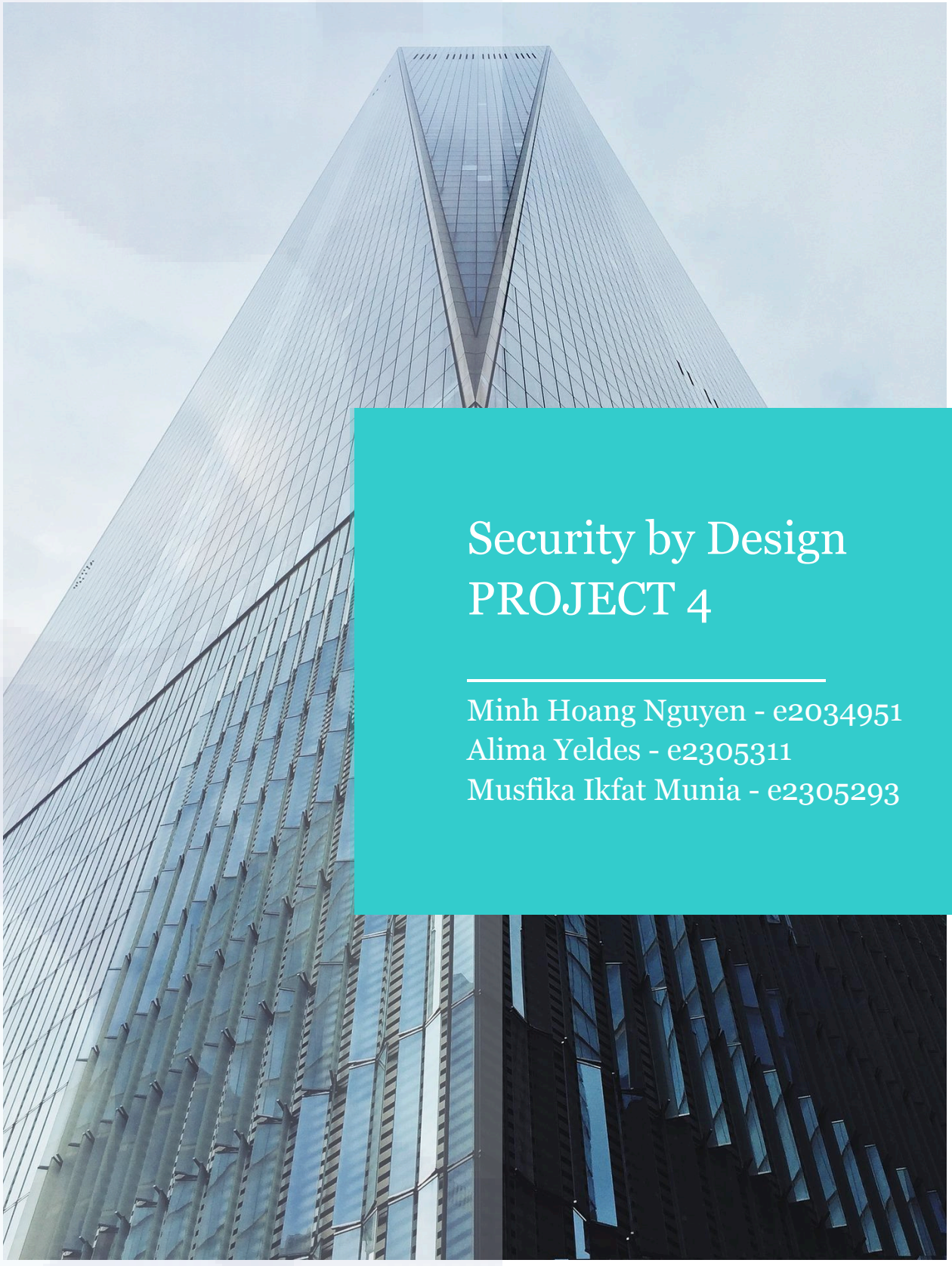


Security by Design
PROJECT 4

Minh Hoang Nguyen - e2034951
Alima Yeldes - e2305311
Musfika Ikfat Munia - e2305293

Project 4:
Industrial automation, plant

The company you are working at has a **paper production plant** and has decided to add a possibility to configure production line settings by an engineering team located in a different geographical location.

