Security Assurance Levels: A Vector Approach to Describing Security Requirements

James D. Gilsinn
Electronics Engineer
National Institute of Standards & Technology (NIST)

Ragnar Schierholz
Principal Scientist
ABB Switzerland Ltd.

Keywords: security, assurance, level, sal, vector, requirement, isa, isa99, industrial, automation, control, system, iacs

ABSTRACT

Safety systems have used the concept of safety integrity levels (SILs) for almost two decades. This allows the safety of a component or system to be represented by a single number that defines a protection factor required to ensure the health and safety of people or the environment based on the probability of failure of that component or system. The overall risk can be calculated based on the consequences that those failures could potentially have. Security systems have much broader application, a much broader set of consequences, and a much broader set of possible circumstances leading up to a possible event. The increased complexity of security systems makes compressing the protection factor down to a single number much more difficult. The concept of a vector of Security Assurance Levels (SALs) to describe the protection factor needed to ensure the security of a system is introduced in this paper.

1 INTRODUCTION

Safety systems have used the concept of safety integrity levels (SILs) for almost two decades. This allows the safety integrity capability of a component or the safety integrity level of a deployed system to be represented by a single number that defines a protection factor required to ensure the health and safety of people or the environment based on the probability of failure of that component or system. The process to determine the required protection factor for a safety system, while complex, is manageable since the probability of a component or system failure due to random hardware failures can be measured in quantitative terms. The overall risk can be calculated based on the consequences that those failures could potentially have on health, safety, or environment (HSE).

Security systems have much broader application, a much broader set of consequences, and a much broader set of possible circumstances leading up to a possible event. Security systems are still meant to protect HSE, but they are also meant to protect the process itself, company-proprietary information, public confidence, and national security among other things in situations where random hardware failures may not be the root cause. In some cases, it may be a well-meaning employee that makes a mistake, and in other cases it may be a devious attacker bent on causing an event and hiding the

evidence. The increased complexity of security systems makes compressing the protection factor down to a single number much more difficult.

This paper describes how a vector containing multiple values can be used to describe the protection factor needed to ensure the security of a system. It has been written to help standards developers, users, and vendors understand the multi-value protection factor without having to read and understand all of the nuances of the many security standards available today.

The vector concept for security proposed in this paper is largely based on the work that has been developed within the International Society of Automation's (ISA's) committee (ISA99) on security for industrial automation and control systems (IACS). While the standards developers in ISA99 are a primary target for this paper, there may be other similar standards efforts underway that may be able to make use of the vector concept for defining security requirements.

2 ISA99 DOCUMENT SERIES

The ISA99 committee has developed a plan to release a series of documents, each describing a different aspect of cyber security for IACS. Figure 1 shows a graphical depiction of the ISA99 document series.

