on the protected position.

Inadvertent Virus Infection

Transferring files to control system workstations using removable media or network shares increases the chance of an inadvertent virus infection. Users performing routine activities may not even know they are spreading a virus across the system by performing these and other actions without following security best practices.

Inbound traffic to the BPCS and SIS should be monitored all times. Misconfigured firewalls can allow injection of malware into the memory of running processes. System administrators should understand the reason and consequences of any firewall rules change.

The most effective methods to prevent an inadvertent virus infection is to control the use of removable media, have antivirus programs installed and effectively scanning the system, and to implement application whitelisting. All these protections should be running on all workstations and servers of the BPCS and SIS system.

Removable Media Access Control

Authenticated DeltaV users (including the non-administrative ones) have access to most of the connected computer's peripherals (e.g. mouse, keyboard, hard drives, USB ports, etc.), and therefore it is crucial to lockdown the workstations and servers to prevent access to unauthorized equipment.

The Department of Homeland Security (ICS-CERT division) has stated: "USB thumb drives represent a significant malware attack vector for control system networks" (Department of Homeland Security – USA, ICS-CERT, USB Usage, 2010)[5]. The ICS-CERT also explains that attacks using removable media have taken four major forms: data theft, social engineering, virus infection, and virus spread. The user's organization must have policies and procedures to govern this vulnerability, and if it decides to forbid the use of removable media, security policy settings must be applied to the control system.

The Knowledge Base Article NK-1600-0336, available on Emerson's Guardian Support Portal[6], helps users to manage removable media on DeltaV systems. Emerson recommends that all removable media access is disabled once the system is deployed, and this implementation can be centrally managed when DeltaV systems are deployed in a Domain environment – alternatively this can be implemented on a per workstation basis if in workgroup environments.

If removable media use is required, Emerson strongly recommends additional protections such as the Symantec Industrial Control System Protection (ICSP) which is comprised of an independent scanner station and an agent (this last one installed on every workstation and server connected to the control system). This solution allows the user to verify that the removable media is not infected prior to its use on DeltaV workstations and servers. Additional details on the Symantec ICSP solution can be found on the white paper *Symantec ICSP Support for DeltaV Systems*[7].

Antivirus and Whitelisting

Per the Department of Homeland Security's *Seven Steps to Effectively Defend Industrial Control Systems* (issued by the National Cybersecurity and Communications Integration Center – NCCIC in 2016), 38% of the cybersecurity incidents reported to the ICS-CERT in 2014-2015 could have been prevented by application whitelisting solutions.

Emerson recommends a two-step approach for endpoint protection. Whitelisting[8] and antivirus (blacklisting) should be used together to make sure only approved applications can run (avoid zero-day events) and if known files are infected, they can still be scanned and either cleaned or quarantined. Application whitelisting prevents unauthorized programs from running or even being accessed on whitelisted systems, hence preventing unknown malware from spreading in a protected system. The *white list* is based on security policies that set exceptions for each application that can run – for a more secure approach, authorized applications should have Authenticode signed files.

The combined scenario based on anti-virus and application whitelisting provides a good protection mechanism against cyber-threats that target file manipulation via malware infection[9].

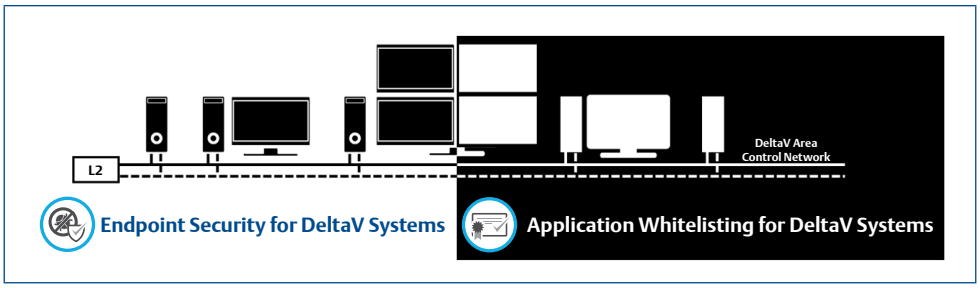

Figure 9 - Blacklisting (antivirus) and Whitelisting service offerings for DeltaV systems.

