



**UNIVERSITY OF
ALBERTA**

Master of Science in Internetworking

Capstone Project Report On

An Analysis of Cybersecurity in Industrial Automation

Submitted by

Bhairvi Singh

Under the supervision of

Mr. Jonathon Baddock

Fall 2022 - Winter 2023

DECLARATION

Bhairvi Singh solemnly declares that the project "**An analysis of Cybersecurity in Industrial Automation**" in the Department of Computing Science, Master's in internetworking, University of Alberta, is based on my work. I guarantee that this report has not been published at any other university.

ACKNOWLEDGEMENT

I want to thank my mentor, Mr. Jonathon Baddock, for providing me with guidance & support throughout the project, which helped me to complete my project on time. Also, I would like to express my appreciation to my colleagues, who provided me with valuable insights throughout the project.

I owe my profound gratitude to Dr. Mike MacGregor and Mr. Shahnawaz Mir for providing me with this valuable opportunity to work on the project, which helped me to learn a lot & gain new skillsets while working on this project.

Finally, I want to thank God for giving me strength & My family for giving me support for the successful completion of this project.

ABSTRACT

DeltaV DCS is a distributed control system designed by Emerson Process Management for use in industrial plants and facilities. It controls and monitors various processes, such as refining and chemical production.

Cybersecurity is a growing concern for organizations worldwide, especially those that rely on Distributed Control Systems (DCS) to manage their operations. The impact of cyberattacks on DCS can be significant, resulting in financial losses, production delays, and damage to the organization's reputation. In this report, I will provide an overview of the cyberattacks faced by DCS and discuss how organizations can protect their DCS from cyber threats.

This report thoroughly examines the various types of cyber threats DeltaV DCS systems can face, including malware attacks, phishing attacks, and denial-of-service attacks. The report also highlights the need for multi-layered security measures to protect DeltaV systems, including access control, network segmentation, and regular security audits.

The report also outlines various further steps that can be taken to protect DeltaV systems, including implementing intrusion detection and prevention systems, conducting regular vulnerability scans, and using security frameworks.

In my project, I implemented these best practices by creating an imaginary scenario where a company has a computer and device network that needs to be protected from external threats, such as hackers and malware. The network includes servers, workstations, and other devices that need to communicate with each other and the outside world.

The company implements the IP Firewall to help secure its network.

To protect the network, I configured a virtual firewall in a VM, allowing me to control and monitor traffic on the network. Implementing the best practices outlined above and configuring the Firewall effectively protected the company's network from cyber threats.

To encapsulate, this report has highlighted the cybersecurity challenges faced by DeltaV DCS, a widely used industrial control system, and proposed several best practices organizations can implement to protect their systems from cyber threats. By following these best practices, organizations can reduce the likelihood of successful cyberattacks and minimize the impact of any attacks that do occur.

Contents

Table of Contents

DECLARATION	2
ACKNOWLEDGEMENT	3
ABSTRACT	4
Contents	6
Section 1: Introduction to Industrial Automation systems:	9
Section 2: What is DeltaV?	10
Section 3: Threats to Control Systems	12
Section 4: What is an Asset & What leads to compromise?	13
Section 5: Vulnerabilities	15
Section 6 : Types of Cyberattacks on Industrial Control Systems	18
• Malware infection	18
• Social Engineering	19
• The Trusted Insider –	19
• Intrusion via Remote Access –	20
• Denial-of-Service (DoS) attacks –	20
• Man-in-the-middle attacks	21
• ARP Spoofing	22
• Network reconnaissance and cracking tools	23
• Impersonation attempts and Elevation of privileges –	23
• Remote Code Execution –	23
Section 7: Strategies used to protect DeltaV Control Systems	24
7.1 Security Policies & Procedures	26
7.2 Securing DeltaV DCS Systems using the Purdue Model: A Comprehensive Approach	29
Level 4/5: Enterprise Zone	31
Level 3.5: Demilitarized Zone (DMZ)	31
Level 3: Manufacturing Operations Systems Zone	31
Level 2: Control Systems Zone	32
Level 1: Intelligent Devices Zone	32
Level 0: Physical Process Zone	32
7.3 Defence in Depth strategy	35

7.3.1 Performing risk assessments[2]	36
7.3.2 Security Hardening.....	37
7.4 Network Architecture	38
7.4 Firewall	41
7.4.1(a.) What is a Firewall?	41
7.4.1(b.)Use of Firewalls in DMZ Layer of DeltaV systems	46
7.4.1(c.) Use of Firewalls in Area Control Network Layer (Level0,Level1) of DeltaV system.....	47
7.4.1(d.) Sample Firewall Configuration using IP fire (Implementation)[27]	49
1.) Open Source Firewall-Deployment of Firewall OS.....	50
2.) Restarting OS after setting inside & outside IP addresses:	51
3.) Configuration of Web Interface	52
4.) Host Creation (Standard In Firewall)	53
➤ Network Diagram	54
5.) Creating Inside& Outside groups-Green/Red	55
6.) Creating Manual Hosts & Binding IP addresses with names	56
7.)Rule Creation	57
8.) Rule Summary	58
7.5 Node Protection:.....	59
7.5 (a.)Antivirus Software :	60
7.5.(b)Whitelisting:	63
7.5(c.) Patch Management & Security Updating:	64
7.6 Users.....	65
7.7 Monitoring :	68
NSN-Traffic Sniffing /Analysis	68
Conclusion:	70
References	71

Table of Figures

Figure 1 : Explanation of Basic Process Control System [4].....	10
Figure 2:CIA Triad [14].....	13
Figure 3: Anatomy of the Triton Malware Attack[13]	16
Figure 4: Picture Depicting Malware[16]	18
Figure 5: Social Engineering[15].....	19
Figure 6:Image Depicting how MIM attack works[18].....	21
Figure 7:Explanation of ARP spoofing attack	22
Figure 8:Attack Vectors on Industrial Control Systems [17]	23
Figure 9:Framework of Security Policies & Procedures[20].....	26
Figure 10:General ISA/Purdue Model[23]	29
Figure 11:Purdue Model for Control Hierarchy[23].....	30
Figure 12: DeltaV Reference Architecture[2].....	33
Figure 13:Layers of Security used by Defense-In-Depth Strategy [24]	35
Figure 14:DeltaV Area Control Network[2].....	39
Figure 15:Firewall allowing good traffic[25]	41
Figure 16:Firewall Blocking Bad Traffic[25].....	42
Figure 17: Firewall installation in different layers of DCS Network[17].....	43
Figure 18:DeltaV Reference Architecture with references to the ISA95 / Purdue Reference Model[2]	45
Figure 19:Open Source Firewall-Deployment of Firewall OS	50
Figure 20:Restarting OS after setting inside & outside IP addresses	51
Figure 21:Configuration of Web Interface	52
Figure 22:Host Creation (Standard In Firewall)	53
Figure 23:Network Diagram	54
Figure 24:Creating Manual Hosts & Binding IP addresses with names.....	56
Figure 25:Rule Creation.....	57
Figure 26: Rule Summary	58
Figure 27:Endpoint Security & Application Whitelisting[24].....	61
Figure 28:Endpoint Security & Application Whitelisting [24].....	63
Figure 29:Password management solution for organization[31].....	66
Figure 30:Packet Sniffers[32]	68

Section 1: Introduction to Industrial Automation systems:

What is DCS?

Distributed Control System can be defined as a fully automatic or computer-operated control system with many control loops. [1]

In DCS, each machinery has its controller & CPU, and each controller runs autonomously. One main advantage of DCS is that if any one controller fails, it will affect only one section of the plant process & will not impact the entire Industrial Plant, as opposed to the case of Centralized control system where the failure of one central processor could affect the whole plant.[1]

A high-speed communication network connects all controllers, and the Operator runs central supervisory control.[1][2]

One significant advantage of Distributed Control system is that it helps in large-scale production and yields a maximum output in less time.[1]

Distributed Control Systems (DCS) have a wide range of applications and are primarily used in sizeable continuous process plants like manufacturing and process industries where reliability & security are essential, like chemical, Oil & gas, pulp & paper, water & wastewater, power, food & beverage, petrochemical industries, etc. [2]

Section 2: What is DeltaV?

DeltaV is a Distributed Control System (DCS) designed and manufactured by Emerson. It is a comprehensive process automation system used in various industries, including chemical, pharmaceutical & oil and gas[5]

It helps improve the operation of the industrial plant by efficiently utilizing new technologies.[5]

Also, it helps to reduce operational complexity by lowering project risk.[3]

Breaking down in more simple form, DeltaV can be defined as follows:

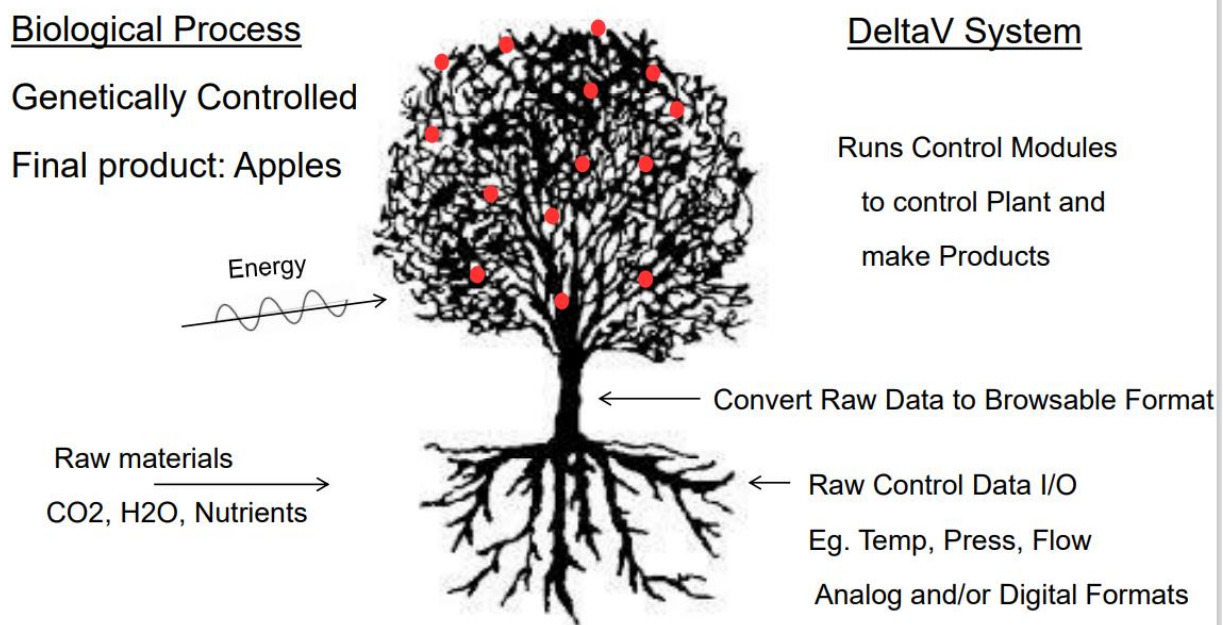


Figure 1 : *Explanation of Basic Process Control System [4]*

The unique design of DeltaV simplifies the commissioning and installation process and helps in faster project completion.[3]


The DeltaV DCS is designed to precisely and reliably control complex industrial processes, such as batch processing and continuous production. It comprises various hardware and software components, including controllers, I/O modules, network infrastructure, and operator interfaces.[3]

The DeltaV DCS is known for its advanced control algorithms, which allow for precise control of process variables such as pressure, temperature, and flow rate. It also includes advanced features such as batch management, recipe management, and process simulation, which make it well-suited for batch processing applications.[3]

In addition to its process control capabilities, the DeltaV DCS also includes a range of integrated software applications, such as asset management, maintenance management, and quality management, which help to streamline plant operations and improve overall efficiency.

Overall, the DeltaV DCS is an intelligent and flexible process automation system that can be customized to meet the unique requirements of various industrial applications.[3]

In the coming sections, I will be giving more detailed descriptions of applications about DeltaV, which will help in getting a clear idea & better understanding of DeltaV systems and how they are protected.

 ***To get a clearer understanding of DeltaV, we will start by describing basic terms used for Cybersecurity, which will be referenced in different sections throughout the research paper, which will help get an idea of the security architecture used to protect DeltaV Systems.***

Section 3: Threats to Control Systems

The term "Security threat" can be defined as the unfavourable impact on the system caused by any input or action (e.g., infection by a computer virus or stealing a password).

Threats can enter the system from various sources (e.g., over the network, through a USB memory stick) & can be intentional or accidental.

Detection of a threat can be termed an attack even if it is unsuccessful. Identifying hazards helps predict different attacks and prepare an appropriate response (protection) for each.

Identifying different types of threats helps to predict various attacks and prepare an appropriate response (protection) for each.

Security threats are categorized based on the outcomes.

However, it is essential to recognize that a given threat may often result in more than one severe outcome or compromise.

Therefore, categorizing threats by the type of compromise often leads to overlooking other types of settlements that might occur, leading to inadequate protection.

For example, a common threat is the insertion of malware onto a computer. When an attack of this type occurs, it can cause undesirable results from the exposure of data to the failure of the computer. Therefore, all types of compromises should be determined to protect assets against this threat. Furthermore, if threats are to be categorized, they should be ordered based on the characteristics of the attack (e.g., those associated with the introduction of malware).[2][7]

Section 4: What is an Asset & What leads to compromise?

Assets are the elements of a system or process that have value to the asset owner, system vendor, or even to outsiders like malicious users.

Examples of assets include intellectual property, production processes, the ability to produce products, and the products themselves. In these examples, production processes include mechanical and computing devices, data, and software.[2][7]

Compromise can be defined as any successful attack against a system that leads to loss to the asset owner and profit/gain to an attacker.

Such assets should be provided with an exceptional level of protection whose compromise can lead to significant losses or gains.[2][7]

Compromises are defined using the CIA acronym- Confidentiality, Integrity & Availability.



Figure 2: CIA Triad [14]

- **Confidentiality** refers to privacy — Confidentiality can be defined as measures taken to protect data from unauthorized access. So, confidentiality compromises are where the privacy of an asset is violated – for example, personal information such as home address or tax ID is disclosed.[8]

- **Integrity** refers to validity — Integrity can be defined as measures taken to protect data from getting altered by unauthorized users.