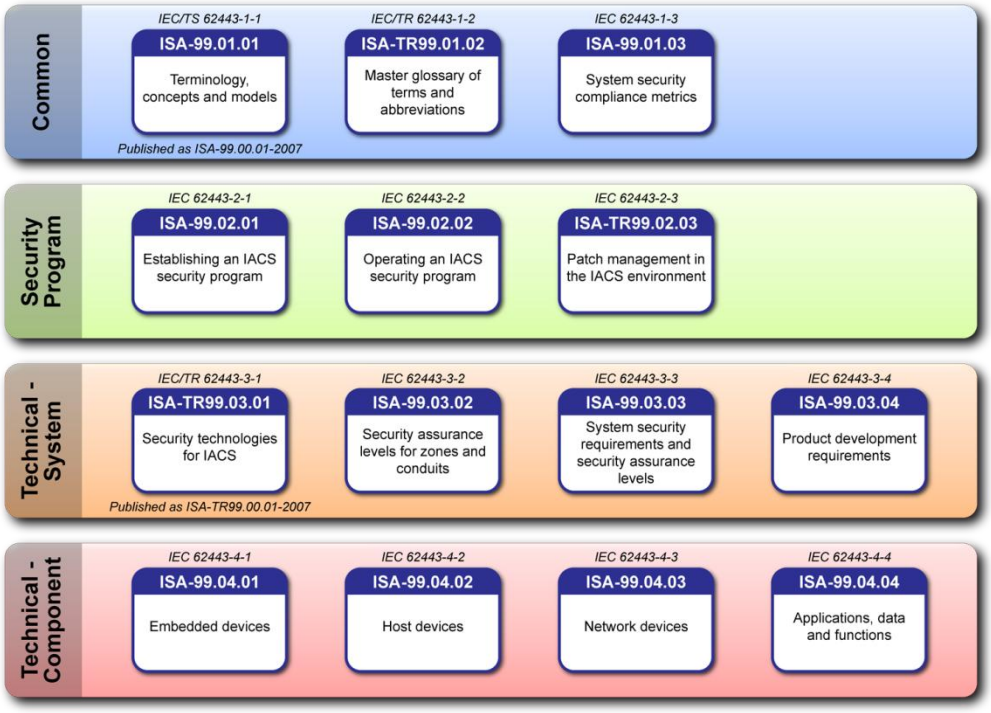

Figure 1 – ISA99 Document Series

There are four major groupings of documents in the ISA99 document series: common, security program, technical – system, and technical – component. The first group of documents describes aspects of security that are common and form the basis for all the other documents in the ISA99 series. The second group of documents focuses on the security program inside a company. These are the

administrative, personnel, and programmatic aspects of an overall security system that a company needs to consider when developing their security program. The third group of documents focuses on the technical security requirements to protect systems within a company. These are many of the system development and integration issues that a company will need to deal with when putting a system together. And finally, the fourth group of documents focuses on the technical security requirements for individual components within a system. These are the hardware, software, and informational pieces of the system and the specific technical security requirements to consider when either building or procuring these types of components.

3 SECURITY ASSURANCE LEVELS

3.1 DEFINITION

Security assurance levels (SALs) were introduced in ISA-99.01.01 [1] as security levels (the ISA99 committee chose to change the name to security assurance level after that standard was published). The following text comes from ISA-99.01.01 and provides a good explanation of what SALs are and how they can be used.

> *Security levels provide a qualitative approach to addressing security for a zone. As a qualitative method, security level definition has applicability for comparing and managing the security of zones within an organization. As more data becomes available and the mathematical representations of risk, threats, and security incidents are developed, this concept will move to a quantitative approach for selection and verification of Security Levels (SL). It will have applicability to both end user companies, and vendors of IACS and security products. It will be used to select IACS devices and countermeasures to be used within a zone and to identify and compare security of zones in different organizations across industry segments.*

In the first phase of development, the ISA99 series of standards tends to use qualitative security levels, using terms such as “low”, “medium”, and “high”. The end-user will be required to come up with their own definition of what those classifications mean for their particular application. The long-term goal for ISA99 is to move as many of the security levels and requirements to quantitative descriptions, requirements, and metrics as possible to establish repeatable applications of the standard across multiple companies and industries. Achieving this goal will take time, since more experience in applying the standards and data on industrial security systems will need to be acquired to justify the quantitative approach.

When mapping requirements to the different SALs, standard developers need some frame of reference describing what the different SALs mean and how they differ from each other. The goal of this paper is to propose such a frame of reference.

3.2 TYPES OF SALS

SALs have been broken down into four different types: target, design, achieved, and capabilities. These types, while they all are related have to do with different aspects of the security life cycle.

- **Target SALs** are the desired level of security for a particular system. This is usually determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation.
- **Design SALs** are the planned level of security for a particular system. These SALs may go through multiple revisions during the design process as different countermeasures are explored to meet the target SALs.
- **Achieved SALs** are the actual level of security for a particular system. These are measured after a system is in place and are used to establish that a security system is meeting the goals that were originally set out in the target SALs.
- **Capability SALs** are the security levels that component or systems can provide when properly configured. These levels state that a particular system or component is capable of meeting the target SALs without additional compensating controls when properly configured and integrated.

Each of these SALs is intended to be used in different phases of the security life cycle according the ISA99 series of standards. Starting with a target for a particular system, an organization would need to build a design that included the capabilities to achieve the desired result. In other words, the design team would first develop the target SAL necessary for a particular system. They would then design the system to meet those targets, resulting in the design SAL. As part of that design process, the designers would pick systems and components with the necessary capability SALs to meet the design SAL requirements. After the system went into operation, the actual SAL would be measured as the achieved SAL and compared to the target and design SAL.