Intentional Attacks

Intentional attacks have different motivations. Social activists will most likely target the safety system to safely shut down the operation of the plant, but not with the purpose of disabling the safety system, which could lead to serious environmental or community impact. On the other hand, terrorists or state-sponsored attackers will not be interested in just triggering a safe shutdown but disabling the safety system so the physical asset is not properly protected against the consequences of process upsets. Since there is typically no intellectual property involved in SIS configuration, intellectual property is not a motivation for infiltrating into the SIS.

Malicious Attacks

This section explains attack scenarios from a malicious hacker, not necessarily terrorists or state-sponsored attackers.

Disabling the safety system by preventing system access via Denial-of-Service (DoS) attacks

A question expressed by users is, “What would be the impact on the safety system if a threat such as a DoS attack is performed, removing the ability to access the system from the engineering workstations?” They also ask if this could result in a dangerous condition. A scenario discussed in some forums is related to removing a bypass or an override. For example, if a value was forced or overridden prior to the loss of service of the engineering station. In some systems, it may be impossible to remove the forced or overridden value without the SIS engineering station. DeltaV SIS provides functionality to avoid this type of scenario by allowing the automatic removal of bypasses after a specified time. When properly configured, the bypass will be removed even if users cannot access the SIS engineering workstation.

Manipulating Logic Solver firmware

Manipulated firmware can compromise control and safety systems, and this type of scenario can occur if the firmware files are not protected within the vendor’s support portal or they can be accessed by unauthorized users within the systems. Control systems should also have protection mechanisms to only allow secure firmware upgrades.

Countermeasures to this threat may include firmware file digital signing, secure file transfer from vendor’s portal to the control system, authenticated file transfer to the embedded nodes, and other automated and/or manual procedures.

DeltaV embedded nodes can be locked (version 13.3.1 and higher) to prevent unauthorized firmware upgrades. Physical presence can be required to unlock the nodes to only allow firmware upgrades when authorized personnel are aware of the procedure. DeltaV SIS does not allow on-line firmware upgrades unless a user physically replaces the standby logic solver card. This also prevents manipulation of firmware by a remote attacker.

Moreover, the DeltaV Controller Upgrade Utility is only accessible to users with high privileges set during account setup. DeltaV system administrators need to provide the correct DeltaV keys to the users to allow them to perform embedded node firmware upgrades.

Accidental Disruption Due to Testing or Equipment Malfunction

An example of disruption due to equipment malfunction would happen if invalid (corrupted) messages are sent to the safety system from some workstation applications. DeltaV SIS provides a mechanism to validate messages sent to logic solvers.

Secure Write Mechanism

The DeltaV SIS Secure Write Mechanism (TÜV-certified) provides validation of messages. The purpose of the Secure Write Mechanism is to substantially reduce the risk of sending an invalid message to the safety system from workstation applications. Secure writes are the only way that a user can send write requests from workstations to SIS modules and Logic Solvers.

The following are functions of the Secure Write Mechanism:

- Security privilege validation to make any changes.
- Confirmation dialogues are provided to allow the user to verify the change request (the user must confirm the secure write within 30 seconds of the original request).
- Corrupted messages check.
- Message delivery confirmation to the intended recipient.
- Change prevention caused by spurious messages.

Five DeltaV applications (DeltaV Explorer, DeltaV Live, DeltaV Operate, Diagnostics, and Control Studio) can use the Secure Write Mechanism. No other applications, or communications such as OPC, can use the Secure Write Mechanism. Secure writes are not applicable to DeltaV controllers or BPCS modules.

Providing an equivalent mechanism to Secure Write on an Interfaced SIS, using Modbus protocol, would require extensive engineering work. This is a great example on how an integrated control and safety system could be more secure than an interfaced SIS with different vendors for SIS and BPCS.

