Mälardalens University, Västerås

The School of Innovation, Design and Engineering

Network Security – DVA 498

Volvo Construction Equipment Scenario Security Measures

Students: Haris Adrović, Valento Bardhoshi

Examiner: Abbas Arghavani, Johan Åkerberg

Västerås, Year 2025, March.

1. Introduction

This report provides a comprehensive security analysis of Volvo Construction Equipment's (VCE) Scenario, focusing specifically on the iAssist functionality. The document details the network architecture, key data flows, assets, threat analysis, and risk assessment—all culminating in a set of recommended security controls to ensure the confidentiality, integrity, and availability of iAssist data and services. The Scope covers on-site network at the construction site (5G Access Point, Edge/Fog server, Controllers, switches, Routers, Firewalls and MCHs (Machines)), Machine data-flows (DF1,DF2,DF5,DF6) directly involved in iAssist's local feedback loop and critical assets including machine efficiency data, iAssist Service, Recommendations, Fog/Edge Server, 5G access Tower, HMI Controller and MCH Load and Engine Sensors.

Furthermore, this report provides specific recommendations such as multi-factor authentication (MFA), encryption, firmware signing, and role based access controls to strengthen the general security of the system. The goal is to show how practical security practices can be woven into existing workflows without causing undue strain on everyday operations. Ultimately, a proactive security strategy not only ensures smooth functionality for iAssist but also reinforces the trust and reliability of the entire on-site infrastructure, promoting safer, more efficient construction activities for VCE and its partners.

The deployment of advanced wireless technologies such as 5G in industrial environments introduces significant cybersecurity considerations. Techniques such as beamforming and Multiple-Input Multiple-Output (MIMO) in 5G can enhance network reliability, capacity, and security. Beamforming directs signals specifically to intended devices, reducing the risk of interception, while MIMO provides spatial multiplexing for improved network resilience and resistance to certain types of denial-of-service (DoS) attacks.

Additionally, in this scenario, deploying Network Access Control (NAC), VLAN segmentation, robust firewall rules, and intrusion detection/prevention (IDS/IPS) is crucial to secure every layer of communication. These measures safeguard iAssist's data flows and ensure that only authorized devices connect to the site network, minimizing both internal and external threats.

2. Scenario overview

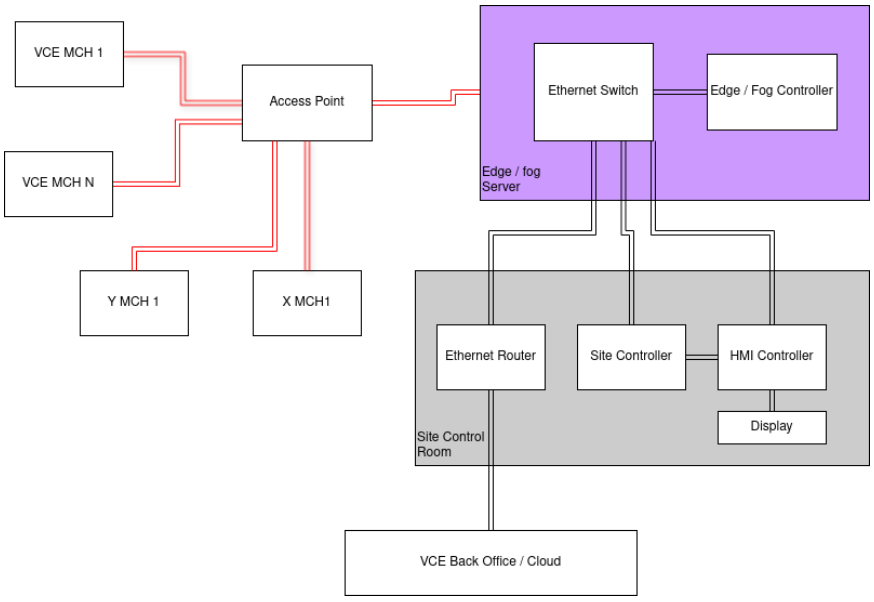
High-Level Architecture

1. Site: The physical construction location with multiple MCHs .

2. Access Point (5G): Provides wireless connectivity to all MCHs.

3. Site Control: Houses an Ethernet switch, Ethernet Router Edge/Fog server (running iAssist), an HMI controller, and optional site controllers for safety signals

4. VCE Back Office: A cloud solution owned by Volvo CE, storing machine data (e.g., productivity, diagnostics) and offering some remote services.