3.3 USING SALS

When designing a new system (green field) or revising the security of an existing system (brown field), the first step is to break the system into different zones and define conduits connecting these zones where necessary. Details on how to accomplish this are given in ISA-99.03.02 [4]. Once a zone model of the system is established each zone and conduit is assigned a target SAL, based on a consequence analysis, which describes the desired security assurance for the respective zone or conduit. During this initial zone and conduit analysis, it is not necessary to have completed a detailed system design. It is sufficient to describe the functionality that should be provided by assets in a zone and the connections between zones in order to meet the security objectives.

Figure 2 and Figure 3 show high-level examples of systems broken down into zones connected by conduits. Figure 2 is a graphical representation of a control system for a chlorine truck loading station. It has three security zones defined: the control system, the safety integrated system (SIS), and the plant network. The control system and SIS both use programmable logic controllers (PLCs) to operate different aspects of the loading station. The two PLCs are connected via a non-routable serial Modbus network. Figure 3 is a graphical representation of a manufacturing plant. It has four zones defined: the enterprise network, the industrial/enterprise demilitarized zone (DMZ), and two industrial networks. The enterprise infrastructure has a wireless local area network (WLAN) and a connection to the Internet. Many companies use a DMZ between important parts of their systems to isolate the network traffic. In this particular example, each industrial network operates relatively independent of each other with its own PLC, field devices, and human-machine interface (HMI).

