Department of Electronic & Telecommunication Engineering
University of Moratuwa

EN4720: Security in Cyber-Physical Systems
Course Project

Milestone 1: Comprehensive Threat Assessment and Mitigation Strategies

Group Name: Decryptors

Pasqual A.C.	200445V
Gunatilake P.T.B.	200439G
Madhushan R.M.S.	200363R
Madusan A.K.C.S.	200366E

March 2, 2025

Contents

1 Description of the Smart Building System

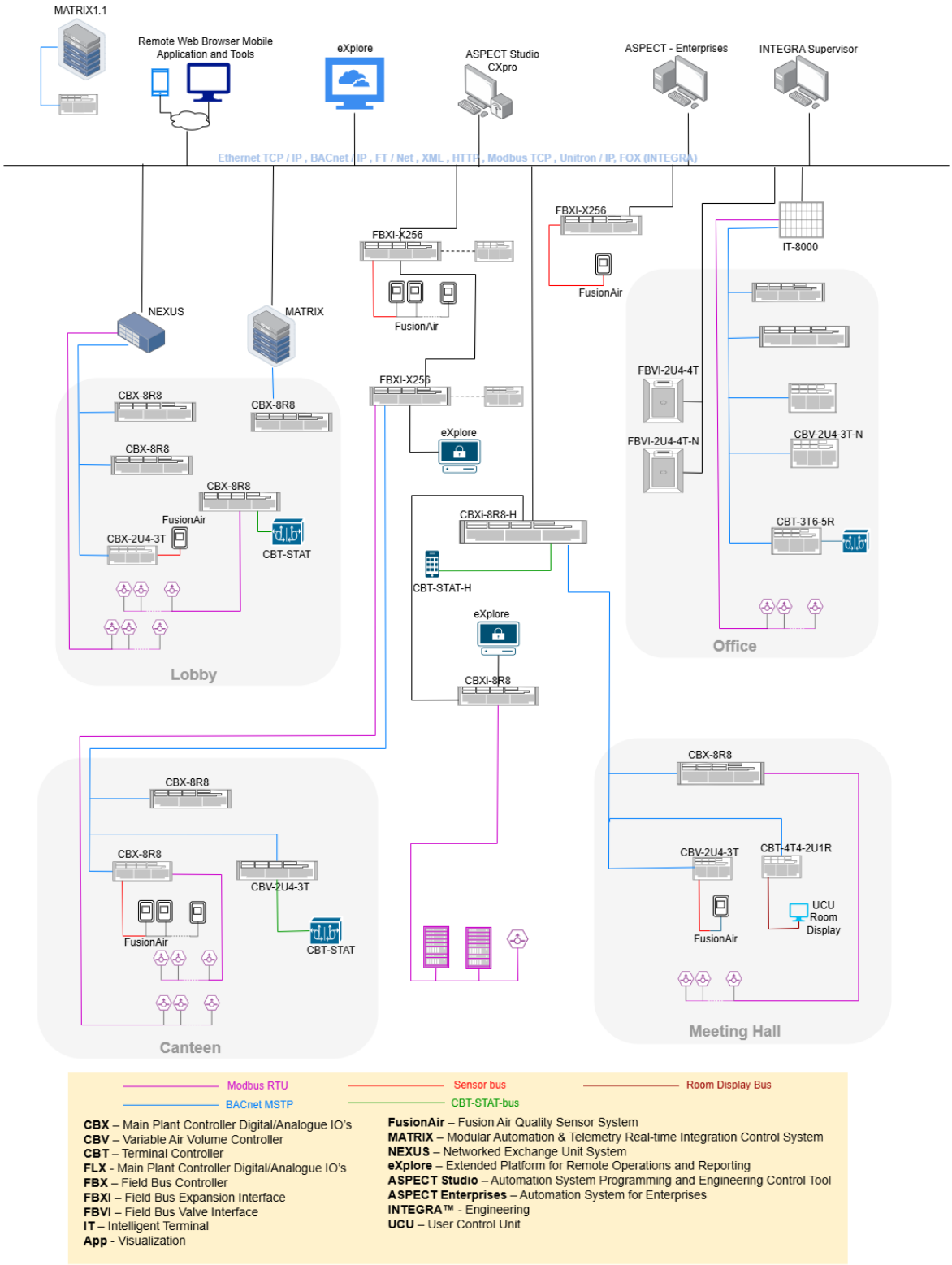

Figure 1: Architecture of the smart building system [1]