Topology Overview - Figure 2.1

The focus on a 5G access Point (AP) implies leveraging modern, high throughput, low latency wireless technology. This is especially critical when up to 20 machines simultaneously transmit sensor data to the Edge/Fog server. The network also includes standard industrial components (switches, routers, controllers, firewalls) typical in an OT setup. Any single point of failure—especially the 5G AP or Fog server—could cripple iAssist's real-time feedback loop. Meanwhile, the VCE Back Office is used primarily for long-term analytics and storage, but it's not the main focus for local real-

time data. In such a setting, localized security measures (like strict segmenting and controlling traffic to/from the 5G AP) become paramount **[1]**.

From a cybersecurity perspective, utilizing advanced 5G features such as beamforming and MIMO provides inherent protections by reducing signal dispersion and making it difficult for unauthorized devices to intercept communication. Beamforming significantly improves security by spatially targeting communication only towards authenticated, intended machines, thus minimizing the wireless attack surface. MIMO further enhances data reliability and integrity through redundant signal paths.

Furthermore, segmenting the network with VLANs prevents broadcast storms or MAC flooding from disrupting performance. By combining 5G security features with VLAN isolation and enforcing 802.1X NAC on switch ports, the environment is protected against unauthorized device access and VLAN hopping attacks. Trunk ports must also be strictly configured to block rogue connections.

3. iAssist Functionallity & Data Flow in Focus

The iAssist Processes raw sensor data locally on the Fog/Edge server and returns real-time fedbaack to machine operators (DF1,DF2), while the Site operators can issue queries (DF5) and receive data back (DF6).
While the original documentation lists DF1–DF6, this report particularly focuses on local flows:

1. DF1: Sensory Data
    - VCE MCH 1 -> 5G AP -> Ethernet Switch -> Edge/Fog Controller
    - Telemetry from the machine's sensors (e.g., load, engine parameters) going into iAssist for real-time analytics.
2. DF2: Feedback & Recommendations
    - Edge/Fog Controller -> Ethernet Switch -> 5G AP -> VCE MCH 1
    - iAssist output returning to the MCH operator, guiding improvements in machine usage.
3. DF5: Request from Site Operator
    - Display -> HMI Controller -> Ethernet Switch -> Edge/Fog Controller
    - An on-site operator requests machine data or iAssist analytics results.
4. DF6: Data for Site Operator

- Edge/Fog Controller -> Ethernet Switch -> HMI Controller -> Display
- iAssist's response displayed to on-site personnel (e.g., efficiency scores, recommended actions).

(DF3 and DF4 involve the VCE Back Office, mostly relevant for remote data requests/storage.)

There are predefined data flow constraints:

- Feedback to MCH must arrive within 100 ms.
- Data requests from the site operator or the VCE Back Office must be fulfilled within 1 second (or 5 seconds if iAssist needs to spin up).
- Up to 20 MCHs operating simultaneously, each requiring stable connectivity.

Since these data flows demand low latency, a flood or jamming attack on the 5G link can halt iAssist's real-time feedback. To mitigate such denial-of-service risks, advanced 5G security settings, a fallback wired link should be implemented and an IDS/IPS capable of spotting malicious traffic are recommended.

4. Asset Identification

In this particular scenario, we defined 8 assets with their Security Objective:

Reference Number	Asset Name	Description	Security Objective
A1	Mahcine Efficiency Data	Processed metrics about how effectively each machine is operating (e.g., bucket load utilization, cycle times). Typically transmitted from the MCH to iAssist and possibly forwarded to the VCE Back Office.	Integrity & Confidentiality
A2	Iassist Service	The software and processes running on the Fog/Edge Server that collect raw data , perform analytics, and generate reccomendations for MCH operators.	Availability & Integrity
A3.1	MCH Load Sensor	A specific onboard sensor measuring load weight (e.g., how many stones are in the bucket). This data is a key input to calculating machine efficiency and generating operator feedback.	Integrity & Confidentiality
A3.2	MCH Engine Sensor	Another specific onboard sensor monitoring engine parameters (e.g., RPM, temperature, fuel consumption). Used by iAssist for	Integrity & Confidentiality

		performance optimization and possibly predictive maintenance.	
A4	5G Tower	The on-site 5G wireless infrastructure (base station/tower) providing connectivity for the machines. Often shared among multiple OEMs.	Integrity & Availability
A5	Fog/Edge Server	The physical or virtual server that hosts iAssist, handles local data processing, and interacts with both the MCH sensors and the VCE Back Office.	Integrity & Availability
A6	Recommend ations	The feedback iAssist provides to the MCH operator or the site operator (e.g., instructions to improve loading efficiency).	Integrity & Confidentiality
A7	HMI Controller	The Human-Machine Interface controller that sends requests to the edge server (DF5) and displays data (DF6) to the site operator. Often includes an ECU running control algorithms and a display for real-time monitoring.	Integrity & Confidentiality

After defining the assets and data flow in this scenario, we can proceed with the TARA approach (Threat Analysis and Risk Assessment). For the Threat Analysis we utilize the STRIDE approach (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) for each asset, focusing primarily on data flows DF1, DF2, DF5, DF6 and how an attacker might exploit them.