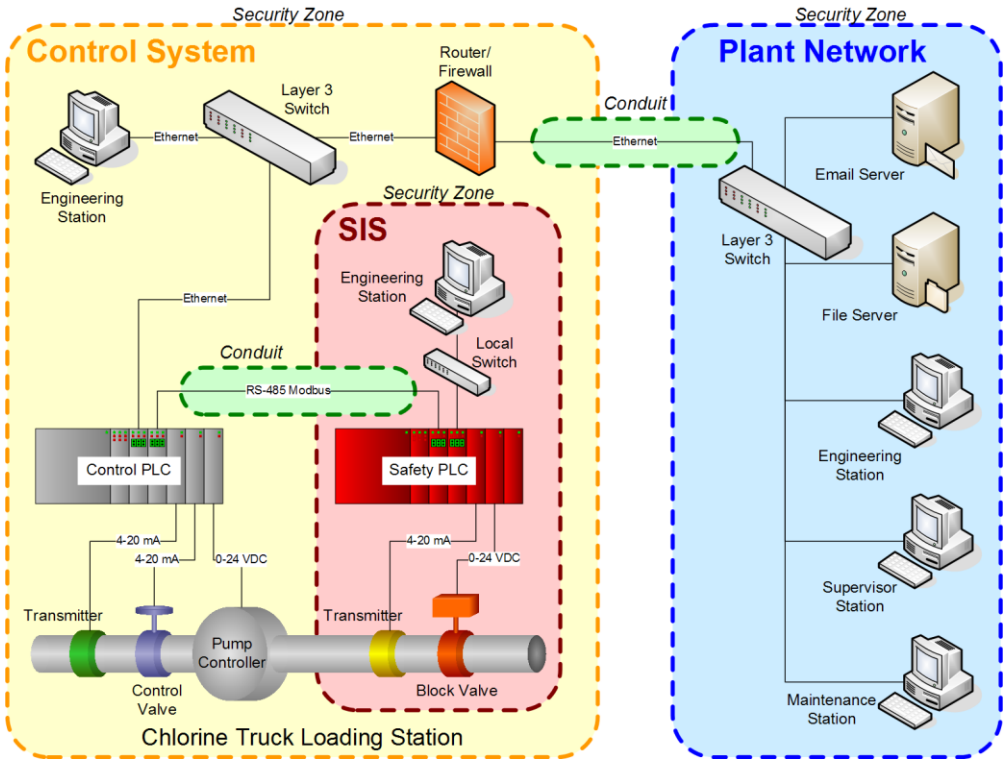

Figure 2 – High-level process-industry example showing zones and conduits

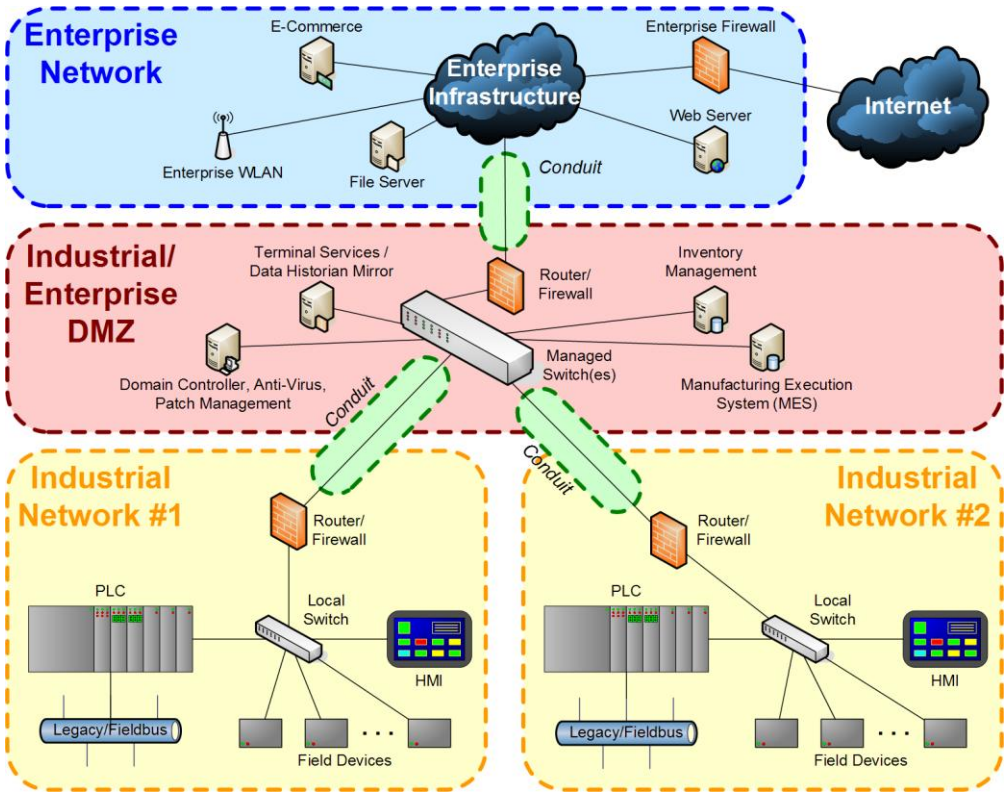

Figure 3 – High-level manufacturing example showing zones and conduits

After determining the target SALs, the system can be designed (green field) or redesigned (brown field) to try to meet those target SALs. The design process is usually an iterative approach where the system design is checked against the target multiple times throughout the process. Multiple parts of the ISA99 series of standards contain guidance on different aspects of the programmatic and technical requirements that go into the design process. ISA-99.02.01 [2] provides guidance on the programmatic aspects of the design process while ISA-99.03.03 [5] and the ISA-99.04.## series define system-level and component-level technical security requirements and relate them to different capability SALs.

During the design process for a system, it is necessary to evaluate the security capabilities of different components and subsystems. Vendors will have to provide these as capability SALs for their products by comparing product features and capabilities with the requirements defined in the ISA99 series for the different capability SALs. These capability SALs can be used to determine whether a given system or component is capable of meeting the target SAL for the system. The vendor or system integrator will also have to provide guidance on how to configure the component or subsystem to meet the claimed SALs.

It is likely that in a particular design there will be some components or systems that cannot fully meet the target SAL. Where the capability SAL of a component or system is lower than the target SAL, compensating controls need to be considered to meet the desired target SAL. Compensating controls may include changing the design of the component or system to increase its capabilities, choosing another component or system to meet the target SAL, or adding additional components or systems to meet the target SAL. After each iteration, the system design SALs should be reevaluated to see how they compare to the target SALs for the system.

Once the system design is approved and implemented, the system needs to be evaluated to prevent or mitigate deterioration of the system's security level. It should be evaluated during or after system modifications and on a regular schedule. ISA-99.02.01 and ISA-99.02.02 [3] provide guidance on the steps necessary to operate the security program and how to evaluate its effectiveness. After the achieved SALs have been determined, it will be necessary to evaluate whether the system is still meeting the original target SALs (e.g. using the system requirements from ISA-99.03.03). If the system is not meeting those requirements, there may be multiple reasons including the lack of maintenance of the program or the need to redesign parts of the system.