ABB Cylon Building Automation and Controls is a smart building system that offers automatic control of various systems such as HVAC and lighting, to optimize energy usage and internal environmental conditions based on sensor inputs. It allows the user to:

- Reduce energy costs
- Monitor and control in real time
- Centrally supervise the whole system

Figure 1 shows an ABB Cylon smart building system [1] that utilizes a range of products developed by ABB [2] to automatically control environmental conditions and lighting. The CBX, CBXi, and FBX series devices are field-level controllers that take sensor inputs and send control outputs to devices such as coolers, heaters, fan coil units, and lights accordingly. They can also connect to lower-level controllers such as the CBV and FBV Variable Air Volume Controllers, and CBT Terminal Controllers for smaller HVAC devices. In addition to ordinary sensors, CBT devices are connected to smart sensors such as CBT-STAT and FusionAir and to room displays through custom buses.

The system uses open communication protocols to integrate between different devices [2]. Modbus is an application layer protocol commonly used in industrial settings to communicate between sensors and controllers. In this system, Modbus is used to connect temperature and humidity sensors and energy meters to the field-level controllers. BACNet is another protocol used in building automation systems. In this system, it is used to connect lower-level controllers such as CBV and CBT to the field-level controllers.

ASPECT Supervisory Building Control [3] is the building management software system used by ABB Cylon. This includes NEXUS and MATRIX embedded control engines that are the main system controllers capable of handling a large amount of connections. The ASPECT-Enterprise server software is used to visualize and manage the system. They connect to the system through a protocol stack including Ethernet, TCP/IP, BACNet, HTTP, and Modbus. The server software can be connected to the internet to access through remote web browsers and mobile applications. ABB has advised that any remote connection should be done through a VPN and a firewall, which will provide secure and encrypted communication channels and only allow authorized personnel to access the system.

2 Identified Vulnerabilities

In this smart building system, several vulnerabilities were found in the ASPECT building management software, including products such as ASPECT-Enterprise, NEXUS Series, and MATRIX Series. These vulnerabilities could be exploited if an attacker is able to reach the system remotely or physically.

2.1 Unauthorized File Access

ABB Cylon's ASPECT system, including ASPECT-Enterprise, NEXUS Series, and MATRIX Series (version 3.08.01 and earlier), contains a vulnerability that allows unauthorized file access due to improper access control configurations [4]. This security flaw allows attackers to collect sensitive files from the web server without authentication, which is a significant risk to data confidentiality and system integrity. This vulnerability enables unauthenticated file disclosure, allowing attackers to extract plain-text credentials and facilitating further exploits within affected systems [5]. Such cases could lead to unauthorized system modifications and data breaches. Since the ASPECT platform is used for building automation, unauthorized access to critical files could interfere with building management operations, compromise security settings, and affect overall functionality. This vulnerability has been classified as critical, with a temporal score of 9.7 out of 10 in CVSS v3.1 and a score of 10 in CVSS v4.0 scoring systems.

2.2 Improper Input Validation

A critical command injection vulnerability has been identified in the network diagnostic component of the ASPECT interface, allowing unauthorized remote code execution [6]. This flaw arises from improper input validation and affects multiple ABB products, including ASPECT-Enterprise, NEXUS Series, and MATRIX Series running on Linux. Even though authentication is officially required to exploit the issue, testing [5] indicates that security measures are enforced inconsistently, potentially exposing systems to unauthorized access as the ASPECT devices aren't expected to be directly internet-facing. Since the attackers can remotely access the smart building system and can run malicious scripts using command injection, it poses a significant threat to the confidentiality of the system functionality.

2.3 Insufficiently Protected Credentials

A critical username enumeration vulnerability has been identified in multiple ABB products, including ASPECT-Enterprise, NEXUS Series, and MATRIX Series, running versions up to and including 3.08.02 on Linux systems [7]. This flaw arises from insufficiently protected credentials, allowing attackers to exploit application-level functionalities such as adding, deleting, modifying, or listing usernames without proper authentication[4]. This vulnerability is highly exploitable over network vectors as an attacker can be in a remote location analyzing the system responses, requiring no user interaction or prior privileges and posing a significant risk to confidentiality out of the CIA triad. It is considered as critical vulnerability as attackers can gain unauthorized access for the automation system by enumerating valid usernames and enable further attacks, such as credential stuffing or phishing.