Each asset can pose a different level of risk depending on how it's targeted. For instance, A1 (Machine Efficiency Data) is integral to generating correct recommendations, so data tampering could cause immediate operational issues. A2 (iAssist Service) is the "brain" of the system; a successful DoS attack here halts all real-time feedback. Meanwhile, A5 (Fog/Edge Server) is a prime target because compromising it can grant an attacker insight into, or control over, nearly all data flows. Notably, the HMI (A7) is often overlooked but is a vital link in on-site command and control. Strengthening operator authentication via MFA is essential to prevent unauthorized or spoofed requests from manipulating iAssist or receiving sensitive data.

In addition, positioning an IDS/IPS behind the Fog/Edge server helps detect anomalies in sensor traffic, preventing exploit attempts on the server OS. Equipping the HMI network segment with NAC (802.1X) further ensures only valid operator devices connect, reducing exposure to spoofed controllers.

5. Threat Analysis

Asset ID	Damage Scenario	STRIDE Category	Threat Scenario	Attack Path	Elapsed Time	Expertise	TOE	Window of Opportunity	Equipment
A1	False or tampered efficiency data leads to poor decisions, decreased productivity, or potential safety issues.	T (Tampering)	An attacker intercepts or injects fake efficiency data (DF1) to manipulate performance metrics.	1) Gain access to the 5G link or site LAN 2) Modify packets carrying machine efficiency data in transit	<= 1 day	Proficient	Restricted Information	moderate	Standard
A2	If iAssist is taken offline (DoS), operators lose real-time feedback, halting efficiency improvements and possibly impacting safety.	D (Denial of Service)	Attackers overwhelm iAssist with excessive traffic or exploit a vulnerability to crash the service.	1) Flood the Fog/Edge server's network interface 2) Exploit OS/service vulnerabilities to force reboots or lock-ups	<= 1 day	Layman	Public Information	easy	Standard
A3.1	Fake load readings cause inaccurate efficiency data and potentially unsafe load operations.	T (Tampering)	Attacker modifies load sensor output by compromising sensor firmware or intercepting internal MCH bus.	1) Physical or firmware-level tampering of sensor 2) Manipulate data before it's sent to iAssist	<= 1 week	Expert	Restricted Information	Difficult	Specialized
A3.2	Altered engine data leads to incorrect performance calculations or missed maintenance, risking machine damage or suboptimal usage.	T (Tampering)	An attacker injects false engine data via sensor compromise or local bus interception.	1) Exploit vulnerabilities in MCH sensor firmware 2) Inject malicious data on the bus	<= 1 month	Expert	Restricted Information	Moderate	Specialized

A4	A jamming or flooding attack could disrupt all machine communications, crippling iAssist feedback loops and site operations.	D (Denial of Service)	Attackers jam or flood the 5G spectrum, or impersonate the tower to disrupt legitimate traffic.	1) High-powered radio interference or rogue base station 2) Overload tower software or control channel	<= 1 day	Proficient	Public Information	Easy	Specialized
A5	A compromise of the server can yield false analytics or block iAssist entirely, halting real-time optimizations.	E (Elevation of Privilege)	Attackers gain root/admin on the Edge server via OS or application exploit, altering or disabling services.	1) Exploit unpatched vulnerabilities 2) Achieve persistent admin access (steal credentials, rootkits, etc.)	<= 1 month	Expert	Strictly Confidential Information	Difficult	Specialized
A6	If recommendations are tampered with, operators could follow unsafe or incorrect instructions; leaks might reveal proprietary strategies.	T (Tampering)	Attackers inject false recommendations or alter them in transit (DF2, DF6).	1) Intercept recommendation messages in transit 2) Modify or spoof data before it reaches operator/HMI	<= 1 day	Proficient	Restricted Information	Moderate	Standard
A7	A compromised HMI might show falsified site data or leak sensitive operational info, leading to poor decisions or sabotage.	T (Tampering)	Malware or firmware hack on HMI manipulates displayed data or intercepts user input.	1) Physical access to HMI ports or OS 2) Malicious software update or local network exploit	<= 1 week	Proficient	Restricted Information	Moderate	Standard

For lateral movement inside the site network, VLAN hopping and unauthorized plug-ins on switch ports pose serious risks. Implementing NAC at Layer 2 (802.1X) and limiting trunk privileges effectively blocks unapproved devices and stops VLAN-based attacks.