3.4 FOUNDATIONAL REQUIREMENTS

SALs are based on the seven foundational requirements (FRs) for security as defined in ISA-99.01.01:

a) Access control (AC)

b) Use control (UC)

c) Data integrity (DI)

d) Data confidentiality (DC)

e) Restrict data flow (RDF)

f) Timely response to an event (TRE)

g) Resource availability (RA)

Instead of compressing SALs down to a single number, it is possible to use a vector of SALs that uses the seven FRs above instead of a single protection factor. This vector of SALs allows definable separations between SALs for the different FRs using language that can be based on the additional consequences associated with security systems or different attacks against the security objectives addressed by the FRs. The language used in the SAL definitions can contain practical explanations of how one system is more secure than another without having to relate everything to HSE consequences.

3.5 SECURITY ASSURANCE LEVELS

The ISA99 standards define SALs in terms of four different levels (1, 2, 3, and 4), each with an increasing level of security. Every SAL defines security requirements and a given system can comply with them or not and a given product can provide the capability to comply with them or not. There is no SAL zero defined in the ISA99 standard series to describe a system which has no special requirements related to security for a particular FR. Thus, it would be useful to introduce a SAL zero. This may allow a software program to be used to compare and aggregate the SAL vectors for a particular zone easier than using a null value or some string value like "no requirement".

The language used for each of the SALs uses terms like casual, coincidental, simple, sophisticated, and extended. This language is intentionally vague to allow the same basic language to be used for all of the standards in the ISA99 series. Each of the individual standards in the series will define the requirements for the SALs that apply to their particular purpose.

While the requirements for each of the SALs will be different throughout the ISA99 series, there needs to be a general understanding of what each of the SALs should protect against. The following sections will provide some guidance on how to differentiate between the SALs.

3.5.1 SAL 1 – PROTECTION AGAINST CASUAL OR COINCIDENTAL VIOLATION

Casual or coincidental violations of security are usually through the lax application of security policies. These can be caused by well meaning employees just as easily as they can be by an outsider threat. Many of these violations will be security program related and will be handled by enforcing policies and procedures.

Using Figure 2, a simple example would be an operator able to change a set point on the engineering station in the control system zone to a value outside certain conditions determined by the engineering staff. The system did not enforce the proper access and use control restrictions to disallow the change by the operator. Also using Figure 2, another example would be a password being sent in clear text over the conduit between the control system zone and the plant network, allowing a network engineer to view the password while troubleshooting the system. The system did not enforce proper data confidentiality to protect the password. Using Figure 3, a third example would be an engineer that means to access the PLC in Industrial Network #1 but actually accesses the PLC in Industrial Network #2. The system did not enforce the proper restriction of data flow preventing the engineer from accessing the wrong system.

3.5.2 SAL 2 – PROTECTION AGAINST INTENTIONAL VIOLATION USING SIMPLE MEANS

Simple means don't require much knowledge on the part of the attacker. The attacker does not need detailed knowledge of security, the domain, or the particular system under attack. These attack vectors are well known and there may be automated tools for aiding the attacker. They are also designed to attack a wide range of systems instead of targeting a specific system.

Using Figure 2, an example would be a virus that infects the email server spreading to the engineering workstation in the plant network since they both use the same general purpose operating system. Using Figure 3, another example would be an attacker compromising a web server in the enterprise network by an exploit downloaded from the Internet for a publicly known vulnerability in the general purpose operating system of the web server. The attacker uses the web server as a pivot point in an attack against other systems in the enterprise network as well as the industrial network. Also using Figure 3, a third example would be an operator that views a website on the HMI located in Industrial Network #1 which downloads a Trojan that opens a hole in the routers/firewalls to the Internet.

3.5.3 SAL 3 – PROTECTION AGAINST INTENTIONAL VIOLATION USING SOPHISTICATED MEANS

Sophisticated means require advanced security knowledge, advanced domain knowledge, advanced knowledge of the target system, or any combination of these. An attacker going after a SAL 3 system will likely be using attack vectors that have been customized for the specific target system. The attacker may use exploits in operating systems that are not well known, weaknesses in industrial protocols, specific information about a particular target to violate the security of the system, or other means that require a greater skill and knowledge set than are required for SAL 1 or 2.