Cybersecurity Standards

Emerson's vision statement regarding the cybersecurity of DeltaV systems is to achieve full compliance with the ISA/IEC 62443 series of standards[10]. There are available accreditation bodies and certification programs that can be used to demonstrate how much a vendor's site or control system products comply with related ISA/IEC 62443 standards. A good example is the ISASecure certification programs provided by the ISA Security Compliance Institute (ISCI)[11]:

- Vendor's development practices (ISASecure Security Development Lifecycle Assurance, aka. SDLA – based on the ISA/IEC 62443-4-1 standard),
- Embedded devices security (ISASecure Embedded Devices Security Assurance, aka. EDSA – based on the ISA/IEC 62443-4-2 and the ISA/IEC 62443-4-1 standards),
- Control systems security (ISASecure System Security Assurance, aka. SSA – based on the ISA/IEC 62443-3-3 and the ISA/IEC 62443-4-1 standards).

The IECEE (IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components) provides security practices certification for vendors, engineering companies and integrators based on the ISA/IEC 62443-2-4 standard. There are other third-party accredited parties that issue "62443-based" certifications based on their own private schemes.

Emerson development sites in Austin, TX – USA and Manila – Philippines are ISASecure SDLA Level 1 certified, meaning that the development processes have been adapted to comply with the ISA/IEC 62443-4-1 standard to develop code for DeltaV, DeltaV SIS and AMS Device Manager products. And for v14.3 and higher, DeltaV systems are now ISASecure SSA Level 1 certified, meaning that the DeltaV and DeltaV SIS platforms are attested products that can be used to deploy a control system architecture that can be certified following the security best practices documented in the ISA/IEC 62443-3-3 standard.

Emerson can provide implementation services by personnel who have security knowledge and who follow security specific procedures when engineering your system to comply with the requirements of the security standard. To take advantage of the security standard compliance the system implementation requires that you, the asset owner work with Emerson or its partners to develop the project scope of work to determine how the security capabilities will be implemented to meet the specific security policies the company or site are looking for.

For additional information please refer to the FAQ: *ISASecure SSA Certification for DeltaV and DeltaV SIS* available online.

DeltaV SIS supports the integrated as well as the interfaced SIS architectures, and both are aligned with the concept of zones and conduits detailed in the ISA/IEC 62443 series of standards. The below figure is based on the ISA/IEC 62443-1-1 standard showing the System-Under-Consideration (SUT) with the zones and conduits highlighted. As stated inISA 62443-3-2 standard "…safety-critical assets shall be grouped into zones that are logically or physically separated from zones with non-safety critical assets…". DeltaV SIS restricts the SIS zone to the safety-critical components that are required to execute the safety function (i.e. logic solver, sensors and final elements). Components that are not necessary for the safety function (e.g. engineering station) are outside of the safety-critical SIS zone. There are absolutely no workstations allowed in the safety network, as opposed with other common architectures in the market. This approach reduces the number of connections to the safety-critical SIS zone, effectively reducing exposure to cybersecurity threats.