The STRIDE-based analysis highlights how Denial of Service (DoS) and Tampering are particularly critical in this environment**[2]**. MCH sensors, the iAssist service itself, and the HMI each present unique avenues for disruption. Attacks on sensors (A3.1, A3.2) compromise the integrity of data at the source, while direct sabotage of the HMI (A7) deceives operators. Gaining root on the Fog/Edge server (A5) is especially devastating, allowing an attacker to manipulate or block all local data flows. These threats underscore the need for strong authentication (potentially MFA) to restrict who can alter critical systems or access sensitive data.

Our assessment leveraged a detailed cybersecurity framework, considering potential vulnerabilities within firmware management, wireless infrastructure including beamforming and MIMO usage, and device-level security practices. Risks were quantitatively evaluated by scoring likelihood and potential cybersecurity impact, prioritizing areas where specialized knowledge or sophisticated cyber equipment significantly raises threat levels.

6. Risk-Assessment

Asset ID	Threat Scenario	Likelihood	Impact	Risk Level	Risk Treatment Decision	Risk Treatment Action	Cybersecurity Goals
A1	Injecting fake efficiency data (Tampering)	Medium	High	High	Mitigate	-End-to-end encryption (TLS/IPsec) -Digital signatures/MAC on data - Network segmentation/firewalls	-Ensure data integrity (no manipulation) -Protect confidentiality (prevent unauthorized viewing)
A2	Overloading iAssist with DoS traffic	Medium	High	High	Mitigate	-Rate limiting & load balancing - IDS/IPS to detect abnormal traffic -High availability cluster for the Fog server	-Maintain availability of real-time analytics -Prevent major service interruptions
A3.1	Modifying load sensor output (Tampering)	Medium	Medium	Medium	Mitigate	-Secure firmware with signing - Encrypt sensor output -Physical tamper protection if possible	-Preserve integrity of sensor data -Prevent malicious manipulations
A3.2	Injecting false engine data (Tampering)	Medium	Medium	Medium	Mitigate	-Signed or encrypted data -Harden MCH bus communications -Firmware update controls	-Maintain data integrity -Detect sensor anomalies early
A4	Jamming or flooding the 5G Tower (DoS)	Medium	High	High	Mitigate	-Anti-jamming/ frequency hopping -Hardening base station SW -Network slicing & QoS for critical traffic	-Ensure availability of wireless link -Maintain connectivity for iAssist flows

A5	Gaining root/admin on Fog/Edge Server (Elevation of Privilege)	Low	High	Medium	Mitigate	-OS/application patching & hardening -Least privilege & strong authentication - Monitoring (IDS) & logging MFA for all privileged logins (local or remote) to prevent stolen credentials from granting root-level access.	-Protect integrity of analytics and configuration -Ensure availability of iAssist
A6	Injecting false recommendations (Tampering)	Medium	High	High	Mitigate	-Encrypt & sign recommendation payload - Validate authenticity at MCH/HMI -Use secure comms channels (TLS)	-Ensure integrity of instructions -Protect confidentiality of operational strategies
A7	Malware on HMI to display fake data (Tampering)	Medium	High	High	Mitigate	-Secure OS (disable unnecessary ports/services) -Digital signing of HMI firmware - Role-based access control MFA for all HMI logins (operator, admin) to preserve integrity of displayed info	-Preserve integrity of displayed info -Protect confidentiality of site data

This table shows how each asset's "Mitigate" decision is driven by the potential for immediate operational harm. For example, A1 (machine efficiency data) has a High impact if compromised because incorrect metrics degrade both safety and efficiency. Similarly, A2's high-level DoS risk stems from its direct effect on real-time feedback.

Taken together, these threats target 5G availability, NAC-lacking networks, or unpatched Fog/Edge servers. Layered defenses—VLAN isolation, NAC, encryption (IPsec or TLS), and intrusion prevention—address these risks while respecting the real-time constraints of iAssist.

The defense-in-depth strategy, combining NAC, VLAN isolation, IP filtering, encrypted traffic, and restricted authentication, reflects recommendations for layered safeguards found in NIST SP 800-53 [2].