Integrity Compromises are when the value of an asset is changed – for example, the unauthorized change of data either as it is communicated or as it resides in a database.[8]

For example, an attacker can manipulate process data, preventing the system from displaying the actual process status and hiding process problems from an operator. [8]

- **Availability** refers to the usefulness of an asset — Availability can be defined as information readily available to authorized users like employees of the company for the company's business, customers, etc.[9]

Availability compromises are when the usefulness of an asset is reduced – for example, impacting the performance of an operator workstation, so it becomes unusable to control the process.

Availability compromises are also referred to as Denial of Service (DoS).[9]

A detailed interpretation of Denial-of-Service attacks will be described in the coming sections.

Section 5: Vulnerabilities

A computer system vulnerability can be defined as the weakness of a computer system that is prone to "Cyberattack."

This can also happen when systems (IT or OT systems) are not protected from threats that expose them to cyberattacks.[10]

We know that internet browsers are well known to have users exposed to malicious websites with malware embedded inside software code. Regularly updating the system reduces the risk of exposure to these well-publicized vulnerabilities. Hence users are not allowed to browse the Internet from workstations that are part of the control system.[2]

Many threat vectors remain in DCS for an extended time without being noticed. For example, OT hackers get through the system by phishing emails or bypassing security protocols.[12]

After successfully placing malware, hackers get access to the control system & manipulate the functions to impact pressure sensors, valves, motors & other equipment. [12]

Moreover, by any chance, if something breaks up at any step during the process, employers or workers are unable to identify damage done by hackers & assume it to be typical damage & fix it. Then after getting fixed, hackers continue their attack undetected.[12]

Taking the example of the TRITON attack, threat vectors had penetrated and stayed inside Distributed Control Systems (DCS), which had been unnoticed for months -or possibly years. The attackers triggered an outage at one point, but the plant's operators attributed it to a mechanical glitch. [12]

Luckily, the company found out about the attack when the attackers tried to change the controller, triggered the safety system & shut down the plant.[12]

This could have led to the release of toxic H₂S gas or immediate danger to life & health, including one at the facility & surrounding area – MIT Tech's Martin Giles wrote about an incident when the malware was found to have attacked a petrochemical plant in Saudi Arabia (via Futurism).[12]

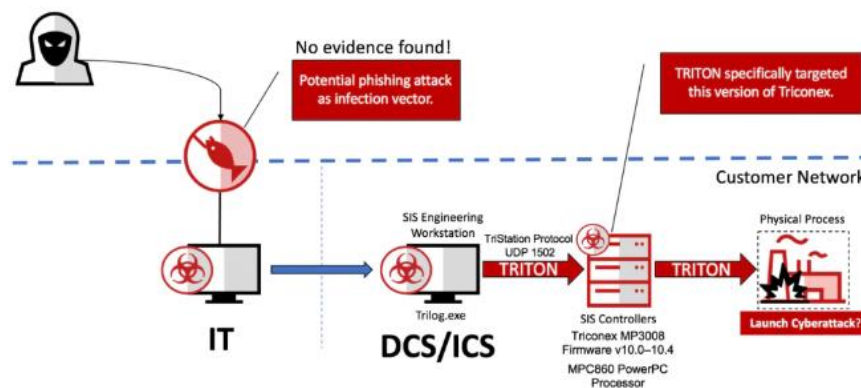


Figure 3: Anatomy of the Triton Malware Attack[13]

Identification of vulnerabilities can be crucial and can help in implementing protective measures.

The best way to identify vulnerabilities can be started by examining the external interfaces of a system & listing the equipment (physical assets) that can be accessed directly or indirectly through these interfaces.[2][11]

Also, the paths of the interfaces should be examined & anything that is not protected should be marked as vulnerable. For this task, automated analysis & testing tools can be used.

Finally, documenting these findings, including network and data flow diagrams, will help while performing hardening tasks. [2][11]

Section 6 : Types of Cyberattacks on Industrial Control Systems

These are the possible Cyberattacks Industrial Control Systems are at risk of if the appropriate policies or defences are not in place:

- **Malware infection** – A standard attack which relies on malicious code installation into the target nodes or malicious code injection on running applications.

DeltaV workstations and servers should never be directly connected to the Internet, as malware infection is still a possible attack since the viruses can be transmitted on internal networks or it can also be transmitted through other means, such as removable media. [16][2]



Figure 4: Picture Depicting Malware[16]

- **Social Engineering** – This indirect attack is targeted to obtain user credentials, becoming an entry point to the control systems.

The attacker convinces a user to divulge their username/password or open a file containing malware that compromises their workstation – allowing the attacker to gain a foothold on the network. Education about possible social engineering attacks can reduce the threat. [15][2]



Figure 5: Social Engineering[15]

- **The Trusted Insider** – Misuse is a critical threat to control systems. Personnel that have been dismissed might still have access to the control system and could use this access to change settings on a live system. Processes to immediately and thoroughly revoke access should be in place.[2]

- **Intrusion via Remote Access** – This attack occurs when an intruder obtains control system user credentials and gains access to the control system using remote access mechanisms.

Remote solid access defences, including two-factor authentication and "jump servers," can mitigate this threat.[2]

- **Denial-of-Service (DoS) attacks** – There are multiple DoS attacks. Still, the consequence of such attacks is to prevent legitimate users, nodes, and services from performing their functions within a control system by reducing their access to any of the available control interfaces.

This attack can affect network communications, embedded nodes, or user access to the system. A well-defended system with a reduced attack surface can lower the possible avenues of DoS attacks.[2]

- **Man-in-the-middle attacks** –An intruder or cybercriminal inserts himself between a legitimate client and the resources the client is attempting to access.

Cybercriminals then eavesdrop on the interactions between client & control systems by inserting themselves between a line of communication established between client & control systems.

The specific exploit will change over time if new protocol weaknesses are discovered and left unpatched. An intense patching regimen and utilization of secure protocols can reduce or even eliminate the possibility of this type of attack.[18][2]



Figure 6:Image Depicting how MIM attack works[18]

- **ARP Spoofing** – This is a specific attack that relies on a first compromise of a system workstation and then uses it to poison the network ARP table to implement a man-in-the-middle attack.

When successfully deployed, ARP spoofing allows the compromised workstation to receive communication packets that were supposed to be delivered to another node whose MAC address was spoofed. [19][2]

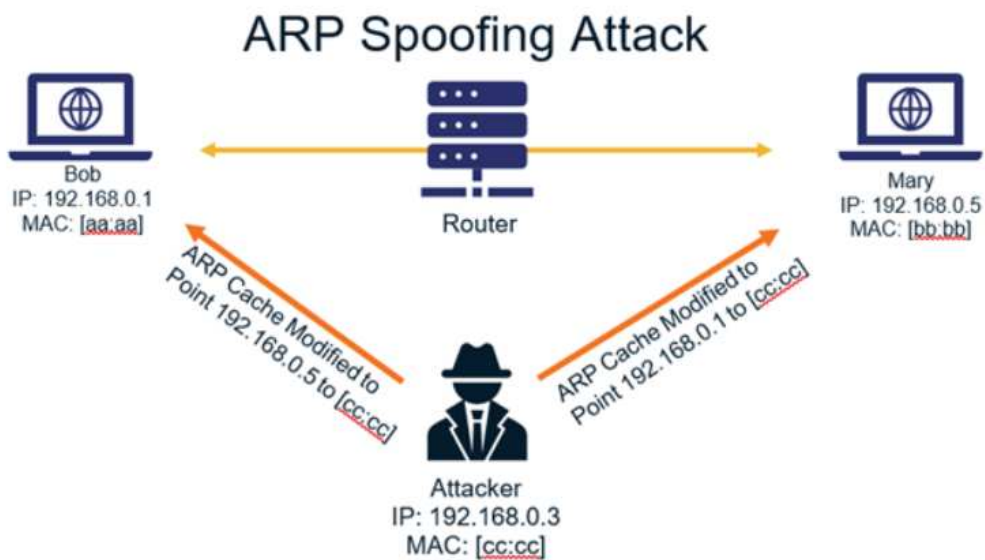


Figure 7: Explanation of ARP spoofing attack

- **Network reconnaissance and cracking tools** – Active and passive reconnaissance tools give administrators and attackers information on network configuration and topology.

"Cracking" tools take that a step further and decipher network traffic, either on-the-fly or offline.

- **Impersonation attempts and Elevation of privileges** – This attack happens when the attacker can run code on a target, and using an exploit, the attacker can get the code to run at a higher privilege level. [2]

- **Remote Code Execution** – Remote code execution is when the attacker can arbitrarily run code on a target system without having physical access to the system under attack.

The attackers can take advantage of a flaw in a network protocol to cause the program to execute instructions sent through the network protocol. There are several mitigations to this type of attack, including but not limited to Data Execution Prevention and application whitelisting. [2][17]

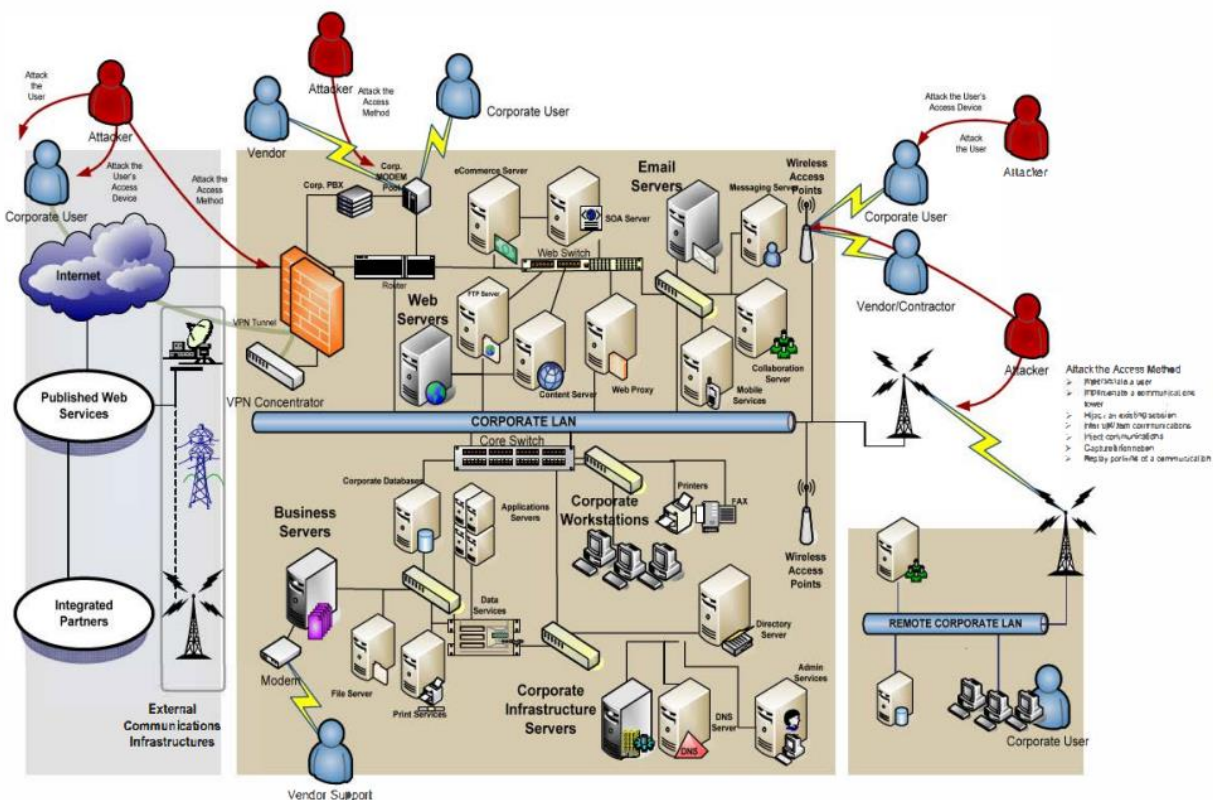


Figure 8: Attack Vectors on Industrial Control Systems [17]

Section 7: Strategies used to protect DeltaV Control Systems

Protecting the DeltaV DCS is essential to prevent unauthorized access, data breaches, and cyber-attacks.

Here are the different strategies used to protect DeltaV DCS:

1. **Policies and Procedures:** Policies and procedures should be established and communicated to all users to ensure they understand their responsibilities and roles in maintaining the system's security. This includes having clear guidelines on password management, access control, and data protection.
2. **Network Architecture:** The network architecture should be designed with security in mind. This includes using firewalls, virtual private networks (VPNs), and other security technologies to protect against external threats.
3. **Node Protection:** Node protection involves ensuring that individual nodes in the DeltaV DCS are protected against unauthorized access. This includes securing the operating system, applying security patches, and using intrusion detection software.

4. **User Training:** User training is essential to ensure that employees are aware of the security risks associated with the DeltaV DCS and how to prevent them. This includes training on safe password practices, recognizing phishing scams, and reporting suspicious activity.

5. **Monitoring:** Monitoring the DeltaV DCS is crucial to detect and prevent security breaches. This includes NSN sniffing/analysis, which is a technique used to monitor and analyze network traffic to detect unusual or non-standard behaviour. It is often used in security investigations to identify potential security threats or malicious activity that traditional security measures may not detect.[26]

The coming sections will describe each strategy used to protect DeltaV Distributed Control Systems.