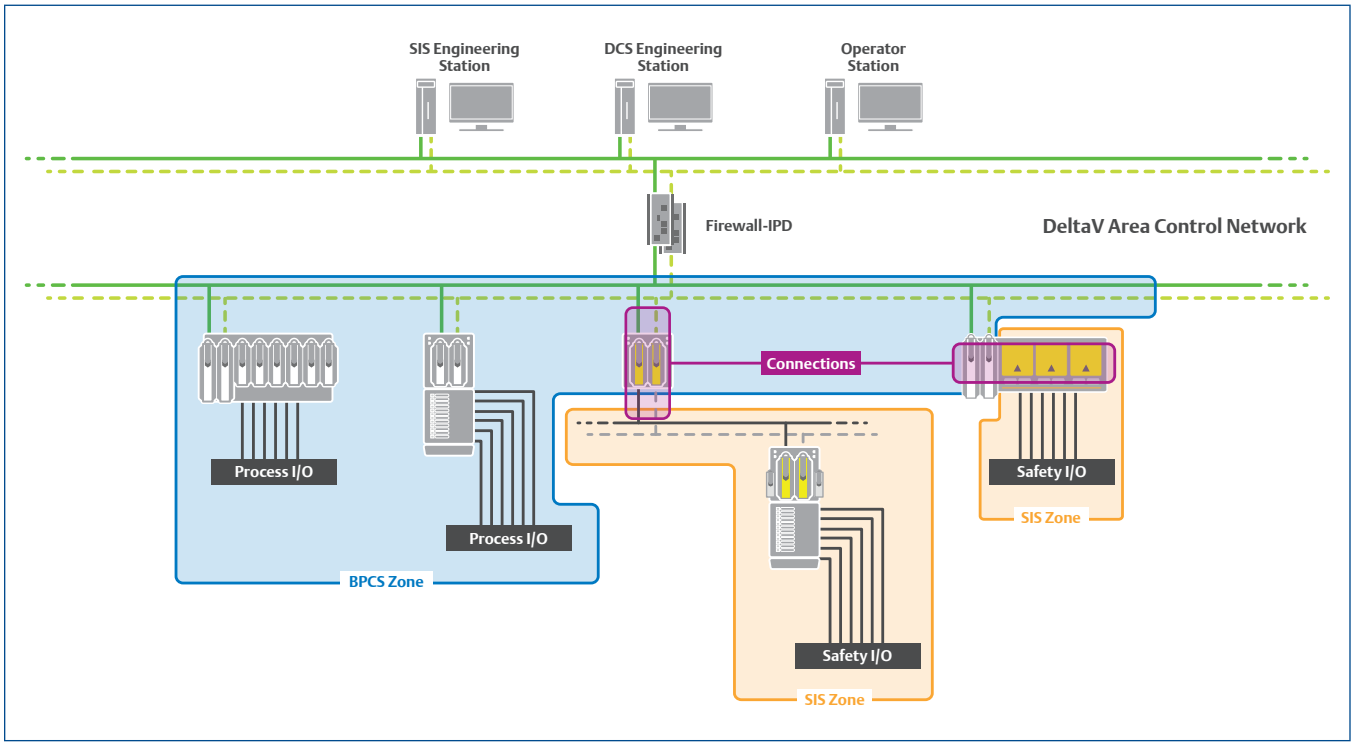

Figure 10 - Integrated DeltaV SIS Architecture.