7.Security Recommendations

7.1 Protecting MCH Sensors (A3 & A4)

1. Firmware Signing: Ensure load/engine sensors have secure firmware updates, preventing malicious modifications.
2. Encrypted Data Output: If feasible, implement encryption or signing at the sensor-level, ensuring integrity before the data leaves the MCH.

7.2 Ensuring Integrity of Recommendations (A7, DF2)

1. Mutual Authentication: iAssist server and MCH must verify each other's identity, e.g., using X.509 certificates.
2. End-to-End Encryption: Use TLS/IPsec for recommendations so attackers can't inject false instructions.

7.3 Mitigating DoS on 5G (A5)

1. Private 5G or Network Slicing: Use dedicated QoS and slicing features if available, limiting the impact of jamming/flooding.
2. Fallback Communication: A wired or secondary wireless link for critical signals if the 5G link is compromised.

7.4 Hardening the Fog/Edge Server (A2, A6)

1. OS Security: Regular patching, minimal services, intrusion detection.
2. Least Privilege: Only essential iAssist processes have elevated rights, and remote management is restricted.
3. Logging & Monitoring: Track unusual patterns in sensor data or system calls, facilitating quick incident response.
4. MFA for Adming Logins: Require multi-factor authentication (e.g., password plus time-based OTP) to access the Fog/Edge server's administrator account, preventing a single stolen credential from granting full control.

7.5 Securing the HMI (A8)

1. Role-Based Access: Operators vs. admins vs. read-only roles, preventing unauthorized data requests or commands.
2. Secure Boot/Firmware: The HMI controller's software stack should be signed/verified at startup.
3. Physical Security: Since HMIs might be physically accessible on-site, lock down ports and use tamper-evident seals.
4. MFA for HMI Logins: Enforce multi-factor authentication when operators or administrators log into the HMI, ensuring that a stolen password alone cannot grant access to critical controls or data.

There are aditional Security Reccomendations that could help secure the network:

-Network Segmentation (VLAN)

1. Split the network so that MCH sensors, Fog/Edge server, and HMI each reside in separate VLANs.
2. Restrict trunk ports to prevent VLAN hopping.
3. Limit broadcast storms or MAC flooding by confining them to a smaller domain.

-NAC (802.1X)**[4]**

1. Enforce Layer 2 authentication on switch ports.
2. Only recognized machines (MCH, HMI, admin workstations) can join.
3. Blocks rogue or spoofed devices from trivially accessing the site network.

-IDS/IPS Deployment

1. Position an intrusion detection/prevention system behind the Fog/Edge server or at the 5G uplink.
2. Monitor sensor data flows for anomalies or exploit signatures, blocking suspicious traffic.
3. Provide real-time alerts if unexpected scanning or infiltration is detected.

Web Application Firewall (WAF)

1. If the iAssist or HMI uses a web-based front end, deploy a WAF to filter HTTP(S) traffic.
2. Mitigates injection (SQLi) or cross-site scripting attacks, preserving the integrity of operator interfaces and iAssist recommendations.

This cybersecurity-focused assessment of Volvo CE’s connected construction equipment and iAssist system highlights the necessity of rigorous security practices tailored for industrial IoT environments. By identifying critical vulnerabilities, such as risks associated with sensor firmware tampering, wireless communication attacks including those mitigated by advanced 5G techniques like beamforming and MIMO, and unauthorized system access, we've proposed a layered defense strategy. Our recommended security measures—encompassing robust encryption, cryptographic firmware management, advanced 5G security implementations, comprehensive authentication methods, and meticulous monitoring—collectively enhance resilience against sophisticated cyber threats. Moving forward, continuous cybersecurity improvements including real-time anomaly detection, advanced security analytics, and adoption of zero-trust security architectures are strongly recommended to further strengthen the operational security posture.

8.Simulation (Cisco Packet Tracer)

In this simulation, the Volvo CE iAssist environment is modeled with two discrete firewalls to shield different segments of the network. Starting from the VCE Back Office, represented by a Server-PT node at 192.168.5.2/30, traffic flows through a “internet-like” Cisco 2911 router that holds three subnets: one connected to the Back Office at 192.168.5.x, one reaching a malicious node at 192.168.6.x, and one leading to the first firewall at 192.168.0.x. Each subnet is /30, ensuring a clear demarcation at the router interfaces.