By implementing these strategies, organizations can better protect their DeltaV DCS against security threats and ensure the safety and reliability of their critical infrastructure.[26]

7.1 Security Policies & Procedures

Systems face security threats from a wide range of sources and are vulnerable to attacks such as computer viruses, hacking, and denial of service attacks. Security threat analysis drives security requirements for a system, allowing system security administrators to specify which threats need to be addressed and mitigated by the system's defence-in-depth strategy. [2]

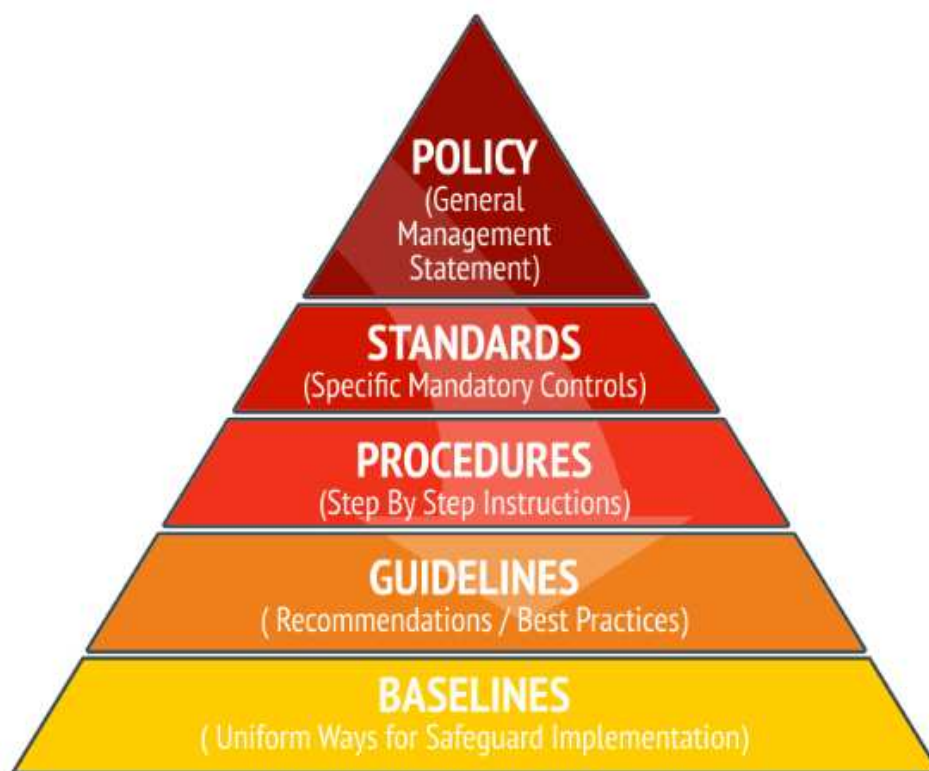


Figure 9:Framework of Security Policies & Procedures[20]

Security policies and procedures define the rules for enforcing system security requirements. They cover both user behaviour (e.g. not allowing USB memory sticks in the control room) as well as system behaviour (e.g. password strength and audit information to be collected that can be used for forensic purposes).

Identifying and implementing appropriate control system security policies and procedures requires careful planning. Participation of the control system owners and users during the development of security policies and procedures is essential for the success of a control system security. [2]

There are many approaches to set security policies and procedures. One approach is to coordinate the control system security policy with the corporate or site IT security/acceptable computer use policy tailored to create an appropriate set of security policies and procedures for the control system. Examples of security policies and procedures include the following:[2]

- All control system networks must be segmented using a firewall and a DMZ network from the business LANs.
- All users must be trained regarding the site security procedures and policies. Training ensures that users know the risks to system integrity and the consequence of a security breach.
- Engineers and supervisors must have unique usernames and passwords.
- Operators should have unique usernames and passwords.
- The built-in operating system Administrator account must be disabled/removed. Users who require operating system administrator access should have the elevated privileges they need to be added to their user accounts.

- Users who have operating system administrator access should not have access to control system parameters (separation of duties) to prevent hackers who gain administrator access from being able to access the control system.
- Access to the control system administrator account must be limited.
- Default passwords for user and service accounts must be changed during system installation or during the Site Acceptance Test.
- Plant disaster recovery plans that describe how to recover from control system security breaches, virus infections on the control network, and other control-system-specific situations should be developed.
- All security-related events, such as invalid login attempts and account management activities (e.g. adding/deleting users, changing passwords), must be logged to a security audit log.[2]

7.2 Securing DeltaV DCS Systems using the Purdue Model: A Comprehensive Approach

A control system comprises I/O devices, controllers, and workstations interconnected by layered networks and buses, as shown in Figure 12.

The Purdue Model can be defined as a reference model based on which Industrial Control Systems are designed. It is designed in such a way that separates IT & OT systems and helps secure them.

Hence separating the network layers helps maintain the hierarchical flow of data between them.[21]

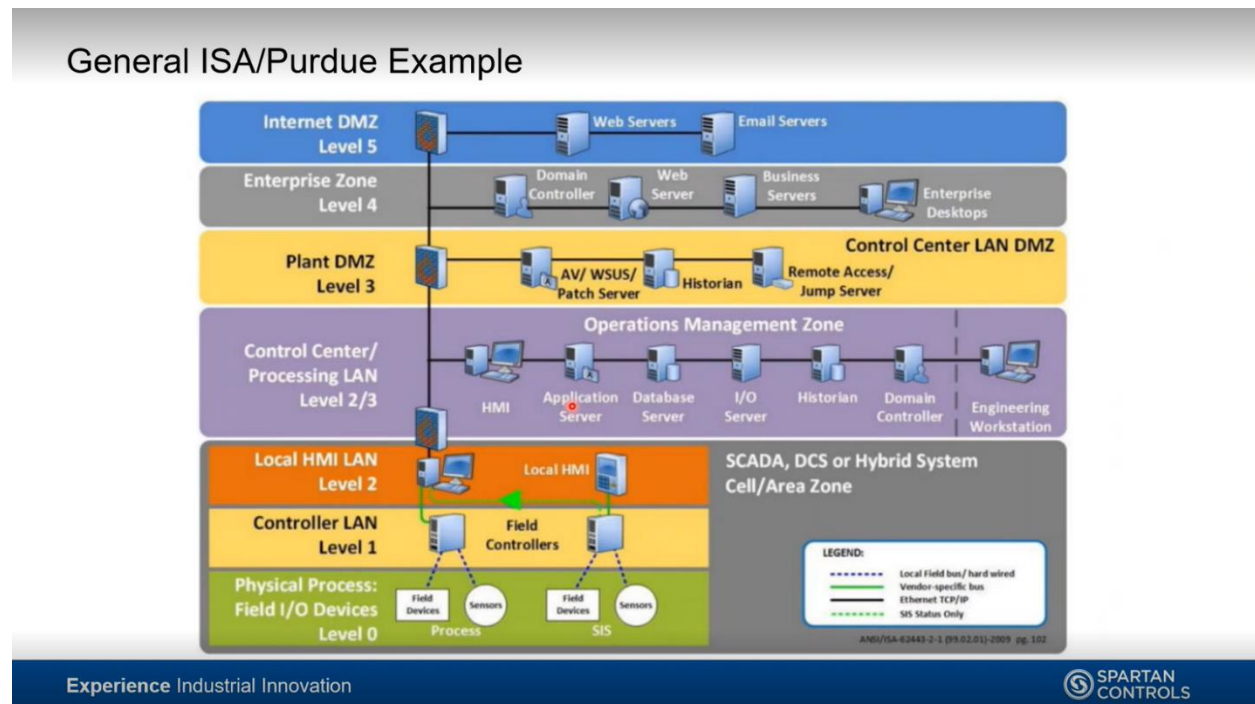


Figure 10:General ISA/Purdue Model[23]

A control system comprises I/O devices, controllers, and workstations interconnected by layered networks and buses.

Using the Purdue model nomenclature standardized by ISA 95.01 - IEC 62264-1, control systems are composed of Levels 0, 1, and 2, and enterprise systems are in Levels 3 and greater.

While not explicitly part of the Purdue model, a network segment referred to as Level 2.5 interconnects Level 2 and Level 3 and provides an additional layer of separation and security.

The Purdue Model can be defined as a reference model based on which Industrial Control Systems are designed. It is designed in such a way that separates IT & OT systems and helps secure them.

Hence separating network layers helps to maintain the hierarchical flow of data between them.

Let us look at each zone in the Purdue reference model, top to bottom.[21][2]

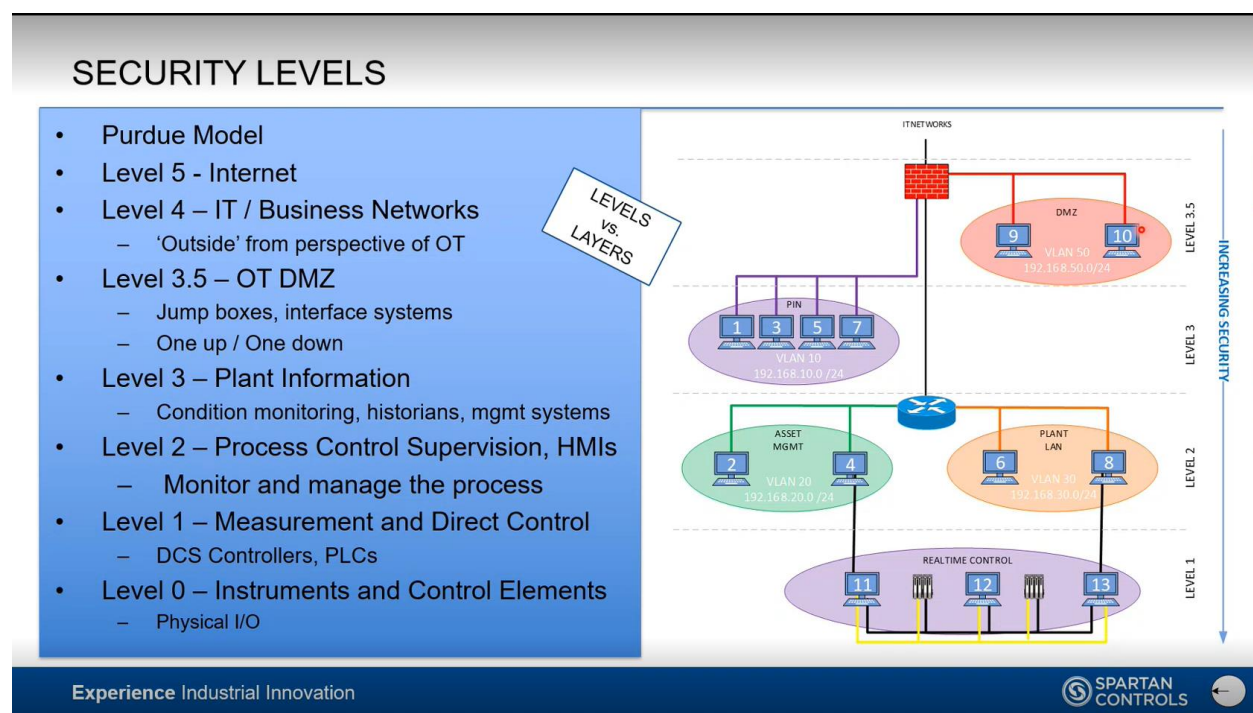


Figure 11:Purdue Model for Control Hierarchy[23]

Level 4/5: Enterprise Zone

This zone consists of a typical IT network which consists of a primary business network. Plant production schedules, material use shipping & inventory levels are being maintained by Enterprise Resource Planning Systems(ERP).

So hence disruptions caused at this layer can lead to prolonged downtime, which can cause economic damage, loss of revenue or failure of critical infrastructure.[21]

Level 3.5: Demilitarized Zone (DMZ)

In order to avoid the movement of threats between the IT & OT layer, a DMZ zone has been created, which consists of security systems like firewalls and proxies. In simple terms, It can be defined as a security interface network between IT & OT Networks.[21]

Level 3: Manufacturing Operations Systems Zone

This zone consists of OT devices that manage production workflows like:

- **Data historians** - It stores process data and performs a contextual analysis.
- **Manufacturing operations management (MOM)** - these systems help to manage production operations.
- **Manufacturing execution systems (MES)** collect real-time data, which aids in optimizing production.

Similar to the case of Level 4&5, disruptions here can lead to critical losses like damage to the economy, various risks to people & safety in plants, etc.[21]

Level 2: Control Systems Zone

This zone consists of systems that supervise, monitor, and control the physical processes:

- **Supervisory control and data acquisition (SCADA)** can be defined as software that monitors & controls physical processes, locally or remotely, and assembles & sends the data to historians.[22][21]
- **Distributed control systems (DCS)** perform SCADA functions locally.
- **Human-machine interfaces (HMIs)** allow basic controls & monitoring by connecting to DCS & PLCs.[21]


Level 1: Intelligent Devices Zone

This zone consists of instruments that send commands to the devices at Level 0 :

- **Programmable logic controllers (PLCs)**
It is an industrial computer that adjusts output based on automated or human inputs.
- **Remote terminal units (RTUs)** can be defined as a microprocessor-controlled electronic device that can act as an intermediate connecting distributed control system with the physical world or, in simple terms, connects hardware in level 0 to systems in level 2 [21]

Level 0: Physical Process Zone

This zone consists of types of machinery like sensors and actuators, which are directly responsible for assembly, lubrication, and other physical processes.

-  From a security perspective, trust levels are highest at the device level and lowest above the Business Network (on the Internet).

This means that if a device is not trusted to operate as expected, it should not be used. On the other hand, workstations on the Internet are not trusted at all. In between, trust diminishes the closer a computing device is to the Internet.