Task: you are given a function/application description that is to be developed by a company where you are working. Depending on the size of the company and the maturity of its products, the company can be either a well-established player in the domain, or a start-up trying to put out a competitive product. The company size might provide assumptions about available resources and scale of processes in place. The criticality level of the function (whether it is safety-critical) that the company is about to develop gives assumptions about how rigorous design activities should be. You also get an application domain in which the company is operating, which might provide you with the context for applicable standards. You as a team of security architects, need to do the following:

1) make assumptions regarding stakeholders needs (the assumptions need to be stated in the report),
2) propose a development process (mention all the phases and list the main activities to be conducted in those phases),
3) create a model of the application (like in the DDD lecture),
4) propose an adequate threat modeling technique and a security framework if applicable,
5) state if there are privacy concerns present,
6) find at least one vulnerability and explain how it can be handled (you do not need to perform the complete threat analysis),
7) based on how the identified vulnerability is handled, derive a set of one or more corresponding security requirements.

Expected outcome: a report with all your findings and explanations (rationale) for all the decisions you have made.

Table of Content:

A. Introduction:

This report addresses the development of a remote configuration solution for an industrial paper production plant, catering to the need for efficient production line settings managed by an engineering team situated in a different geographical location.

Operating in the domain of paper production, we acknowledge the importance of contextual standards to guide our development. This project aims to provide a seamless and secure remote access solution, optimizing efficiency and global collaboration. As security architects, we will explore stakeholder needs, propose a development process encompassing key phases, create a domain-driven design model, employ a suitable threat modeling technique and security framework, assess privacy concerns, identify and briefly address a vulnerability, and outline corresponding security requirements based on mitigation strategies. Through these considerations, our goal is to ensure a robust and compliant solution for remote configuration in the industrial automation space.

B. Assumptions and Stakeholders' needs:

1. Assumptions:

a. Assumptions regarding company's background:

- The company is a start-up in the paper production industry;
- The headquarters of the company is located in France and the to-be-developed functions and applications need to follow the regulations and standards as defined by the government if applicable;
- The remote engineering team will be located in a different geographical location inside France;
- The company is in the industrial automation on a budget (paper production plant);
- The company has limited access to resources, and manually configures and handles the automation systems and machineries at the moment;
- The scope of the security architect project is to ensure the security while developing the application to configure production line settings remotely by the engineering team;
- The company has a lean manufacturing process;
- The company deploys machineries and Programmable Logic Controllers (PLC), which are controlling and configuring machineries at the paper production plant.

b. Assumptions regarding Safety Management:

- The company places a high emphasis on safety management, given the nature of the paper production industry, and will ensure that any remote access and configuration solution adheres to strict safety protocols. The Safety Management System system tracks compliance status and also actively monitors safety parameters in real-time through sensors integrated into machinery;
- Regular safety audits and incident reporting are part of the company's safety management system to maintain a secure working environment.

c. Assumption regarding User Experience:

- Training programs are in place to familiarise the remote engineering team with the remote access solution, ensuring efficient and effective use.

d. Assumptions regarding Technology Integration and Compatibility:

- The existing industrial networks (LANs) and potentially a wide area network (WAN) as well as existing Programmable Logic Controllers (PLCs) controlling the machinery are compatible with the new remote access solution;
- The remote access solution is designed to seamlessly integrate with these networks and controllers, ensuring minimal disruptions during implementation.

e. Assumption regarding Cost-Effectiveness:

- Given the budget constraints of the start-up, cost-effectiveness is a crucial factor in the development and implementation of the remote access solution.

f. Assumptions regarding Innovativeness and Competitiveness:

- The company is committed to innovation to stay competitive in the paper production industry;
- Continuous improvement in automation processes and technology is part of the company's strategy to maintain competitiveness.

g. Assumptions regarding Data Privacy & Security:

- Data privacy, compliance with data protection regulations like GDPR are a priority, especially considering the sensitive nature of production line settings;
- The security architecture of a company reflects the company's commitment to safeguarding data from unauthorised access.

h. Assumption regarding Upgradability:

- The current company's system is designed with upgradability in mind to accommodate future technological advancements and changes.

i. Assumption regarding Environmental Impact:

- The company is environmentally conscious and is exploring ways to minimise the environmental impact of its production processes;
- The Environmental Monitoring System is designed to actively monitor environmental conditions related to paper production. This includes tracking energy consumption through the Energy Management System, waste processing through the Waste Management System, and overall environmental impact through the generation of environmental reports.