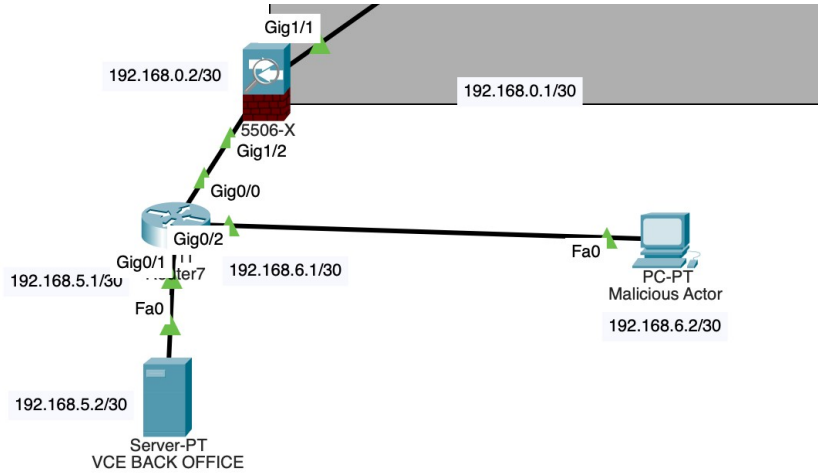


Figure 8.1 – Simulating the Internet

This router stands in for an external WAN or ISP link, simulating what the iAssist environment would face in a real deployment.

Once traffic leaves the 2911 router on 192.168.0.x, it encounters the first firewall, which is tasked with defending the construction site from general internet threats. This firewall holds the IP 192.168.0.2/30 on its outside interface, facing the 2911 router’s 192.168.0.1/30. On its inside interface, it uses 192.168.2.2/30 to connect with an inside router (ISR4331) at 192.168.2.1/30. Simple yet strict ACLs or Security Levels define what inbound connections are allowed from the external side, effectively blocking all nonessential ports.