To provide this trust, computing devices must be built to operate as expected and protected from threats that could compromise their correct operation. Development and testing practices are used to assure the robustness of computing devices, and defence-in-depth strategies are used to provide layers of security that must be traversed to access them.[21][2]

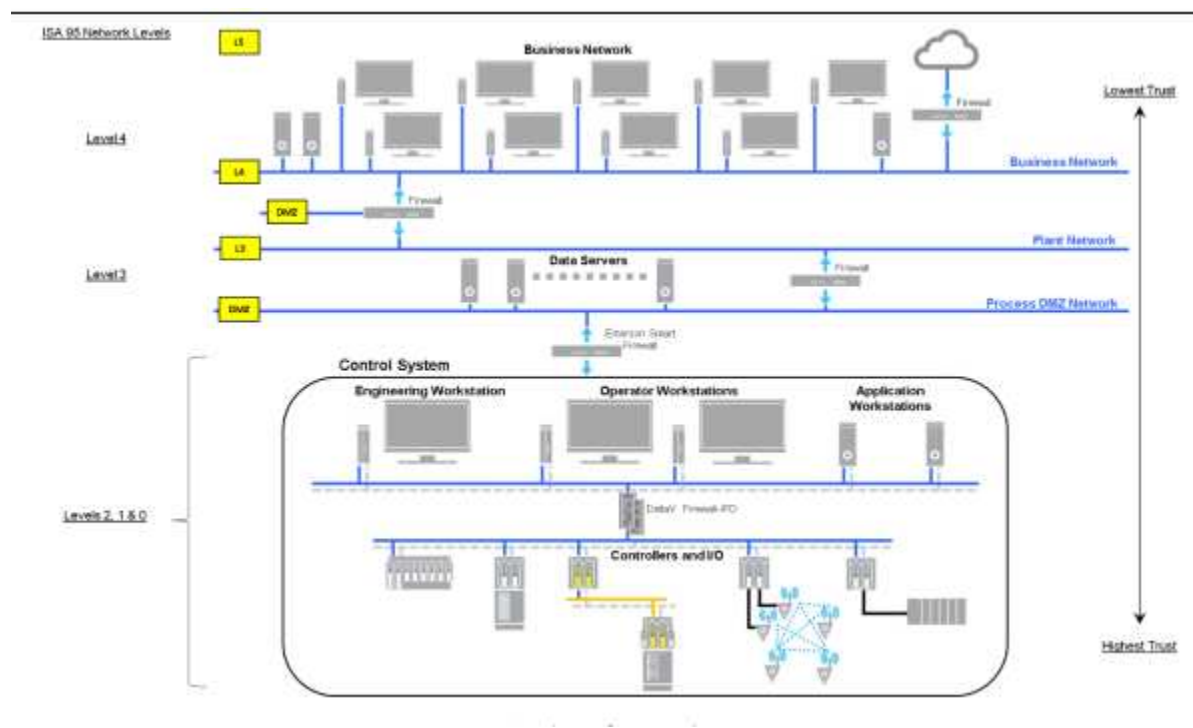


Figure 12: DeltaV Reference Architecture[2]

Network segmentation is a significant factor in the success of defence-in-depth strategies. Therefore, control system networks must be strongly segmented or isolated from other LANs on the site. [2][26]

Segmentation is accomplished by creating security zones and using security firewalls or other security devices to allow only authorized traffic between security zones. [2][26]

In the system diagram above (Figure 12), the control system is segmented from the business network using a DMZ and firewalls. Computing devices (e.g. workstations and servers) above the DMZ (i.e. on the Business Network) that are authorized to access the control system are required to connect to servers in the DMZ, which in turn, maintain separate connections to the control system. [2][26]

This protects the control system from direct attacks from the business network. In this approach, the Firewall at the upper control system boundary (L2.5 network) is configured to block traffic from the business network. The Firewall at the top of the DMZ is configured to allow only authorized Business Network workstations to connect to servers in the DMZ. [2][26]

The L3 (Plant Network) highlighted in the system diagram above is the infrastructure to interconnect multiple systems within the same site (allowing multi-vendor systems connectivity) and multiple sites into a single network. Additionally, users can create specific DMZ networks between L3 and L4 layers to provide further network segmentation for user-specific applications.[2]

7.3 Defence in Depth strategy

When a control system is to be installed, defence-in-depth strategy is recommended to be implemented during installation. Defence-in-depth strategies use layers of security to force threats to overcome multiple protective mechanisms (safeguard). When the system is installed, the defence-in-depth strategy must be implemented to support the security policies and procedures of the site where it is being installed. In addition, it may be necessary to augment the system with additional security features. These processes are collectively referred to as hardening the system. The layers of security in a defence-in-depth strategy typically include a combination of four fundamental types of security safeguards[2][24]

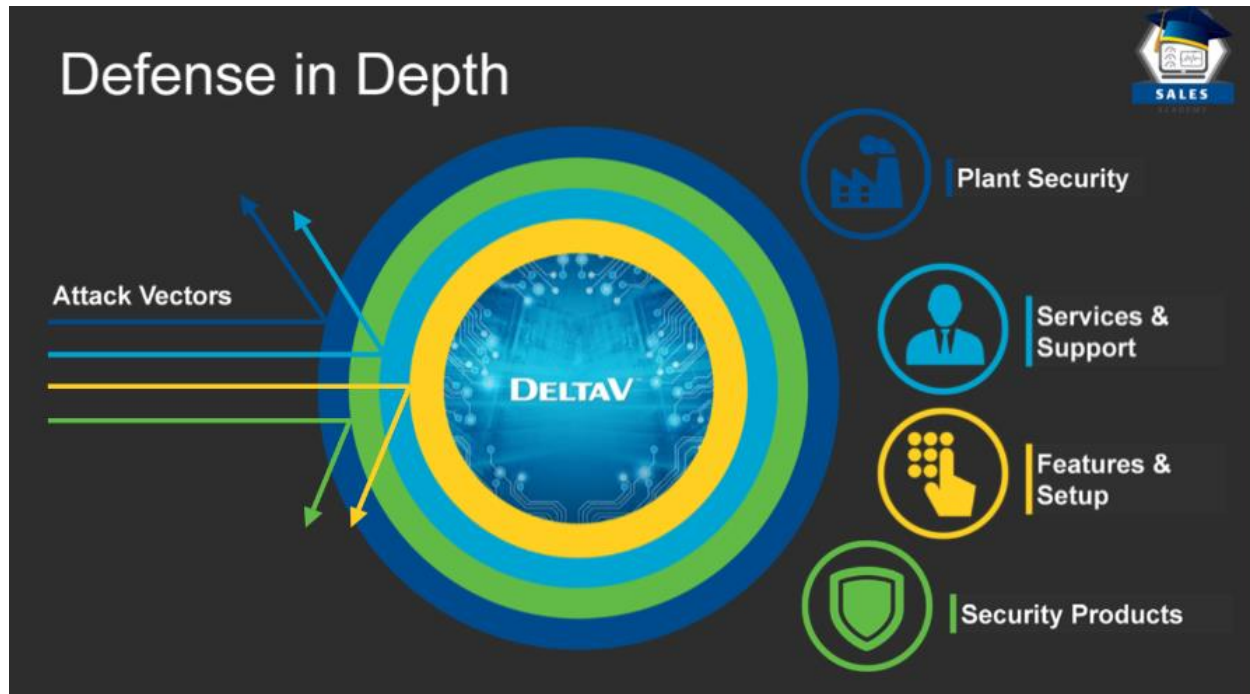


Figure 13: Layers of Security used by Defense-In-Depth Strategy [24]

- **Physical security** – protecting the control system from unauthorized physical access by users and intruders (e.g. fences, badges, locked doors),
- **Physical connectivity** – protecting the control system from unauthorized devices from being connected to the control system (e.g. preventing users from connecting their laptops to the system).
- **Communications security** – protecting the control system from unauthorized communications and from authorized communications from being viewed or altered by unauthorized users/software
- **User security** – setting up and maintaining user accounts that define access permissions (what users can access) and system privileges (what users can do).[2][24]

7.3.1 Performing risk assessments[2]

Security risk assessments are conducted to ensure the system adequately implements the defence-in-depth strategy. Risk assessments must be performed:

- on the design prior to project implementation to provide guidance for hardening the system as part of the design,
- upon installation and commissioning after hardening to evaluate the effectiveness of the hardening process, and
- on an ongoing basis, periodically after installation to respond to changes in the system, changes in threat profiles, and changes in the environment where the system is installed.

Risk assessments generally examine threats, assets, and vulnerabilities. Although many risk assessments methodologies can be used, most are designed to determine the following:

- what assets need to be protected,
- what types of losses (compromises) are of importance,
- what types of attacks are possible and probable,
- whether the defence-in-depth strategy is adequate, and if not, where the system is vulnerable to attack and how the attacks occur (which paths they take through the system),
- what safeguards (countermeasures) can be used to mitigate the attacks.[2]

7.3.2 Security Hardening

When a system is developed, the implementer defines a defence-in-depth strategy composed of architectural features (e.g. network segmentation) and security mechanisms.

When a system is installed, the architectural features and the security mechanisms must be configured to support the security policies and procedures of the site where it is being installed and to protect against the threats deemed to be applicable. In addition, it may be necessary to augment the system with additional security features. This process is referred to as hardening the system.[2]

7.4 Network Architecture

Physical segmentation defines how different network segments are connected to an integrated network. For example, as shown in the Figure below, a DeltaV system is composed of the following:

- a DeltaV/DMZ Perimeter Security Device (typically an Emerson Smart Firewall),
- a DeltaV 2.5 Network,
- a DeltaV Remote Network that connects remote DeltaV workstations,
- a DeltaV Inter-Zone Network that connects DeltaV systems together,
- a DeltaV Area Control Network (ACN) that interconnects workstations, servers, embedded controllers and I/O nodes (e.g. CIOCs and WIOC), and
- one or more I/O networks or buses used to connect field devices to controllers or I/O nodes on the ACN. DeltaV workstations/servers shown in Figure below are delivered with multiple ethernet adapters, referred to as Network Interface Cards (NICs). [2]

Network segmentation is a significant factor in the success of network security. [2]

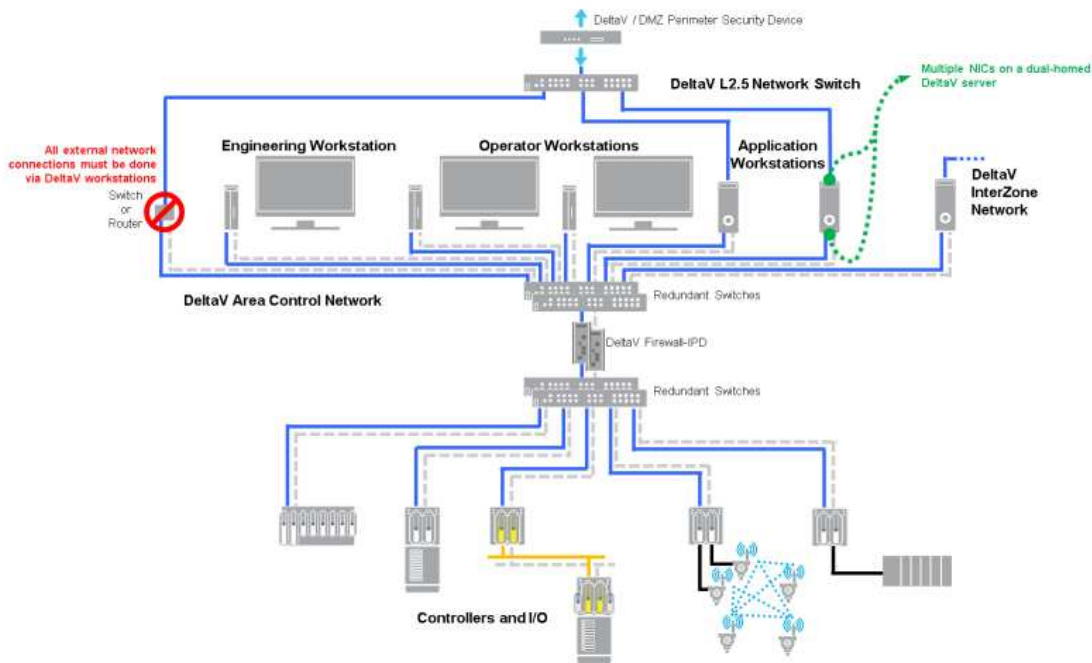


Figure 14:DeltaV Area Control Network[2]

DeltaV networks must be strongly segmented internally and segmented and isolated from other networks on the site. Segmentation is accomplished by creating security zones and then implementing security firewalls or other security protections when communicating between security zones.[2]

In the system diagram above, the business network is segmented from the DeltaV Area Control Network (ACN) using a DMZ, a DeltaV / DMZ Perimeter Security Device, a DeltaV 2.5 Network, and intervening DeltaV workstations/servers. Workstations and servers in the DMZ authorized to access the DeltaV system can communicate only with specific TCP/UDP ports of DeltaV workstations/servers connected to the DeltaV 2.5 Network. [2]

For example, in the Figure above, only two DeltaV Application Workstations are connected to the DeltaV 2.5 Network. [2]

In the Figure above, the Engineering Workstation and Operator Workstations are not accessible from the DMZ.[2]

While the DeltaV /DMZ Perimeter Security Device should be configured to enforce restrictions on the network traffic flowing between the DMZ and the DeltaV 2.5 network, and physical connectivity limitations should be implemented as they are the first level of defence.

The DeltaV defence-in-depth strategy does not allow physical connections between DeltaV ACN switches and DeltaV 2.5 Network or higher switches, routers, or firewalls.

In addition, connections between Business Network computers and DeltaV workstations/servers should be expected to connect through servers in the DMZ, thus protecting the DeltaV system from direct attacks from the business network. To support this, the Firewall at the top of the 2.5 networks is configured to block traffic from the business network.[2]

7.4 Firewall

7.4.1(a.) What is a Firewall?