2. Stakeholders' needs:

- An efficient application that seamlessly integrates with current operations of automation systems and machineries, minimising disruptions which can potentially hinder day-to-day operations of the plant production;
- Need to be secured and reliable in remote access to configure production line settings;
- Require access to real-time data to make informed decisions by utilising a robust remote interface through application with high uptime, real-time data access, and robust troubleshooting capabilities;
- Need assurances that the system is secure, does not introduce additional risks to the production process, and complies with industry regulations;
- Need a system that is maintainable, scalable, and integrates well with existing OT infrastructure;
- The to-be-developed functions and applications need to follow the applicable standards and security framework:
    - GDPR;
    - NIST CSF;

3. Requirements:

- In the context of remote production line configuration for paper plant the remote access solution shall provide the remote engineering team with the ability to remotely modify specific production line settings, encompassing speed, temperature, and pressure parameters.
- In the context of remote production line configuration for paper plant the remote access solution shall provide the remote engineering team with the ability to access their information and essential services from any location if required and allowed by company's policy.
- In the context of remote production line configuration for paper plant the remote access solution shall provide the remote engineering team with the ability to retrieve critical production information at any time, ensuring accuracy, completeness, and confidentiality according to predefined access permissions.
- In the context of the organization environment of the company the remote access solution for the paper plant shall provide regulatory authorities with the ability to audit the remote access system to ensure compliance with industry regulations and security standards, including GDPR and NIST CSF.
- In the context of security considerations the remote access solution shall provide remote engineering team with the ability to control the access based on roles and responsibilities, ensuring that individuals only have access to the systems and data necessary for their specific tasks

- In the context of security considerations, the remote access solution shall provide the remote engineering team with the ability to continuously monitor remote access activities and maintain detailed logs for audit and forensic purposes.

C. Development Process:

I. Why DevSecOps?

The continuous integration and continuous deployment characteristics of DevOps practice will enable rapid and reliable software updates, which is crucial for maintaining and enhancing the application to remotely manage the production line settings. With the strong capabilities in collaboration and communication through DevOps strategy, it can ensure that the engineering team can work effectively despite being in different geographical locations as defined in the project's requirement and assumption. Moreover, DevOps can incorporate automated testing to ensure that changes to the production line settings do not introduce errors and ensure safety risks which is paramount in the context of industrial automation of paper production plants that needs to minimize the risks as minimal as possible and ensure the safety of the working environment. The continuous monitoring in DevOps strategy will quickly identify and resolve issues in the remote paper production management application, ensuring minimal downtime and disruption to the production process through collaborating smoothly between engineering teams around different geographical locations. With the DevOps approach, we can efficiently manage the large resources and can be scaled as per the needs of the paper production plant if needed in the future. Last but not least, DevOps can support the alignment with applicable standards in the paper production industry, ensuring compliance and maintaining quality throughout the development and deployment processes.

By considering DevOps as the strategy for the development phase to resolve current challenges, it is crucial to integrate security into DevOps practice to address security concerns in the development and operation of the remote production management application for the paper production plant, as well as ensure the security by design practice for the development process.

DevSecOps integrates security practices into every phase of the software development lifecycle. This ensures that security considerations are not an afterthought but are incorporated from the planning stage through development, testing, deployment, and operation, ensuring that security is a continuous and integral part of the process. Automation in DevSecOps strategy enables continuous security testing throughout the development process which helps in early identification and resolution of vulnerabilities, reducing the risk of security breaches. Moreover, DevSecOps will foster collaboration between development, operations, and security teams which can provide a collaborative approach to ensure that security is a shared responsibility and is effectively integrated into all processes. Continuous monitoring in DevSecOps will help in detecting and responding to threats in real-time. Additionally, it ensures compliance with industry standards and regulations, which is crucial for a company operating in a regulated sector like paper production. Last but not least, with the DevSecOps capability of rapid response to security incidents, the security can immediately respond to any identified security incidents, minimizing potential damage and ensuring immediate remediation and recovery which is significant in the safety context of industrial automation of paper production.