2.4 Improper Authentication from Default Credentials

In the ASPECT system products (ASPECT-Enterprise, NEXUS Series, and MATRIX Series), the software installation package contains a default credential for the PHPmyAdmin tool, and it does not enforce changing the password during installation [8]. This tool is used to access the backend databases of the system. If a system configured with the default password was exposed to the internet without a VPN or a firewall, an attacker might be able to login and gain remote read/write access to the internal SQL database. Using this access, the attacker could modify system configurations to cause disturbances or damage equipment. They could also make changes to the data collected by the product, which can cause issues if this data is used as input to a later process.

2.5 Privilege Escalation

In the ASPECT system products, if the software was misconfigured to allow direct external access through the internet, its administrative interface can be accessed using the default credentials given in the ASPECT Control Engine user manual. After obtaining initial access, another vulnerability will allow an attacker to gain access to the underlying operating system and internal network infrastructure through a reverse shell [9]. Although this access is gained as a user with a low privilege level, there is an unintended privilege escalation vulnerability in the OS that allows the attacker to increase their access level to root [6]. With root-level access, the attacker can run arbitrary code on the device, which could be malicious software. They could also attempt to infect the other devices on the network with malicious software. Furthermore, they could modify the firmware of the device and cause major disruptions in the smart building system.

3 Mapping of Vulnerabilities to CVE

The above described vulnerabilities are represented by CVEs as in Table 1. It also shows reports where these vulnerabilities have been identified by third parties.

Table 1: Vulnerabilities in a smart building system.

Vulnerability	**Brief Description**	**Breach of security goal**	**Any known real-life case with URL**
CVE-2024-6209	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise; NEXUS Series; MATRIX Series v3.08.01 allows attacker to access files unauthorized	Confidentiality, Integrity	ABB Smart Building Software Flaws Invite In Hackers
CVE-2023-0636	A command injection vulnerability in ABB ASPECT-Enterprise, NEXUS, and MATRIX series upto version 3.07.0. allows remote attackers to execute unauthorized commands due to improper input validation.	Confidentiality, Integrity, Availability	ABB Smart Building Software Flaws Invite In Hackers
CVE-2024-51545	Username Enumeration vulnerabilities allow access to application-level username add, delete, modify, and list functions in ABB ASPECT; NEXUS Series; MATRIX Series upto version 3.08.02 products.	Confidentiality, Integrity	ABB Cylon Aspect 3.08.01 (jsonProxy.php) Username Enumeration - Zero Science Lab
CVE-2024-4007	Default credential in install package in ABB ASPECT; NEXUS Series; MATRIX Series version 3.07 allows attacker to login to product instances wrongly configured.	Confidentiality, Integrity, Availability	ABB Cylon Aspect 3.07.01 (config.inc.php) Hard-coded Credentials in phpMyAdmin - Zero Science Lab
CVE-2023-0635	Improper Privilege Management vulnerability in ABB ASPECT-Enterprise Linux OS allows Privilege Escalation to root.	Confidentiality, Integrity, Availability	Privilege Escalation and RCE Vulnerabilities for Multiple ABB Appliances [ASPECT, Matrix, Nexus] - Prism Infosec

4 Proposed Mitigation Strategies

This section proposes methods to mitigate the system being impacted by the above listed vulnerabilities.

4.1 Unauthorized File Access

To reduce the risk of unauthorized file access in ABB Cylon's ASPECT system, the following actions can be followed [4]. ASPECT devices should not be exposed directly to the internet, whether through direct ISP connections or NAT port forwarding. If remote access is a user requirement, the system must operate behind a firewall, and access should be restricted to secure VPN gateways configured according to industry standards. Upgrading all ASPECT products to the latest firmware version is critical to resolving known vulnerabilities. Additionally, default passwords must be changed into strong passwords, and physical controls should be included to prevent unauthorized access to devices and networks. The system developers should set up access control configurations such that system files cannot be accessed without authentication.

4.2 Improper Input Validation

As ASPECT devices are not intended to be directly internet-facing, the devices should operate behind a firewall with network access only to authorized persons. In addition, the firewall should block all access to all the ports except port 443 (default SSL port) [6]. Also, the user should purchase an SSL certificate from a valid certification authority and install it in the ASPECT devices. Furthermore, the system should be configured to close ports 3306, 8245, and 30144, preventing access to the device UI and the underlying database. Lasty, the system developers should disable remote code execution functionality and access to the operation system to prevent remote command injection.