A firewall is a network security device that helps to protect a computer network from unauthorized access or malicious activity. It acts as a barrier between a private internal network and the public Internet, allowing authorized traffic to pass through while blocking unauthorized traffic. Firewalls can be configured to monitor and filter incoming and outgoing network traffic based on predefined security rules. By controlling network access and limiting traffic flow, firewalls help prevent unauthorized access, data breaches, and other security threats.[33][34]

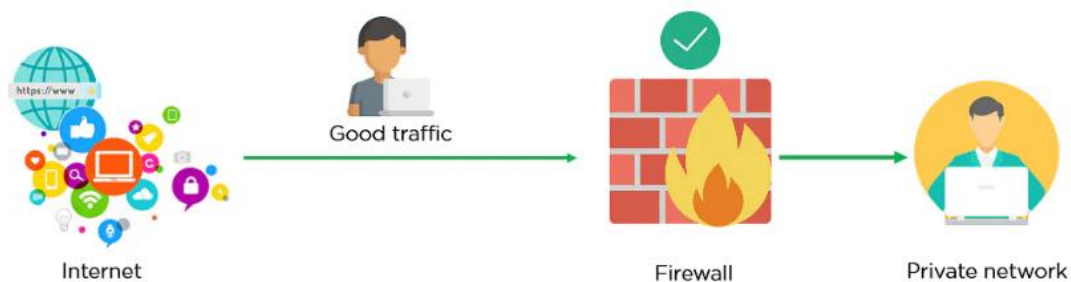


Figure 15: Firewall allowing good traffic[25]

Firewalls can be hardware-based, software-based, or a combination of both. They use a set of rules to determine whether to allow or block traffic based on factors such as the source and destination IP addresses, port numbers, and protocols used. Firewalls can also be configured to block specific types of traffic, such as viruses and malware, or to allow certain traffic, such as traffic related to business-critical applications.[25][26]

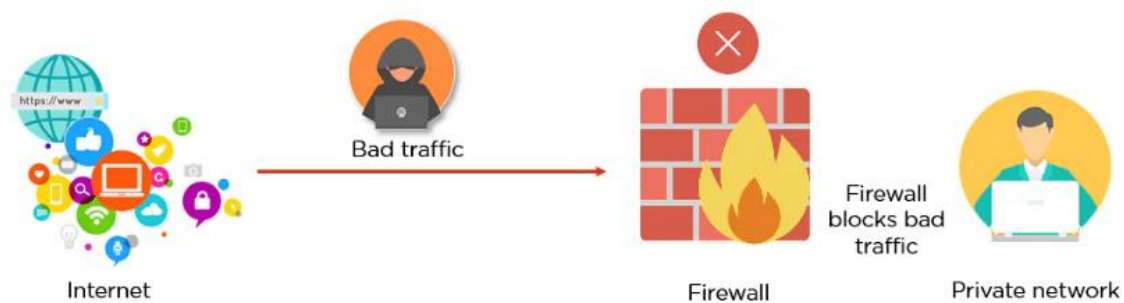


Figure 16:Firewall Blocking Bad Traffic[25]

In addition to protecting against external threats, firewalls can help prevent internal security breaches by controlling traffic flow within an organization's network. Firewalls are an essential part of a comprehensive network security strategy, but they are not a complete solution on their own and should be used with other security measures such as antivirus software, intrusion detection systems, and user education.[34]

In a DCS, a firewall can protect the network and its components from unauthorized access and control traffic flow within the network. This can include blocking traffic from unauthorized sources, monitoring network traffic for suspicious activity, and enforcing security policies to ensure that only authorized users and systems can access critical resources.[26][2]

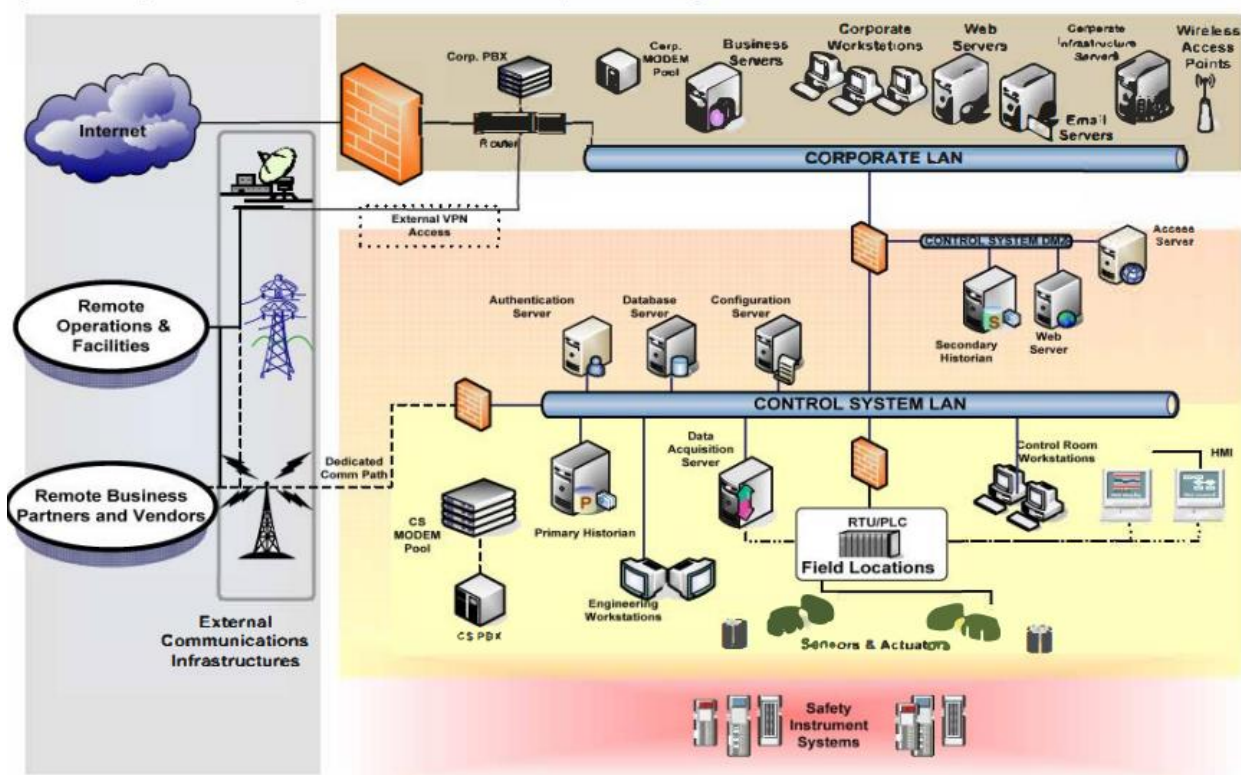


Figure 17: Firewall installation in different layers of DCS Network[17]

A firewall in a DCS should be able to handle the large volumes of data and complex communication protocols that are commonly used in DCS environments.

Some firewalls used in DCS environments are purpose-built for industrial applications and may include features such as intrusion detection and prevention, deep packet inspection, and the ability to block specific types of traffic. Firewalls can also be integrated with other security measures, such as access control systems, to provide a layered approach to security.[26][2]

Firewalls are commonly used in Level 0, Level 1, and the DMZ layer of the Purdue Model in DeltaV systems.

At Level 0, firewalls can be used to protect field devices and sensors from unauthorized access or cyber-attacks. The Firewall can be configured to allow only authorized traffic to pass through and block any unauthorized access attempts.

At Level 1, firewalls can protect controllers from unauthorized access or cyber-attacks. The Firewall can be configured to allow only authorized traffic to pass through and block any unauthorized access attempts.

In the DMZ layer, firewalls are used to create a secure boundary between the enterprise and control networks and control traffic flow between these two networks. They are also configured to monitor traffic, detect and prevent malicious activity, and segment the network to contain potential security incidents. [26][2]

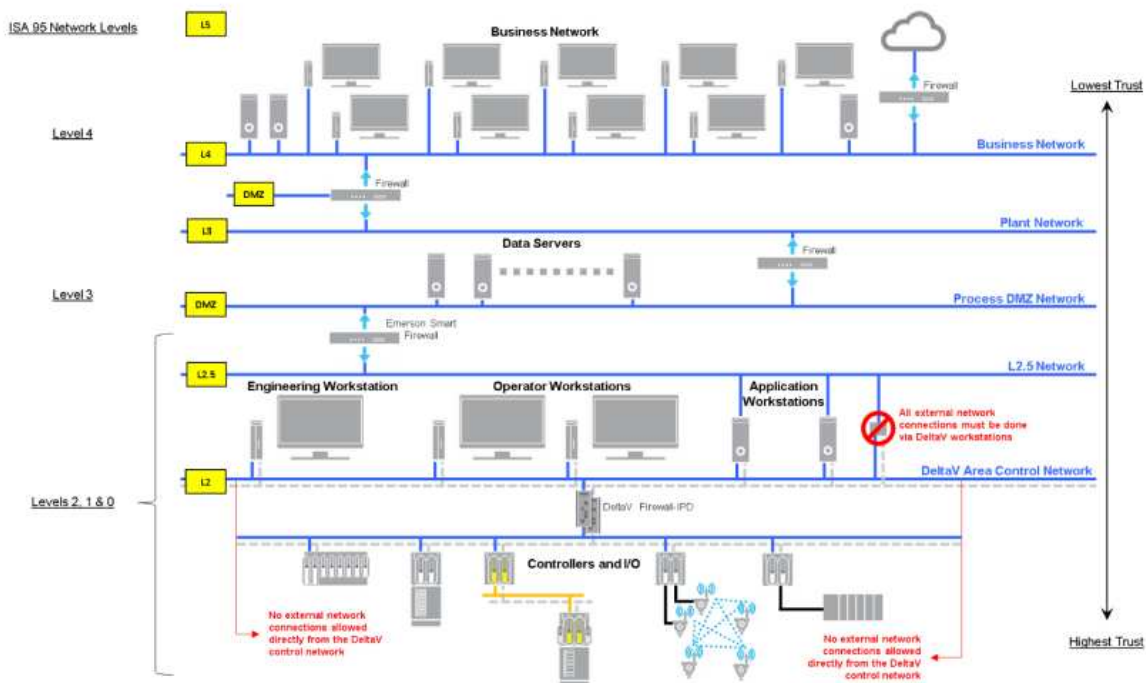


Figure 18:DeltaV Reference Architecture with references to the ISA95 / Purdue Reference Model[2]

The use of firewalls in these layers of the Purdue Model is critical for ensuring the security and reliability of industrial control systems.

7.4.1(b.)Use of Firewalls in DMZ Layer of DeltaV systems

The DMZ layer is a barrier between the enterprise and control networks. The DMZ layer typically consists of firewalls and other security devices that help protect the control network from external threats.

Firewalls are essential components of the DMZ layer, as they help control traffic flow between the enterprise and control networks. They are configured to allow only authorized traffic to pass through while blocking any unauthorized attempts. Additionally, firewalls are equipped with various security measures, such as intrusion detection and malware detection, to protect against attacks.

By segmenting the network into different zones, firewalls help to contain security incidents and limit their impact. They also monitor traffic and alert security personnel of any suspicious activity, which can help detect potential threats before they can escalate into more significant security incidents.

They provide an essential layer of defence against external threats in the DMZ layer and help ensure the safe and reliable operation of industrial control systems.[26][2]

7.4.1(c.) Use of Firewalls in Area Control Network Layer (Level0,Level1) of DeltaV system

Level 0 of the Purdue Model represents the physical processes, Level 1 represents the control devices and systems, and Level 2 represents the supervisory control and data acquisition (SCADA) systems. The operator workstation typically resides at Level 2, while the controllers are located at Level 1 or Level 0.

Firewalls can be used to provide an additional layer of security between the operator workstation and the controllers at Level 0 and Level 1. The purpose of this Firewall is to prevent unauthorized access or cyber-attacks from reaching the controllers, which can lead to potentially disastrous consequences.

At Level 0, a firewall can be used to protect field devices and sensors from unauthorized access or cyber-attacks. The Firewall can be configured to allow only authorized traffic to pass through and block any unauthorized access attempts.

At Level 1, a firewall can be used to protect the controllers from unauthorized access or cyber-attacks. The Firewall can be configured to allow only authorized traffic to pass through and block any unauthorized access attempts. This can help to prevent malicious actors from gaining access to the controllers and potentially disrupting the physical processes.

Firewalls can also be used to control the data flow between the operator workstation and the controllers. This can help prevent data manipulation or tampering that could compromise the system's integrity.

Hence the use of firewalls at Level 0 and Level 1 can provide an important layer of security in industrial control systems, helping to protect against cyber attacks and ensure the safe and reliable operation of critical processes.[26][2]

Overall, a firewall is an important component of a comprehensive security strategy in a DCS environment and can help to protect critical infrastructure and prevent costly downtime and equipment damage.[26][2]

7.4.1(d.) Sample Firewall Configuration using IP fire (Implementation)[27]

So this is the example scenario I have created to get a better understanding of how Firewall helps to secure a company's network:

A company has a computer and device network that needs to be protected from external threats, such as hackers and malware. The network includes servers, workstations, and other devices that need to communicate with each other and the outside world.

The company implements the IP Fire Firewall to help secure its network. They deploy the Firewall on a dedicated server and configure it with two network interfaces: one for the internal network (Green) and one for the external network (Red).

They then use the web interface to configure various firewall rules, such as allowing inbound traffic on specific ports for their web servers and blocking traffic from known malicious IP addresses. They also create host objects for each device on the network and assign them to the appropriate Green or Red group. This helps ensure that traffic is adequately filtered and that only authorized devices can communicate with each other and the outside world.

As a result of implementing the IP Fire Firewall, the company can significantly improve its network's security and better protect its data and assets from external threats.

1.) Open Source Firewall-Deployment of Firewall OS

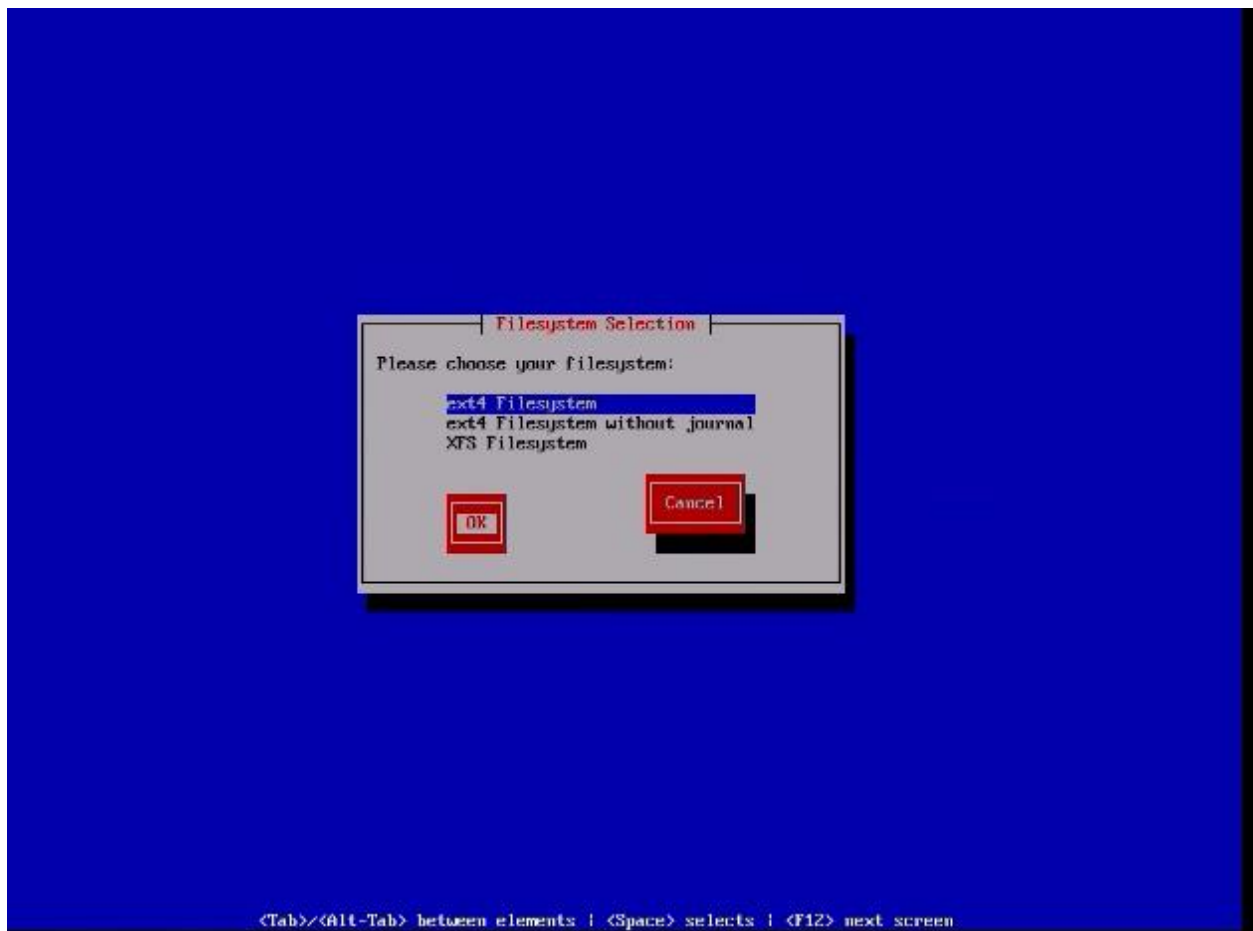


Figure 19:Open Source Firewall-Deployment of Firewall OS

- Deploying a Firewall OS involves installing the operating system onto a dedicated machine or virtual machine that will act as the Firewall.
- The installation process typically involves booting the machine from the IPFire Firewall ISO image. Once the installation is complete, the Firewall OS is ready to be configured.