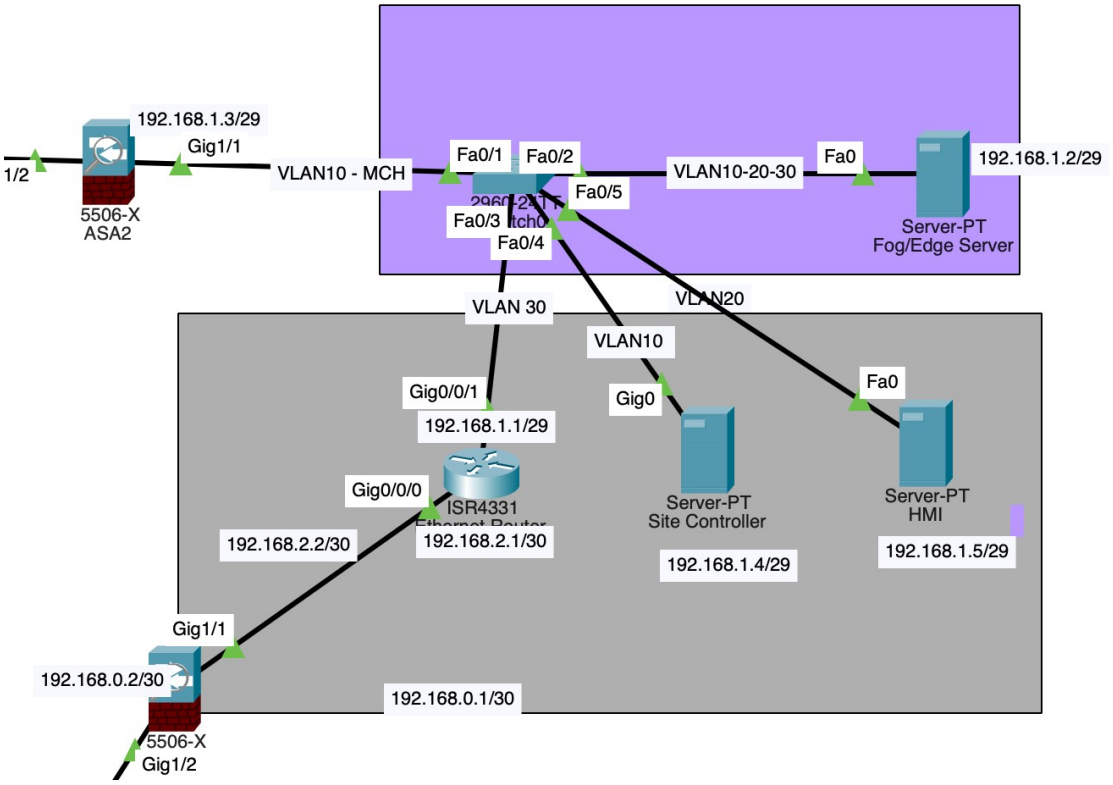


Figure 8.2 – Site Control and Fog/Edge rooms

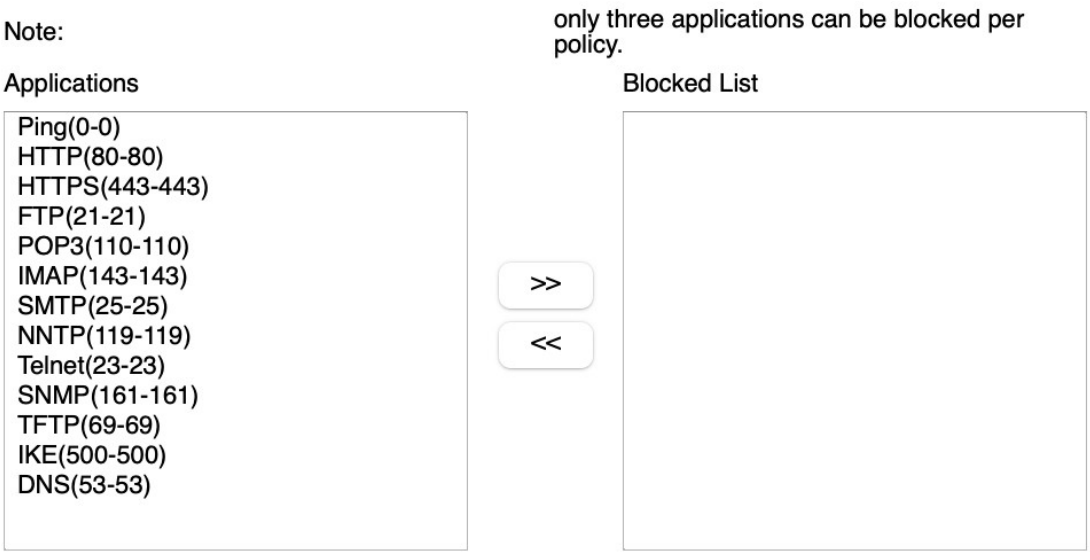


Figure 8.3 – Ports

Figure 8.2 and Figure 8.3 llustrates this firewall segment and the neighboring components, highlighting how minimal port openings and robust security rules together form a strong boundary against unwanted traffic from the external network (In the simulation, the ports could not be blocked. I did not succeed to resolve the problem)

Beyond the inside router, which transitions the IP scheme to 192.168.1.x, stands a Catalyst 2960 switch that organizes multiple VLANs, each assigned to a specific function. VLAN 10 links to one firewall interface (192.168.1.3/29), VLAN 20 hosts the HMI (192.168.1.5/29), VLAN 30 hosts the Site Controller (192.168.1.4/29). The Fog/Edge server at 192.168.1.2/29 can either trunk multiple VLANs or be statically assigned to just one, depending on the desired traffic management approach.

To secure the site's internal machine network, the simulation introduces a second firewall handling addresses at 192.168.3.x. This second firewall specifically defends the on-site machine environment and is assigned 192.168.3.1 for the interface facing the WRT300N tower and 192.168.3.2 for the interface connecting back to the Catalyst switch. By dedicating a separate firewall to 192.168.3.x, you effectively add another security boundary that checks traffic traveling between the core site network and the MCH "wireless" segment. In practice, it only allows necessary protocols, such as encrypted sensor data or IPsec from machines, while dropping unauthorized traffic or suspicious flows.

The WRT300N device, labeled as a 5G tower, obtains 192.168.3.1/30 on its link to the second firewall's 192.168.3.2. The WRT300N then NATs and distributes addresses from a DHCP pool in the 192.168.10.0/27 range to the actual machines. Those machines connect over a pseudo-wireless link, representing how real MCHs would link to a 5G tower. Since a malicious actor could attempt to masquerade as a legitimate MCH, this second firewall on 192.168.3.x, along with NAC or VLAN checks, ensures that only validly authenticated endpoints pass traffic to the Fog server.

At the site's heart, the Fog/Edge server runs an HTTPS-based iAssist service at 192.168.1.2/29. Operators access it via DNS name https://www.iassist.com, with a self-signed SSL certificate ensuring confidentiality. Credentials (Haris Adrovic / Harovic99()), plus a pseudo 6-digit MFA code, guard the final step of data retrieval or machine metrics.