II. Phases of Development Process:

1. Continuous Development:

- **Concept and Feasibility Phase:** Assess the feasibility of the project, considering technological capabilities, budget constraints, and compliance requirements.

- **Design Phase:** Design the architecture of the remote access solution, ensuring it integrates seamlessly with existing systems like PLCs and complies with GDPR and NIST CSF.
- **Code Development:** Development of the application with the capability of integrating with the machineries and systems in the factory. For Hardware, ensure that the software being developed is compatible with existing PLCs and machinery and emphasize on API development for smooth hardware-software interaction. For Software Development, develop modular, scalable, integrable software to manage production line settings
- **Version Control:** Use version control systems to manage changes and maintain the integrity of the codebase.
- **Security by Design:** Implement 'Security by Design' principles from the outset, ensuring that security considerations are embedded in the development process.
- **Static Analysis and Code Review:** Implement automated static analysis through Automated Code Scanning tools that run every time code is committed to the version control system. This ensures that code is automatically analyzed for security vulnerabilities, code quality issues, and compliance with coding standards, to early identify and rectify security vulnerabilities, such as SQL injections or Insecure Deserialization leading to Remote Code Execution, before the code moves further down the development pipeline.

2. Continuous Testing:

a. **Building**
   - **Automated Build:** Set up automated builds to compile and assemble code into executable software, ensuring every change is build-ready.
   - **Security Checks:** Include security checks in the build process to detect vulnerabilities early.

b. **Testing**
   - **Automated Testing:** Implement a comprehensive suite of automated tests (unit, integration, security) to validate functionality and security.
   - **Integration Testing:** Test the integration of different components and with existing systems.
   - Performance Testing: Testing the application under simulated load conditions.
   - **Performance Testing:** Test the software under simulated load conditions to ensure it can handle real-world use.
   - **Security Testing:** Conduct regular security testing, including penetration testing and automated source-code review to scan security vulnerabilities.

3. Continuous Integration:

- **Integration Strategy:** Use a Continuous Integration (CI) server such as Gitlab CI, Jenkins and CircleCI to automatically integrate code changes, ensuring that new code works with the existing codebase.
- **Merge Changes:** Integrate changes from different development branches regularly.
- **Collaboration:** Facilitate real-time collaboration between team members, ensuring smooth integration of different modules.

4. Continuous Deployment:

- **Automated Deployment:** Automate the deployment process to quickly and reliably push code to production.
- **Configuration Management:** Manage and automate the configuration of production environments.

- **Automated Deployment:** Automate the deployment process to production environments.
- **Staging Environments:** Use staging environments to simulate the production environment.
- **Rollback Mechanisms:** Implement fail-safes for quick rollback in case of failure, minimizing disruption to the production line.
- **Compliance Checks:** Ensure all deployments comply with relevant industry standards and regulations.

5. Continuous Operations:

- **Access Control:** Continuously review and manage user access rights to ensure they align with current roles and responsibilities.
- **Logs and activities:** Implement periodic reviews of access logs and user activities for signs of abnormal or unauthorised access.
- **Automated Backup:** Maintain regular backups of critical data and system configurations.
- **Disaster Recovery:** Develop, update and test a disaster recovery plan to ensure rapid restoration of services in case of major incidents.

6. Continuous Monitoring:

- **Real-time Monitoring:** Set up real-time monitoring of both the application and underlying infrastructure to quickly identify and respond to issues.
- **Performance Monitoring:** Monitor the application performance in real-time.
- **Security Monitoring:** Continuously monitor for security threats or anomalies.
- **Log Management:** Collect and analyze logs for insights and potential issues.
- **Incident Response:** Implement an incident response plan for quick reaction to detected issues.