2.) Restarting OS after setting inside & outside IP addresses:



Figure 20: Restarting OS after setting inside & outside IP addresses

- After the Firewall OS is deployed, the next step is configuring the network interfaces. This involves setting up the Firewall's inside and outside IP addresses, which are typically assigned to the green and red network interfaces, respectively. Once the IP addresses have been set, the firewall OS must be restarted for the changes to take effect.

3.) Configuration of Web Interface

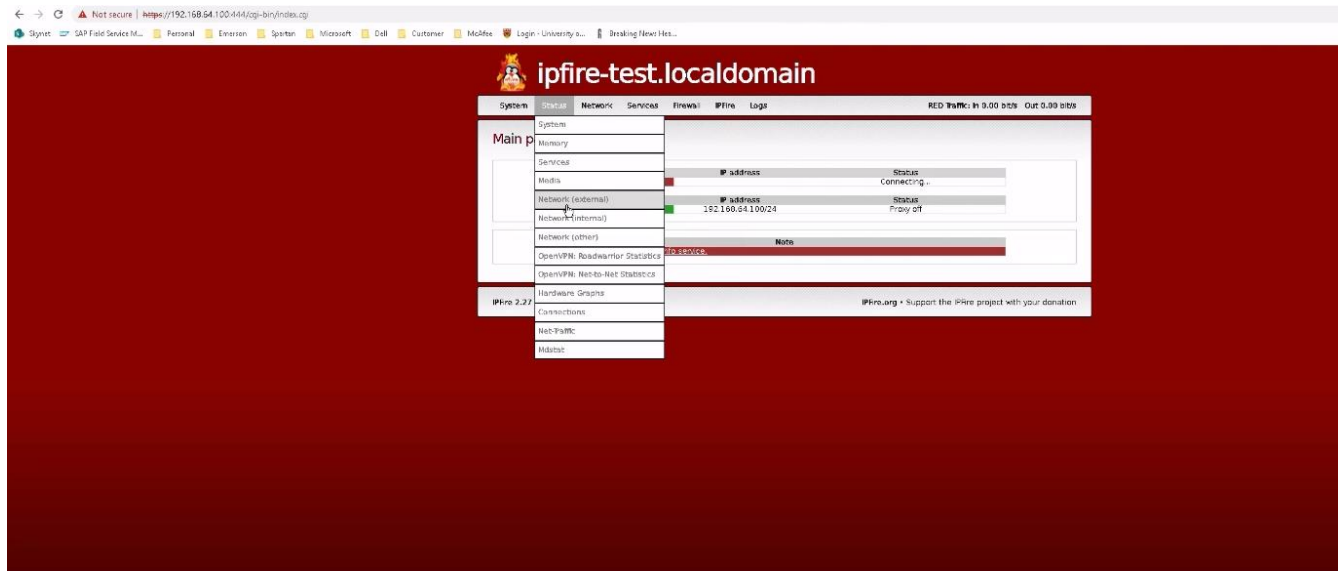


Figure 21: Configuration of Web Interface

- After the Firewall OS has been deployed and the network interfaces have been configured, the next step is to configure the web interface. The web interface allows users to manage the Firewall and configure its settings. The configuration process typically involves setting up the administrator account, configuring the network interfaces, and setting up any additional services required for the Firewall.

4.) Host Creation (Standard In Firewall)

ipfire-test.localdomain

System Status Network Services Firewall IPFire Logs RED Traffic: In 0.00 bit/s Out 0.00 bit/s

Hostname ?

Add a host

Host IP address: * 192.168.64.11 Hostname: * PROPLUS
Domain name: DELTAVIDCS Generate PTR: ☒
Enabled: ☒

* Required field Add

Current hosts

Host IP address	Hostname	Domain name	PTR	Action
192.168.64.10	PROPLUS	DELTAVIDCS	Yes	<input checked="" type="checkbox"/> [edit icon] [trash icon]

Legend: ☒ Enabled (click to disable) ☐ Disabled (click to enable) [edit icon] Edit [trash icon] Remove

IPFire 2.27 (x86_64) - Core-Update 172 IPFire.org • Support the IPFire project with your donation

Figure 22: Host Creation (Standard In Firewall)

- In a standard firewall setup, hosts refer to devices or machines on the network that require access to the Internet or other networks. Host creation involves setting up rules to allow or block traffic from specific hosts based on their IP address, MAC address, or other identifying information.

➤ Network Diagram

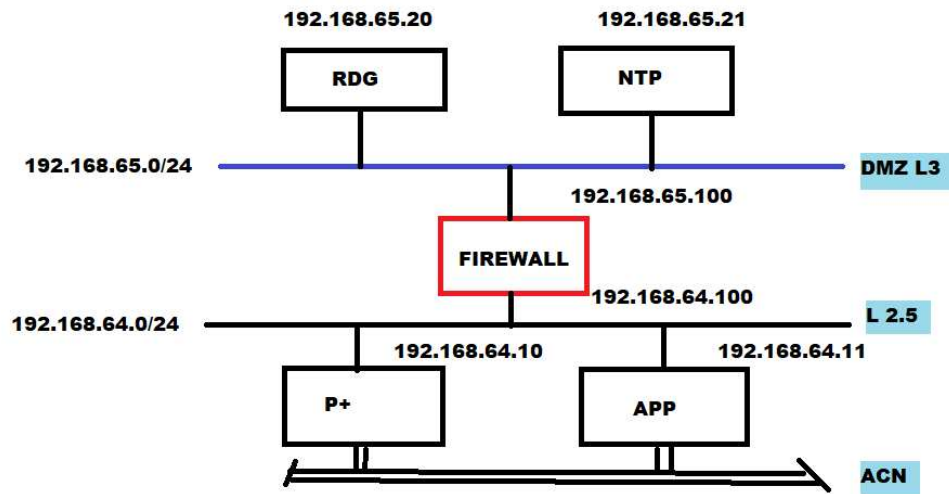


Figure 23:Network Diagram

5.) Creating Inside& Outside groups-Green/Red

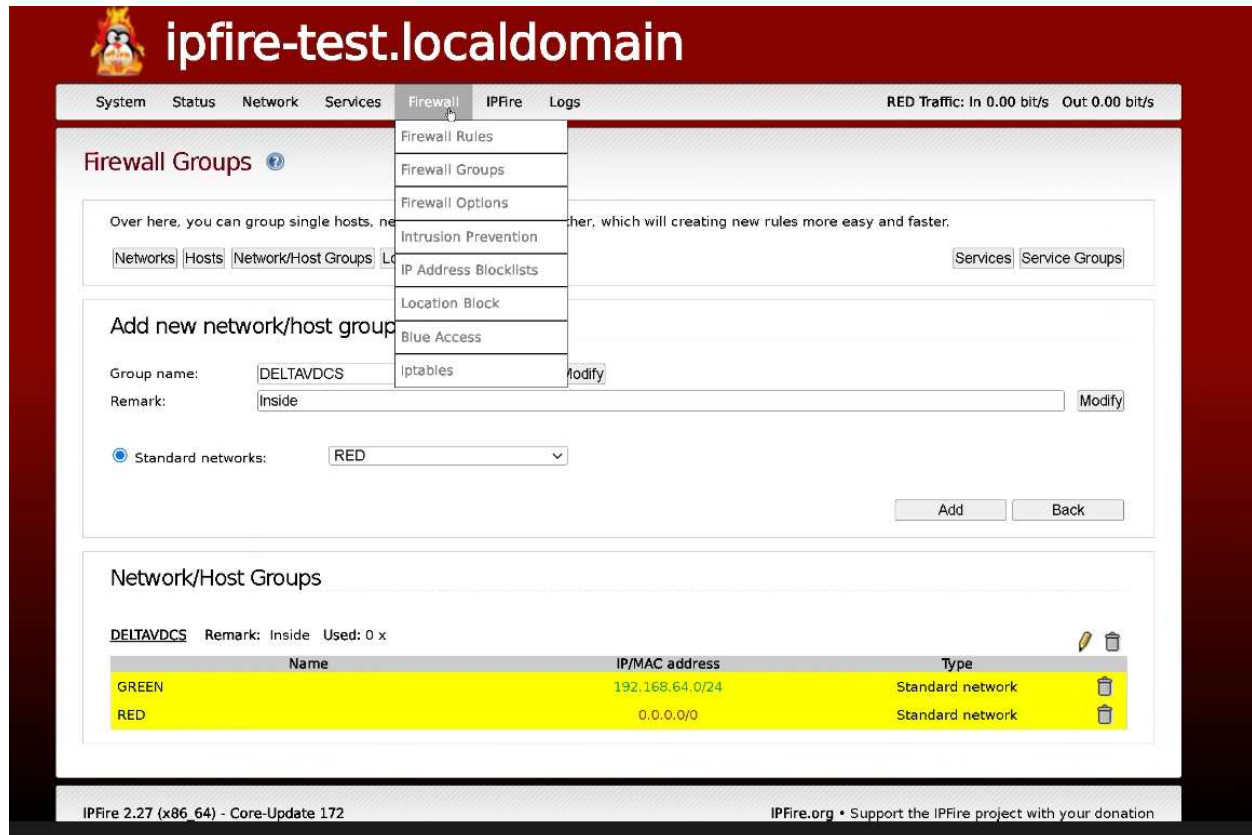


Figure 24: Creating Inside & Outside Groups

- After creating the host objects, inside (Green) and outside (Red) groups need to be created.
- Inside and outside groups refer to groups of hosts on the internal and external networks, respectively. These groups are typically used to define policies for traffic between internal and external networks. Creating inside and outside groups involves defining the hosts that belong to each group and setting up rules to control traffic flow between them.

6.) Creating Manual Hosts & Binding IP addresses with names

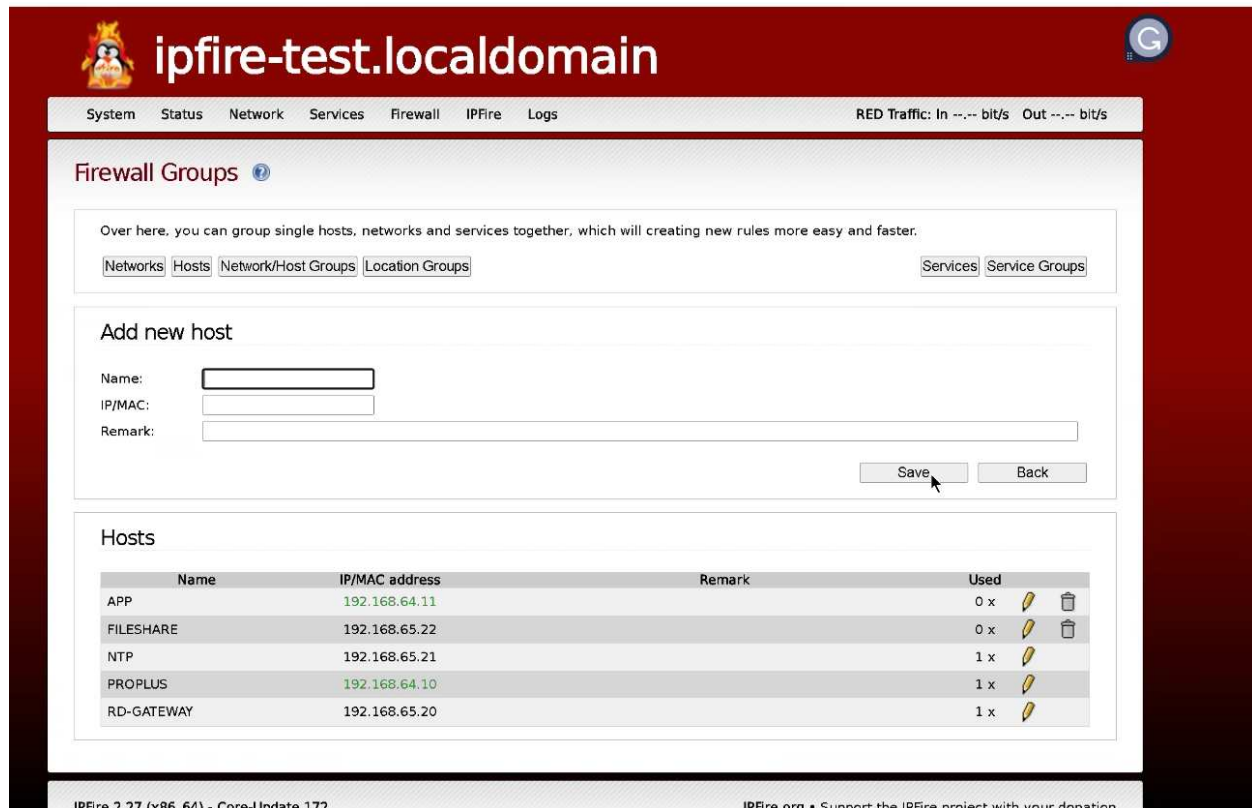


Figure 24: Creating Manual Hosts & Binding IP addresses with names

- Manual hosts refer to hosts that are not automatically discovered by the Firewall. These hosts can be added manually by specifying their IP address, MAC address, or other identifying information. Manual host creation is typically used for devices that do not support automatic discovery or for devices that require custom configuration settings. In addition to specifying the host's IP address, it is also common to bind a hostname to the IP address.