An example of sophisticated means could be password or key cracking tools based on hash tables. These tools are available for download, but applying them takes knowledge of the system (i.e. the hash of a password to crack). Using Figure 2, another example would be an attacker that gains access to the safety PLC through the Modbus conduit after gaining access to the control PLC through a vulnerability in the Ethernet controller. Using Figure 3, a third example would be an attacker that gains access to the data historian by using a brute-force attack through the industrial/enterprise DMZ firewall initiated from the enterprise wireless network.

3.5.4 SAL 4 – PROTECTION AGAINST INTENTIONAL VIOLATION USING SOPHISTICATED MEANS WITH EXTENDED RESOURCES

SAL 3 and SAL 4 are very similar in that they both involve sophisticated means used to violate the security requirements of the system. The difference comes from the attacker having extended resources at their disposal. These may involve high-performance computing resources, large numbers of computers, or extended periods of time.

An example of sophisticated means with extended resources would be using super computers or computer clusters to conduct brute-force password cracking using large hash tables. Another example would be a botnet used to attack a system using multiple attack vectors at once. A third example would be an organized crime organization that has the motivation and resources to spend weeks attempting to analyze a system and develop custom zero-day exploits.

4 SAL VECTOR

4.1 FORMAT

A vector can be used to describe the security requirements for a zone, conduit, component, or system better than a single number. This vector may contain either a specific SAL requirement or a zero value for each of the foundational requirements (see 3.5).

FORMAT → SAL-?([FR,]domain) = { AC UC DI DC RDF TRE RA }

Where:

SAL-? = (Required) The SAL type (see 3.2). The possible formats are:

- *SAL-T = Target SAL*
- *SAL-D = Designed SAL*
- *SAL-A = Achieved SAL*
- *SAL-C = Capabilities SAL*

[FR,] = (Optional) Field indicating the FR that the SAL value applies. The FRs are written out in abbreviated form instead of numerical form to aid in readability.

domain = (Required) The applicable domain that the SAL applies. In the standards development process, this may be Procedure, System, or Component. When applying the SAL value to an actual system, it may be something like Zone A, Pumping Station, Engineering Workstation, etc.

EXAMPLE 1 → SAL-T(Control System Zone) = { 2 2 0 1 3 1 3 }

EXAMPLE 2 → SAL-C(Engineering Workstation) = { 3 3 2 3 0 0 1 }

EXAMPLE 3 → SAL-C(RA, Safety PLC) = 4

The following sections of this paper give a basic purpose statement for each of the FRs and then presents, in practical terms, the SALs for each of the FRs. The purpose statements have been taken from the ISA99 series of standards. The descriptions are intended to further refine the different SALs (see 3.5) for each of the foundational requirements (see 3.4). They are being proposed by the authors and have not yet been vetted by the ISA99 committee for inclusion in the standard series.

4.2 FR1 – ACCESS CONTROL (AC)

4.2.1 PURPOSE

Identify and authenticate IACS users (including human users, processes, and devices), assign them to a pre-defined role, and allow them access to the system or assets.

4.2.2 SAL DESCRIPTIONS

SAL	AC-SAL Descriptions
1	Identify and authenticate IACS users by mechanisms which protect against casual or coincidental access by unauthorized entities.
2	Identify and authenticate IACS users by mechanisms which protect against intentional unauthorized access by entities using simple means.
3	Identify and authenticate IACS users by mechanisms which protect against intentional unauthorized access by entities using sophisticated means.
4	Identify and authenticate IACS users by mechanisms which protect against intentional unauthorized access by entities using sophisticated means with extended resources.

4.3 FR2 – USE CONTROL (UC)

4.3.1 PURPOSE

Enforce the assigned privileges of an authenticated IACS user to perform the requested action on the system or assets, and monitor the use of these privileges.

4.3.2 SAL DESCRIPTIONS

SAL	UC-SAL Descriptions
1	Restrict use of the system or assets according to specified privileges to protect against casual or coincidental misuse.
2	Restrict use of the system or assets according to specified privileges to protect against circumvention by entities using simple means.
3	Restrict use of the system or assets according to specified privileges to protect against circumvention by entities using sophisticated means.
4	Restrict use of the system or assets according to specified privileges to protect against circumvention by entities using sophisticated means with extended resources.