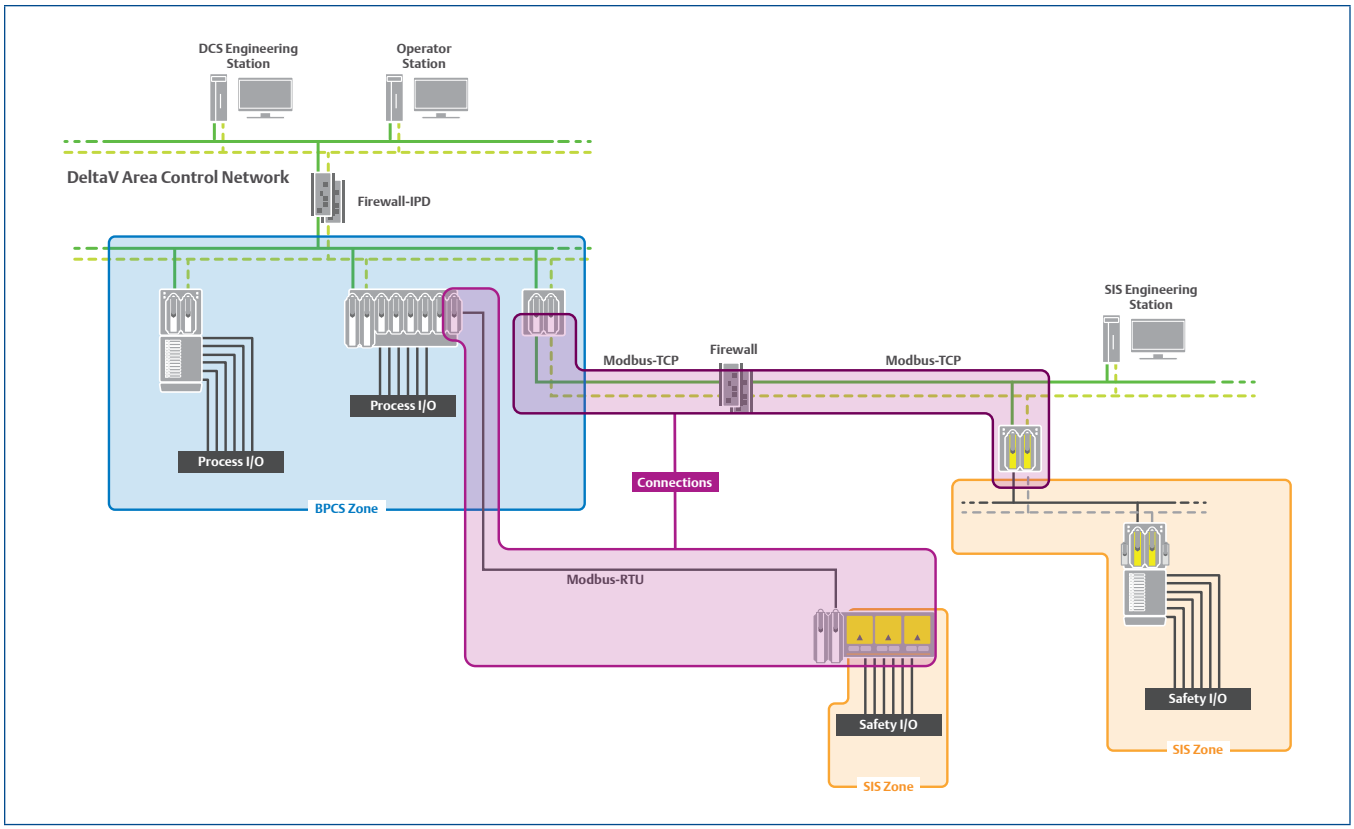

Figure 11 - Interfaced DeltaV SIS Architecture.

Achilles Communications Certification

Another internationally recognized certification is Achilles Communication Certification. “Designed to assess the network robustness of industrial devices and certify that they meet a comprehensive set of requirements. It provides device manufacturers with an independently verified result to communicate their product security to customers, while providing the operators of control systems with the most complete, accurate, and trustworthy information possible about the network resilience of their deployed products.”[12]

There are two levels for the communications certification. Level 1 is an established industry benchmark for industrial control system equipment robustness. Level 2 is an enhanced version with additional tests and tighter success criteria.

Devices subjected to Achilles Communication Certification need to have a connection to external networks (external reference or entry point). Therefore, for DeltaV SIS with Electronic Marshalling, only the SZ Controller is subjected to Achilles Communications Certification. For DeltaV v12, the SZ Controller is Achilles Level 1 certified. For DeltaV v13.3.1 and higher, the SZ Controller is Achilles Level 2 certified. Similarly, the SLS1508 is not subjected to Achilles Communications Certification as it has no direct network connection. Only the controller (e.g. MX controller) which communicates directly to the SLS1508 through a proprietary bus interface is Achilles certified.

Conclusions

Protection against cyber-threats on SIS should not depend solely on architecture considerations. An interfaced SIS is not more defendable just because it is interfaced. Moreover, and not all integrated SISs are the same. Comprehensive built-in security features on the SIS are the foundation for the implementation of security practices leading to a defendable SIS.

While vendor compliance to security standards is important, users should realize that vendor compliance is achieved as "system capability" compliance. Compliance only indicates that the system has the product features and capabilities allowing the system to be implemented in compliance with the requirements of the security standard. Users should still follow specific procedures when implementing the system.

Emerson can assist in developing the project scope of work to determine the best way to implement the security capabilities, and that effort also includes the DeltaV SIS platform.

References

1 - **DeltaV Safety Network Components product data sheet**

2 - **DeltaV Security Manual**

3 - **Whitepaper from the Cyber Security Working Group of the 61508 Association**

4 - **Smart Card Two-Factor Authentication white paper**

5 - **USB Usage article from the Department of Homeland Security (ICS-CERT division)**

6 - **Emerson's Guardian Support portal**

7 - **Symantec ICSP Support for DeltaV Systems white paper**

8 - **Application Whitelisting for DeltaV Systems**

9 - **Endpoint Security for DeltaV Systems service data sheet**

10 - **ISA99 Committee website**

11 - **ISASecure website**

12 - **Achilles® Communications Certification website**

13 - **Independent DeltaV Domain Controller white paper**

Emerson
North America, Latin America:
+1 800 833 8314 or
+1 512 832 3774

Asia Pacific:
+65 6777 8211

Europe, Middle East:
+41 41 768 6111

www.emerson.com/deltavsis