7.)Rule Creation

The screenshot displays a 'Rule Creation' form with the following sections:

- Source:** Includes radio buttons for 'Source address (MAC/IP address or network):', 'Standard networks:', 'Hosts' (selected), 'Network/Host Groups', and 'Location'. Each has a corresponding dropdown menu. The 'Firewall' radio button is also present with a dropdown set to 'All'.
- NAT:** A checkbox labeled 'Use Network Address Translation (NAT)'.
- Destination:** Similar to the Source section, with radio buttons for 'Destination address (IP address or network):', 'Standard networks:', 'Hosts' (selected), 'Network/Host Groups', and 'Location'. The 'Firewall' radio button is also present with a dropdown set to 'All'.
- Protocol:** A dropdown menu currently set to 'All'.
- Action:** A horizontal bar with three colored segments: green for 'ACCEPT', red for 'DROP' (selected), and cyan for 'REJECT'.
- Additional settings:** A section at the bottom for further configuration.

Figure 25:Rule Creation

- The final step is to create firewall rules. Firewall rules are used to control network traffic and involve setting up rules to allow or block traffic based on specific criteria, such as the source IP address, destination IP address, or port number. Rule creation is typically done using a graphical user interface, which allows users to define rules using a series of drop-down menus and input fields.

8.) Rule Summary

The screenshot displays the IPFire web interface for 'ipfire-test.localdomain'. The top navigation bar includes links for System, Status, Network, Services, Firewall, IPFire, and Logs. A status bar on the right shows 'RED Traffic: In 0.00 bit/s Out 0.00 bit/s'. The main section is titled 'Firewall Rules' and contains a 'New rule' button and an 'Apply changes' button. Below this is a table of Firewall Rules:

#	Protocol:	Source	Log	Destination	Action
1	TCP	RD-GATEWAY: 3389	<input type="checkbox"/>	PROPLUS	<input checked="" type="checkbox"/>
2	TCP	NTP: 123	<input type="checkbox"/>	DELTA VDCS	<input checked="" type="checkbox"/>
3	TCP	APP: 445	<input type="checkbox"/>	FILESHARE	<input checked="" type="checkbox"/>

Below the table, the status is 'GREEN' and the policy is 'Internet (Allowed)'. The footer shows 'IPFire 2.27 (x86_64) - Core-Update 172' and a link to 'IPFire.org'.

Figure 26: Rule Summary

- Once the rules have been created, a rule summary is typically generated, which provides a summary of the rules and their associated settings.

7.5 Node Protection:

In DeltaV DCS (Distributed Control System), nodes refer to the physical devices or components that make up the system. These nodes can be any combination of controllers, I/O (input/output) devices, operator workstations, network switches, or other components.[23][24]

Protecting nodes in a DeltaV DCS involves several measures to ensure the system's security and reliability. Here are some ways to protect nodes in a DeltaV DCS:

1. **Use Antivirus software:** Antivirus software helps to protect the DeltaV DCS nodes from malware and other cyber threats. Regularly update and scan the system to detect and remove any viruses or malware that may have infiltrated the system.
2. **Implement Patch Management:** Regularly updating DeltaV DCS nodes with security patches and firmware updates help to keep the system up-to-date and secure.
3. **Perform Regular Backups:** Regular backups of the DeltaV DCS system ensure that critical data is safe and can be quickly restored in the event of a system failure or cyber-attack.
4. **Implement Physical Security:** Physical security measures, such as surveillance cameras, access controls, and security personnel, can help prevent unauthorized access to the DeltaV DCS nodes.
5. **Implement Access Control:** Access control restricts access to DeltaV DCS nodes to authorized personnel only. Assigning user privileges and using strong passwords can help prevent unauthorized access to the system.[23][24]

7.5 (a.)Antivirus Software :

Using an antivirus solution is integral to protecting DeltaV DCS from cyber threats. In addition, using it with other security measures, such as access control, Firewall, and patch management helps to increase security.

It works by detecting and removing malware from the DeltaV DCS system. It scans the system for known malware signatures and suspicious behaviour, then removes any infected files or applications.[2][26]

To effectively protect DeltaV DCS, choosing antivirus software specifically designed for industrial control systems (ICS) is essential. ICS-focused antivirus solutions are designed to protect the unique requirements of DeltaV DCS and other industrial control systems.

The antivirus software should be configured to perform regular system scans, including critical files, operating systems, and applications. The software should also be configured to automatically update its virus definition files and software patches to ensure it is up-to-date and capable of detecting the latest malware threats.[2][26]

It is essential to regularly test and validate the antivirus software's effectiveness in protecting the DeltaV DCS system. Regular security audits and penetration testing can help identify vulnerabilities and ensure the antivirus software works as expected.

McAfee(now named Trellix) Antivirus is a specialized solution for Emerson's DeltaV DCS (Distributed Control System). It is intended to protect the system from malware, viruses, and other cyber threats that could compromise its operation.[2][26]

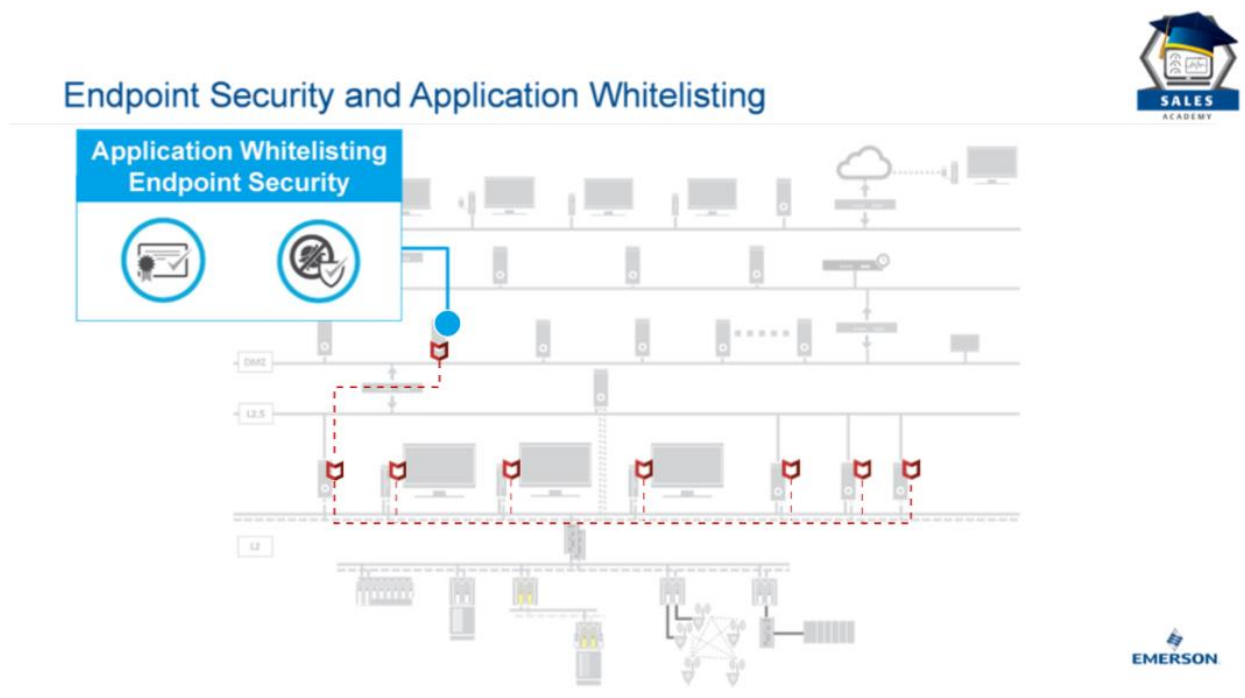


Figure 27:Endpoint Security & Application Whitelisting[24]

McAfee Antivirus software to protect DeltaV DCS (Distributed Control System) has the following functionalities:

1. Protection against malware: McAfee Antivirus software provides real-time protection against various types of malware, including viruses, worms, Trojans, and other cyber threats. This helps to prevent malware from compromising the DeltaV DCS system and causing damage to the industrial control process.[29][35]
2. Advanced threat detection: McAfee Antivirus software uses advanced threat detection techniques, including behaviour-based scanning and machine learning, to detect and block emerging threats that may not be identified by traditional signature-based antivirus software.[29]
3. Improved system performance: McAfee Antivirus software is designed to have a minimal impact on system performance, ensuring that DeltaV DCS can continue to operate efficiently without any slowdowns or disruptions caused by antivirus scanning.
4. Centralized management: McAfee Antivirus software provides centralized management and reporting capabilities, making it easy for system administrators to monitor the system's security status and quickly respond to any threats or issues.[29]
5. Integration with DeltaV DCS: McAfee Antivirus software is specifically designed to integrate with DeltaV DCS, ensuring that it can effectively protect the system without causing compatibility issues or disruptions.

Using McAfee Antivirus software to protect DeltaV DCS offers a comprehensive and effective solution for safeguarding industrial control processes against cyber threats.[2][29]

7.5.(b)Whitelisting:

Whitelisting is an effective way to prevent malware and other cyber threats from infiltrating a system because it restricts the ability of attackers to run malicious code. By allowing only trusted applications and processes to run, whitelisting can significantly reduce the risk of unauthorized access, data breaches, and other security incidents.

DeltaV DCS uses Application whitelisting, which involves creating a list of trusted applications that can run on a system. Any application that is not on the whitelist is automatically blocked.[28]



Figure 28:Endpoint Security & Application Whitelisting [24]

7.5(c.) Patch Management & Security Updating:

Installing patches and applying regular security updates is essential to maintaining the security of DeltaV DCS (Distributed Control System) and protecting it from cyber threats. Here's a brief overview of the patch installation process and regular security updates for DeltaV DCS:

1. **Patch installation:** Patches are software updates that fix bugs and security vulnerabilities in the DeltaV DCS software. To install patches, system administrators must download the patch files from the vendor's website and apply them to the system. Before applying patches, it is essential to test them in a non-production environment to ensure they do not cause any issues with the system.
2. **Regular security updates:** In addition to patches, regular security updates should be applied to DeltaV DCS to keep it protected against emerging cyber threats. These updates may include antivirus definitions, firewall rules, and other security-related configurations.
3. **Risk assessment:** Before applying any patches or security updates, assessing the risk associated with each update is essential. This involves evaluating the update's impact on the system's stability and security and determining the appropriate level of testing required.
4. **Change management:** Installing patches and security updates should follow a formal change management process to ensure that changes are appropriately documented, tested, and approved before being implemented in a production environment.
5. **Best practices:** It is essential to follow best practices such as regularly reviewing security logs, restricting access to sensitive data, and monitoring the system for any signs of suspicious activity to ensure that DeltaV DCS is always up-to-date and secure.

Overall, installing patches and applying regular security updates are critical to maintaining the security and stability of DeltaV DCS. System administrators should follow a formal change management process and best practices to ensure that updates are properly tested and implemented in a secure and efficient manner.[2][26]

7.6 Users

Educating employees on security best practices helps to prevent security breaches.

Ensure they understand the importance of strong passwords, the risks of opening suspicious emails, and the need to report suspicious activity.

Several types of training can be provided to users to help protect DeltaV Distributed Control Systems (DCS) from cyber-attacks. Some of the best training methods include:

1. Security awareness training: This training provides users with an understanding of the risks and threats associated with cyber-attacks. It covers topics such as phishing, malware, password management, social engineering, and other security best practices.
2. Role-based training: This type of training is customized based on the user's role in the organization. For example, administrators might receive training on configuring security settings, while end-users might receive training on identifying and reporting potential security threats.
3. Simulated attacks: Simulated attacks can be used to provide users with hands-on experience in identifying and responding to potential cyber-attacks. These simulated attacks can include phishing emails, social engineering attempts, and other types of attacks.
4. Regular refresher training: Regular refresher training can be provided to users to reinforce security best practices and ensure that they remain up-to-date with the latest threats and risks.
5. Testing and assessments: Regular testing and assessments can be used to evaluate the effectiveness of training programs and identify areas for improvement.

6. Incident response training: Incident response training provides users with an understanding of how to respond to a cyber-attack, including how to report incidents, isolate affected systems, and restore operations.
7. Password Management: Over time, passwords can become vulnerable to attacks due to factors such as human error, malicious attacks, or compromised systems. Regular password changes can help mitigate these risks by ensuring that passwords are not used for an extended period and reducing the likelihood of a password breach.