4.4 FR3 – DATA INTEGRITY (DI)

4.4.1 PURPOSE

Ensure the integrity of information on communication channels and in data repositories to prevent unauthorized manipulation.

4.4.2 SAL DESCRIPTIONS

SAL	DI-SAL Descriptions
1	Protect the integrity of information in the system against casual or coincidental manipulation.
2	Protect the integrity of information in the system against manipulation by someone using simple means.
3	Protect the integrity of information in the system against manipulation by someone using sophisticated means.
4	Protect the integrity of information in the system against manipulation by someone using sophisticated means with extended resources.

4.5 FR4 – DATA CONFIDENTIALITY (DC)

4.5.1 PURPOSE

Ensure the confidentiality of information on communication channels and in data repositories to prevent dissemination.

4.5.2 SAL DESCRIPTIONS

SAL	DC-SAL Descriptions
1	Prevent the dissemination of information via eavesdropping or casual exposure.
2	Prevent the dissemination of information to an entity actively searching for it using simple means.
3	Prevent the dissemination of information to an entity actively searching for it using sophisticated means.
4	Prevent the dissemination of information to an entity actively searching for it using sophisticated means with extended resources.

4.6 FR5 – RESTRICT DATA FLOW (RDF)

4.6.1 PURPOSE

Enforce the segmentation of the system via zones and conduits by limiting the flow of data to conduits between zones.

4.6.2 SAL DESCRIPTIONS

SAL	RDF-SAL Descriptions
1	Prevent the casual or coincidental circumvention of zone and conduit segmentation systems.
2	Prevent the intended circumvention of zone and conduit segmentation systems by entities using simple means.
3	Prevent the intended circumvention of zone and conduit segmentation systems by entities using sophisticated means.
4	Prevent the intended circumvention of zone and conduit segmentation systems by entities using sophisticated means with extended resources.

4.7 FR6 – TIMELY RESPONSE TO AN EVENT (TRE)

4.7.1 PURPOSE

Respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and taking timely corrective action when incidents are discovered.

4.7.2 SAL DESCRIPTIONS

SAL	TRE-SAL Descriptions
1	Monitor the operation of the system and respond to incidents when they are discovered by providing the forensic evidence when queried.
2	Monitor the operation of the system and respond to incidents when they are discovered by actively collecting forensic evidence from the system.
3	Monitor the operation of the system and respond to incidents when they are discovered by actively pushing forensic evidence to the proper authority.
4	Monitor the operation of the system and respond to incidents when they are discovered by actively pushing forensic evidence to the proper authority in near real-time.

4.8 FR7 – RESOURCE AVAILABILITY (RA)

4.8.1 PURPOSE

Ensure the availability of the system or assets against the denial of essential services.

4.8.2 SAL DESCRIPTIONS

SAL	RA-SAL Descriptions
1	Ensure that the system operates reliably under normal production conditions and prevents denial-of-service situations caused by the casual or coincidental actions of an entity.
2	Ensure that the system operates reliably under normal and abnormal production conditions and prevents denial-of-service situations by entities using simple means.
3	Ensure that the system operates reliably under normal, abnormal, and extreme production conditions and prevents denial-of-service situations by entities using sophisticated means.
4	Ensure that the system operates reliably under normal, abnormal, and extreme production conditions and prevents denial-of-service situations by entities using sophisticated means with extended resources.

5 BIBLIOGRAPHY

The following references were either used in the creation of this document or provide further information on specific topics discussed in this document.

[1] ANSI/ISA-99.01.01-2007, Security for industrial automation and control systems: Concepts, terminology and models

[2] ANSI/ISA-99.02.01-2009, Security for industrial automation and control systems: Establishing an industrial automation and control system security program

[3] ISA-99.02.02, Security for industrial automation and control systems: Operating an industrial automation and control system security program

[4] ISA-99.03.02, Security for industrial automation and control systems: Security assurance levels for zones and conduits

[5] ISA-99.03.03, Security for industrial automation and control systems: System security requirements and security assurance levels