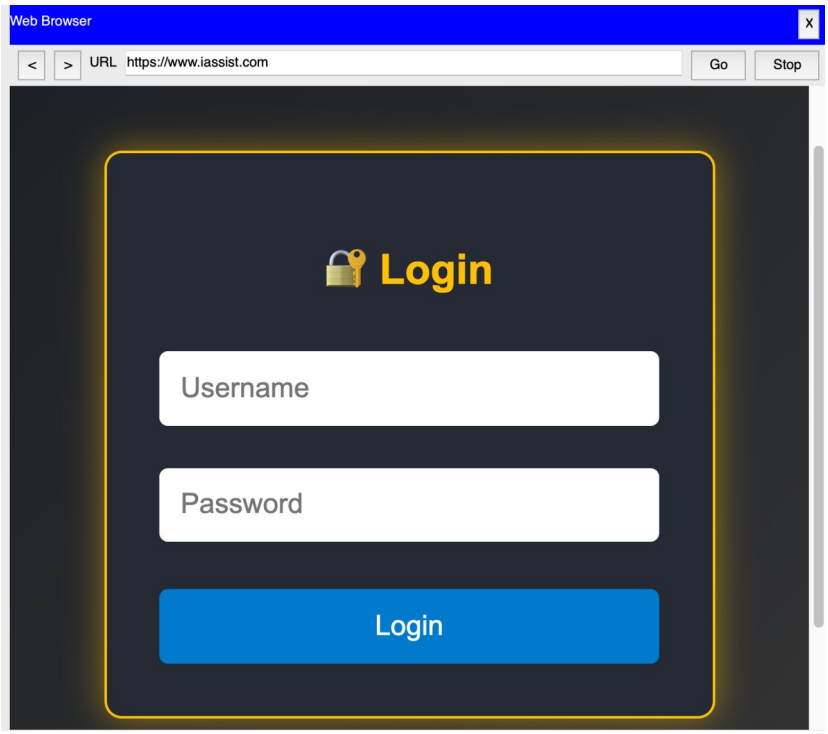


Figure 8.4 – Login Page

The screenshot displays the Fog server's web interface or JavaScript login, highlighting how only TLS-based connections are accepted. By restricting traffic to port 443 on both firewalls, unencrypted flows (HTTP) are disallowed, guaranteeing that iAssist data remains both private and tamper-resistant.

One further enhancement is the demonstration of 802.1X NAC on the Catalyst switch. Under NAC, any device plugging into a site VLAN—be it the HMI or a newly introduced sensor—must pass RADIUS or local credential checks before it's granted full VLAN membership. This approach negates stealth insertion of rogue endpoints.

Overall, the two-firewall design underscores that not only do you have a perimeter firewall (the first one at 192.168.0.x defending from the outside), but also a dedicated firewall for the on-site MCH network at 192.168.3.x. Such a structure exemplifies a belt-and-suspenders approach to industrial IoT or ICS security, ensuring that the internal "machine" side is likewise restricted from potential inside threats or unknown traffic bridging from the main site LAN. Combined with NAC, VLAN segmentation, an NGFW approach (application inspection, ACLs), and encrypted iAssist communications, the environment robustly defends sub-100 ms real-time flows from unauthorized interception, manipulation, or infiltration attempts.

9.Conclusion

This scenario demands rigorous defenses across multiple layers. Combining advanced 5G security (beamforming, MIMO) with VLAN-based segmentation, NAC (802.1X), carefully tuned firewall rules, and an IDS/IPS architecture provides a robust shield against sensor tampering, 5G denial-of-service attacks, Fog server compromises, and HMI intrusions. By isolating devices through VLANs, the threat of lateral movement is minimized, while NAC stops rogue endpoints at Layer 2. Meanwhile, an IDS/IPS can swiftly detect malicious traffic targeting iAssist's real-time data flows.

It is important to note that each additional security measure—be it encryption, NAC checks, or deep packet inspection—incurs performance and latency overhead. In a real-time industrial setting like iAssist, system designers must balance the strict sub-100ms requirement against the benefits of strong security. Some measures might require careful tuning or partial disablement to maintain operational performance while accepting certain residual risks. Overall, the recommended approach ensures that confidentiality, integrity, and availability remain aligned with iAssist's mission of safe, efficient machine operation.

10.References

[1] Volvo CE, “Use Case Description for Network Cyber Security course at MDU,” v1, 2024-02-20.

[2] Microsoft, “STRIDE Threat Modeling Methodology,” 2022.

[3] NIST SP 800-53, “Security and Privacy Controls for Information Systems and Organizations,” Rev. 5, 2020.

[4] IEEE 802.1X-2020, “Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control,” 2020.

[5] Cisco, “Cisco IOS Configuration Fundamentals Command Reference,” 2007.