4.3 Insufficiently Protected Credentials

To mitigate the threats caused by insufficiently protected credentials such as the recognized username enumeration vulnerability, the system developers should implement generic error messages that do not specify the validity of the usernames entered [7]. Additionally, the system should integrate stronger authentication, and use logging mechanisms to monitor access and modification activity of the user lists [10]. Also, separating the critical entry points and username-related functions in the system reduces the threat caused by username enumeration attacks.

4.4 Improper Authentication from Default Credentials

To mitigate the vulnerabilities caused by default credentials, the user should change all default credentials to new unique credentials with sufficient strength. If remote access to the system is required, it should also use a firewall and VPN that only allows access to authorized users [8].

4.5 Privilege Escalation

To avoid the privilege escalation vulnerability, firstly the default credentials of administrative interfaces should be changed to unique strong credentials to avoid attackers gaining initial access. Furthermore, the software can be configured such that the default main page accessible in the web server is not a system administration page [6]. This reduces the possibility of an attacker discovering the system as a target. Privilege escalation to root in the OS can be avoided by measures such as giving regular users the minimum possible permissions, restricting root access through remote connections, and frequently updating the OS and related software. As the user, the building management software should be updated regularly to ensure that no security risks remain.

5 Recommendations for Best Practices to Enhance Overall Security

The below practices can be followed to improve the overall system security against attackers, in addition to addressing specific vulnerabilities.

- ASPECT devices should not be exposed directly to the internet. If remote access is required, the system should be secured with a firewall and a VPN that restricts access to authorized users only.
- All ASPECT products should be updated regularly to the latest firmware version, to ensure that earlier vulnerabilities have been closed.
- Default credentials should always be changed to unique, strong credentials.
- Install physical controls to prevent unauthorized personnel from accessing devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programming software to any network other than the one intended for the devices.
- Scan all data imported into the user environment before use to detect potential malware infections.
- Minimize network exposure for all ASPECT ports and endpoints to ensure that they are not accessible directly from the Internet.

References

[1] ABB, "Cylon® NEXUS series technical datasheet," https://library.e.abb.com/public/5d414818e0c64ad9bd8bd51206eec2a1/DS0114%20NEXUS%20Series.pdf?x-sign=FNOEmHjFxzfg26vbD48G46T04nLzc2sijf3aKOFXbbA74rHDvU4/6h%20nUsCUy4io, 2021.

[2] ——, "Webinar "ABB Cylon® Smart Building Solutions"," https://library.e.abb.com/public/449d48e082964c12a2b206a103576891/Webinar-ABB-Cylon-February-2021_PR_EN_V1-0_9AKK107991A8225.pdf, 2021.

[3] ——, "ASPECT® Supervisory Building Control," https://new.abb.com/low-voltage/products/building-automation/product-range/abb-cylon/system-information/portfolio/aspect-supervisory-building-control.

[4] ——, "Cylon® NEXUS ASPECT System, multiple vulnerabilities reported," https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch, 2025.

[5] VulnCheck, "Exploring ABB Vulnerabilities and Their Impact on Industrial Control Systems CVE ID: CVE-2023-0635, CVE-2023-0636 ," https://vulncheck.com/blog/exploring-abb-ics-vulns, 2024.

[6] ABB, "Cylon® NEXUS ASPECT® Control Engines (ACE) CVE ID: CVE-2023-0635, CVE-2023-0636 ," https://search.abb.com/library/Download.aspx?DocumentID=2CKA000073B5403&LanguageCode=en&DocumentPartId=&Action=Launch, 2023.

[7] socca.tech, "CVE-2024-51545: (ABB ASPECT – Enterprise v3.08.02: Critical) ," https://socca.tech/cve-2024-51545/, 2024.

[8] ABB, "Cylon® NEXUS aspect system operating with default credentials while exposed to the internet," https://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A6101&LanguageCode=en&DocumentPartId=&Action=Launch, 2024.

[9] Prism Infosec, "Privilege Escalation and RCE Vulnerabilities for Multiple ABB Appliances [ASPECT, Matrix, Nexus]. (CVE-2023-0635 / CVE-2023-0636)," https://prisminfosec.com/privilege-escalation-and-rce-vulnerabilities-for-multiple-abb-appliances-aspect-matrix-nexus-cve-2023-0635-cve-2023-0636/, 2023.

[10] Ogma, "Understanding and Mitigating CVE-2024-51545: Username Enumeration Vulnerability in ABB Products," https://ogma.in/understanding-and-mitigating-cve-2024-51545-username-enumeration-vulnerability-in-abb-products, 2024.