The frequency of password changes depends on the organization's security policies and the level of risk associated with the system. Changing passwords at least every 90 days is recommended, but some organizations may require more frequent password changes.[2][26]

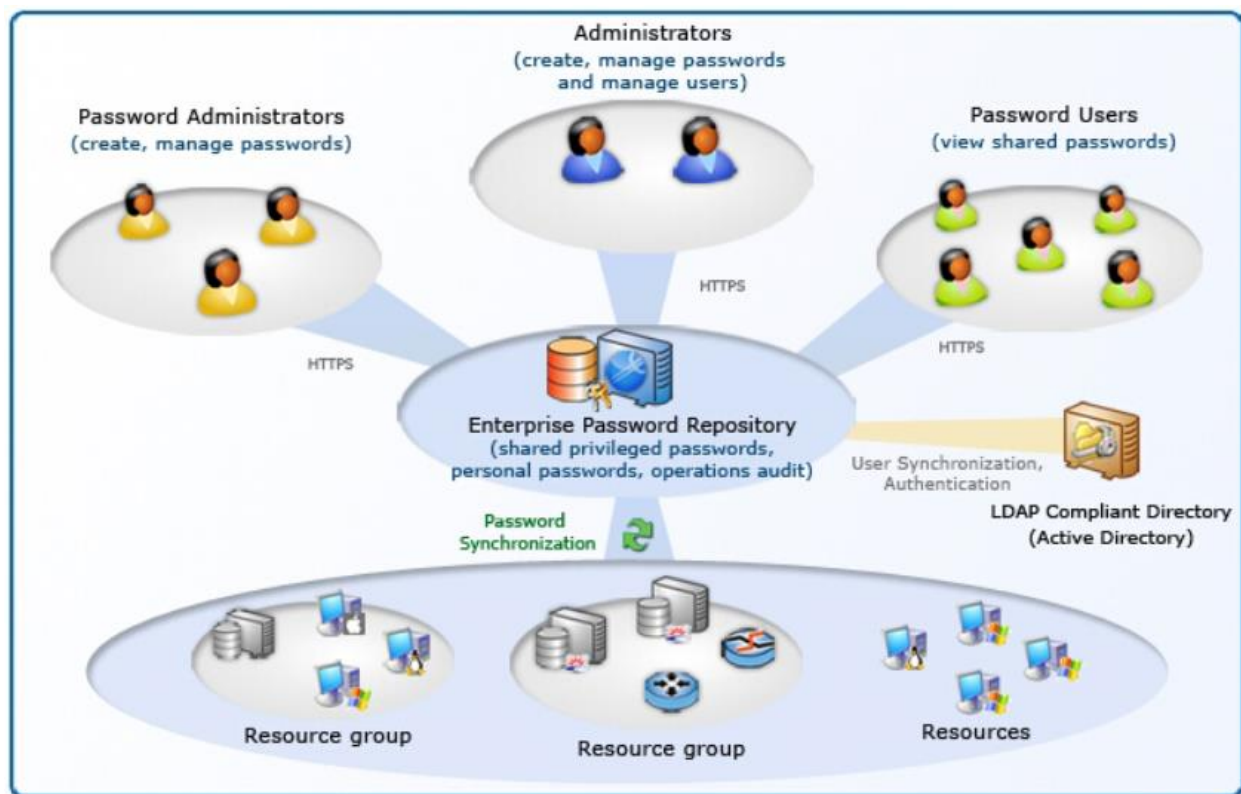


Figure 29: Password management solution for organization[31]

- It is also essential to ensure that users do not reuse old passwords or use weak passwords that are easy to guess. Passwords should be complex, unique, and challenging to crack to ensure that they provide adequate protection against cyber-attacks.
- By providing users with these types of training, organizations can help improve their overall security posture and reduce the risk of cyber-attacks on their DeltaV DCS. Therefore, it is essential to ensure that training is ongoing and that users remain vigilant in identifying and reporting potential security threats.
- Regular password changes are an essential aspect of password management and should be included in training for DeltaV DCS users. By following these best practices, users can help protect critical infrastructure components and prevent unauthorized access to the system.[2][26]

7.7 Monitoring :

NSN-Traffic Sniffing /Analysis

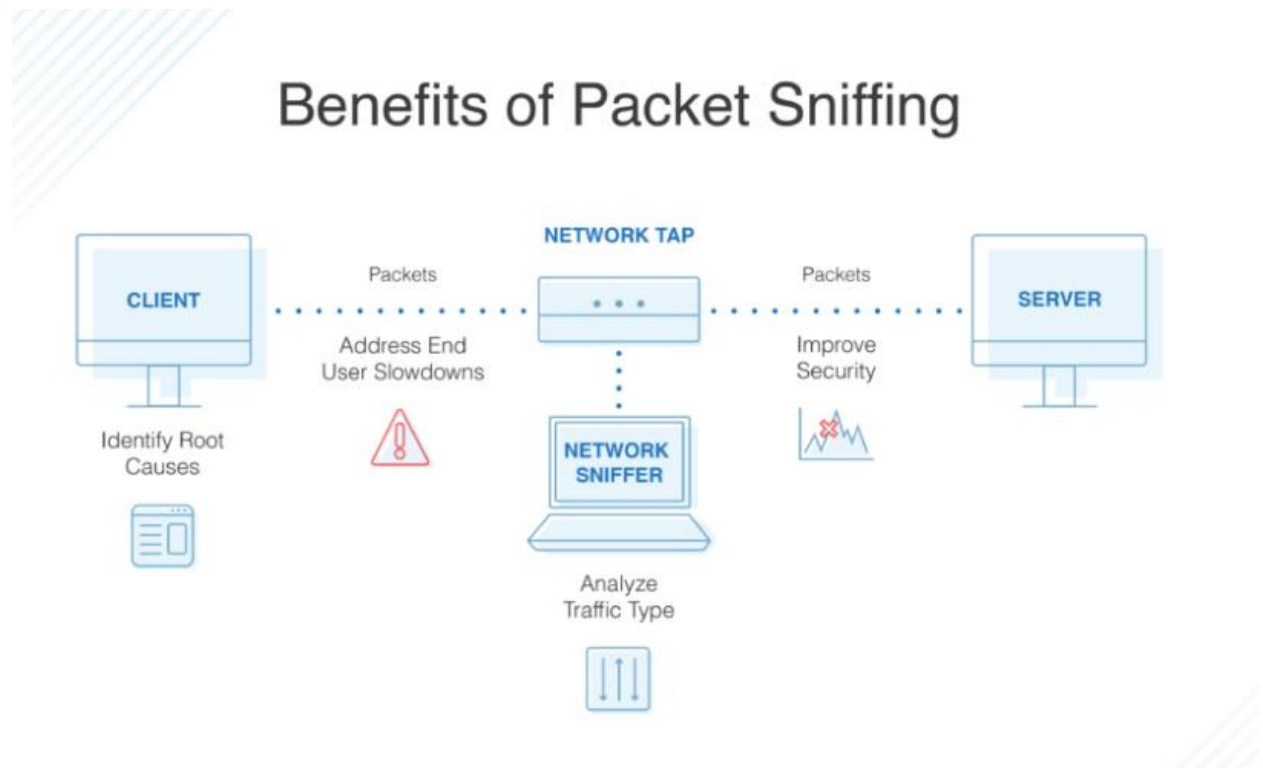


Figure 30:Packet Sniffers[32]

Network sniffers, also known as network analyzers or packet sniffers, are software tools or hardware devices used to capture and analyze network traffic. They can be used to monitor and analyze network traffic for various purposes, including troubleshooting network issues, monitoring network performance, and detecting and preventing cyber-attacks.[30]

In the context of DeltaV Distributed Control Systems (DCS), network sniffers can be beneficial in protecting the system from cyber-attacks in the following ways:

1. Detecting malicious traffic: Network sniffers can detect malicious traffic, such as malware or suspicious packets, that may be attempting to access the DeltaV DCS. By analyzing network traffic, sniffers can identify unusual traffic patterns and help administrators take appropriate action to prevent cyber-attacks.
2. Monitoring for unauthorized access: Network sniffers can be used to monitor network traffic and detect unauthorized access attempts to the DeltaV DCS. Administrators can identify suspicious login attempts or unusual network activity that may indicate a potential security breach by analyzing network traffic.
3. Analyzing system logs: Network sniffers can be used to capture network traffic and analyze system logs for potential security breaches. By analyzing network traffic and system logs, administrators can identify patterns of suspicious activity and take appropriate action to prevent cyber-attacks.
4. Mitigating network performance issues: Network sniffers can be used to monitor network performance and identify potential issues that may impact the performance of the DeltaV DCS. By analyzing network traffic, administrators can identify bottlenecks, network congestion, or other issues that may impact the system's performance and take appropriate action to resolve them.

Network sniffers can be a valuable tool in protecting DeltaV DCS from cyber-attacks. They can help administrators monitor network traffic, detect potential security breaches, and take appropriate action to prevent cyber-attacks. However, it's essential to ensure that network sniffers are used appropriately and configured correctly to avoid any unintended consequences or impact on system performance.[30]

Conclusion:

In this report, I have described an overview of the cyberattacks faced by Distributed Control Systems (DCS) and how organizations can protect their DCS from cyber threats.

Cybersecurity is a growing concern, and cyberattacks can cause organizations significant financial losses. With advancements in new technologies, hackers are also learning new ways to exploit vulnerabilities in DCS. By following good cybersecurity practices, which include following security policies and procedures, implementing the Purdue Model for secure system design, separating IT and OT systems, implementing a defence-in-depth strategy, conducting regular security risk assessments, and deploying security measures such as antivirus, whitelisting, patch management, and NSN sniffing monitoring. These measures can significantly reduce the risk of cyberattacks and protect organizations from potential financial and reputational harm.

As responsible employers, we must protect our organizations and control systems from cyberattacks by taking necessary cybersecurity training, reporting any vulnerabilities to management, and increasing awareness. By practicing suitable cybersecurity measures, we can avoid cyberattacks, ensure the safety and security of our operations, and protect our organization's reputation from the negative impact of cyberattacks.

References

- [1] Top 5 Advantages of a Distributed Control System(DCS System) - INSTBLOG.
<https://instrumentationblog.com/distributed-control-system-dcs-system/>
- [2] Delta V security manual "Implementing Security on Delta V Distributed Control Systems," Emerson,2013-2020
- © Emerson 2013-2020. All rights reserved.
- [3]Bela G.Liptak, Halit Eren. *Instrument Engineer's Handbook*. CRC Press, August 2011.
- [4]Management, Emerson Process. *DeltaV Digital Automation System Guidebook*. n.d.
- [5]*DeltaV RWB*. n.d.
- [6] Emerson's DeltaV Digital Automation System - Process Industry Forum. (2018, October 22). Retrieved from <https://www.processindustryforum.com/article/emersons-deltav-digital-automation-system#:~:text=DeltaV%20is%20Emerson's%20Digital,within%20an%20end%20user%20environment.>
- [7] Risk terminology: Understanding assets, threats, and vulnerabilities
HYPERLINK "https://www.vigilantsoftware.co.uk/blog/risk-terminology-understanding-assets-threats-and-vulnerabilities" <https://www.vigilantsoftware.co.uk/blog/risk-terminology-understanding-assets-threats-and-vulnerabilities>
- [8] Wesley Chai, Confidentiality, integrity, and availability (CIA triad)-
<https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA>
- [9] Confidentiality, Integrity, And Availability – The CIA Triad
<https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/>
- [10] Top 5 Computer Security Vulnerabilities,
<https://www.compuquip.com/blog/computer-security-vulnerabilities>
- [11] Why OT Environments Are Getting Attacked And What Organizations Can Do About It
<https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/why-ot-environments-are-getting-attacked-and-what-organizations-can-do-about-it/#:~:text=Weak%20passwords%3A%20OT%20devices%20lack,unchanged%20default%20use,rnames%20and%20passwords.>

[12] Defending Against Cyberattacks On Operational Technology, Ryan Moody

<https://www.forbes.com/sites/forbestechcouncil/2021/10/28/defending-against-cyberattacks-on-operational-technology/?sh=382bc74b5e76>

[13] Triton Malware Spearheads Latest Attacks on Industrial Systems | McAfee Blogs. (n.d.).

Retrieved from <https://www.trellix.com/en-us/about/newsroom/stories/research/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems1.html>

[14] <https://uniserveit.com/>. (2021, September 22). The CIA Triad of Information Security: An Overview. Retrieved from <https://uniserveit.com/blog/the-cia-triad-of-information-security>

[15] CoLtd, A. E. (n.d.). Six ways to spot social engineering - ATCKIT. Retrieved from <https://atckit.com/thi-truong-cong-nghe/thi-truong/109-6-cach-phat-hien-tan-cong-phi-ky-thuat.html>

[16] What is Advanced Malware and How Do I Find and Remove It? (n.d.). Retrieved from <https://home.sophos.com/en-us/security-news/2020/does-malware-exist>

[17] CPNI-Centre for protection of National Infrastructure. (2010, November). Configuring and Managing Remote Access for Industrial Control Systems. Retrieved from https://www.cisa.gov/uscert/sites/default/files/recommended_practices/RP_Managing_Remote_Access_S508NC.pdf

[18] Magnusson, A. (2023, February 13). Man-in-the-Middle (MITM) Attack: Definition, Examples & More. Retrieved from <https://www.strongdm.com/blog/man-in-the-middle-attack>

[19] Vojtko, M. (2021, February 24). Everything You Need to Know About ARP Spoofing. Retrieved from <https://www.thesslstore.com/blog/everything-you-need-to-know-about-arp-spoofing/>

[20] M. (2021, June 10). Develop Policies for an All-round Approach to Information Security - Information Security Blog - 7Security. Retrieved from <https://www.7sec.com/blog/develop-policies-for-an-all-round-approach-to-information-security/>

[21] What Is the Purdue Model for ICS Security? | Zscaler. (n.d.). Retrieved from <https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security>

[22] P. (2022, October 14). What is SCADA? Supervisory Control And Data Acquisition. Retrieved from <https://plcynergy.com/what-is-scada/>

[23] Introduction to Networking in Industrial Control Systems, Bootcamp, 2022

[24] DeltaV Cybersecurity Solutions-Emerson Process World

ProcessWorld - Your Connection to Global Information. (n.d.-b). Retrieved from
<https://processworld.emersonprocess.com/>

[25] What Is Firewall: Types, How Does It Work, Advantages & Its Importance

<https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall>

[26] Emerson. (n.d.). PSS DV - CS L1 - Cybersecurity Associate Certification Path.

[27] IPFire.org - IPFire Development Team. (n.d.). Introduction - The IPFire Wiki. Retrieved from <https://wiki.ipfire.org/configuration/firewall/introduction>

[28] Reasons for implementing identity and access management.

<https://macpaw.com/how-to/identity-access-management>

[29] Antimalware: Protecting Your Devices from Malicious Software.

<https://www.delfinuniverse.com/2023/02/antimalware-protecting-your-devices.html>

[30] Network Sniffers: What Are They and How Can I Use Them? | PagerDuty. (2020, September 16). Retrieved from <https://www.pagerduty.com/resources/learn/what-are-network-sniffers/>

[31] M. (n.d.). Privileged password management solution |Privileged user account manager. Retrieved from

<https://www.manageengine.com/products/passwordmanagerpro/privileged-password-manager.html>

[32] Contributor, S. (2021, December 15). 10 Best Packet Sniffers - Comparison and Tips - DNSstuff. Retrieved from <https://www.dnsstuff.com/packet-sniffers>

[33] What Is a Firewall? (2023, February 8). Retrieved from

<https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>

[34] Firewall: The First Line of Defense Against Cyber Attacks.

<https://www.linkedin.com/pulse/firewall-first-line-defense-against-cyber-attacks-shahidul-islam>

[35] Antimalware: Protecting Your Devices from Malicious Software.

<https://www.delfinuniverse.com/2023/02/antimalware-protecting-your-devices.html>