Additional phases which can be considered:

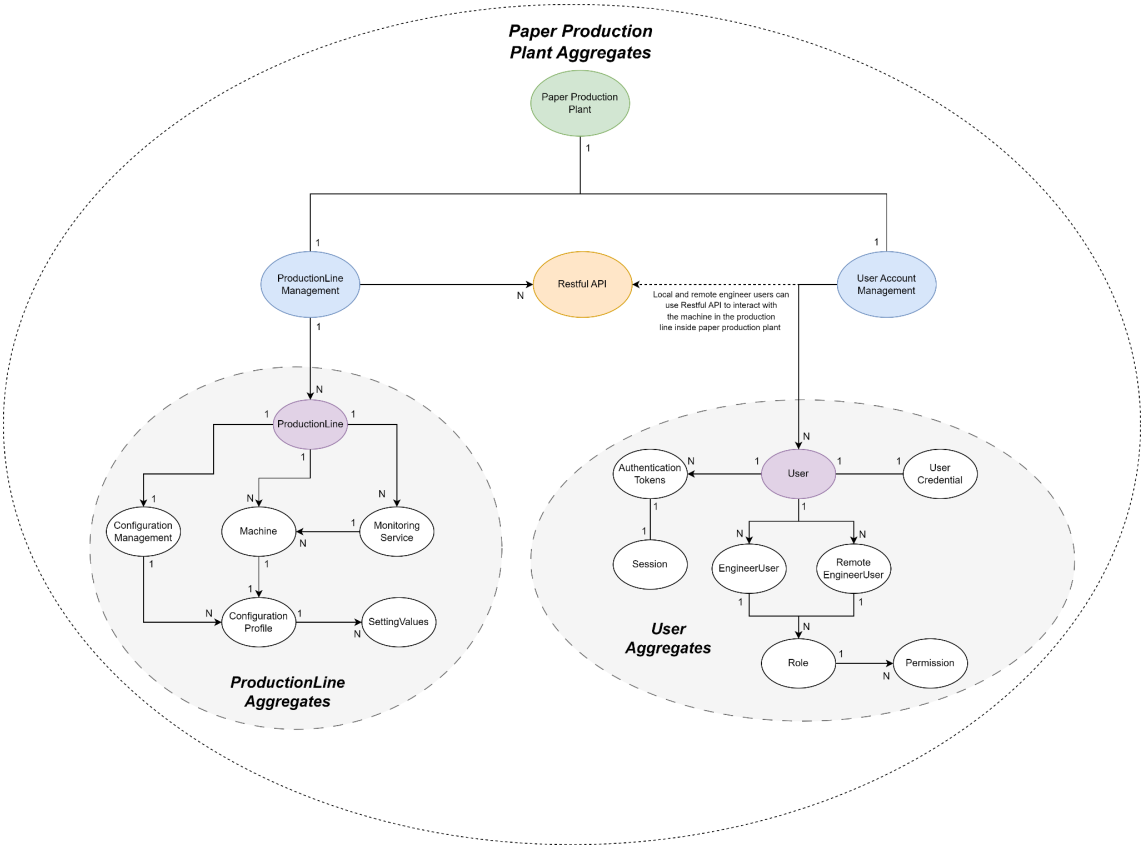
Maintenance and Validation:

- **Regular Updates:** Implement regular updates for system enhancements and security patches.
- **Feedback Loop:** Incorporate user feedback and operational data to continually improve the system.
- **Validation of Requirements and Compliances:** Ensure that all stakeholder requirements and applicable compliances in adherence to industry standards and regulations have been met.
- **Verification of Implementation:** Verify that the system is implemented as designed, both in terms of functionality and security.

By following this structured development process, incorporating DevOps and DevSecOps practices, the project can effectively manage the complexities of developing a secure and efficient application to remotely access and control the machinery and systems in the paper production plant. This approach ensures that security is not an afterthought but is integrated into every stage of the development process, aligning with the company's emphasis on safety, innovation, and regulatory compliance.

D. Models of the Application:

I. Domain-Driven Design (DDD):



a. Paper Production Plant Aggregates: Encompasses one ProductionLine Management and User Account Management entities which interacts with each other through Remote Access and Configuration Function by utilizing Restful API.

- **ProductionLine Management:** Multiple ProductionLine as well as its Aggregates (N) are controlled and managed by a ProductionLine Management (1).
- **User Account Management:** Multiple Users and its Aggregates (N) are controlled and managed by a User Account Management (1).
- **Restful API:** Multiple Restful APIs (N) are provided by a ProductionLine Management (1) which will provide the capability to integrate with the machines of each production line in the factory to remotely access and control those machines.

b. Production Line Aggregate: Encompasses one ProductionLine entity, multiple Machine entities within it, and associated ConfigurationProfiles, along with the Configuration Management for multiple Configuration Profiles and the Monitoring Service to monitor multiple Machines.

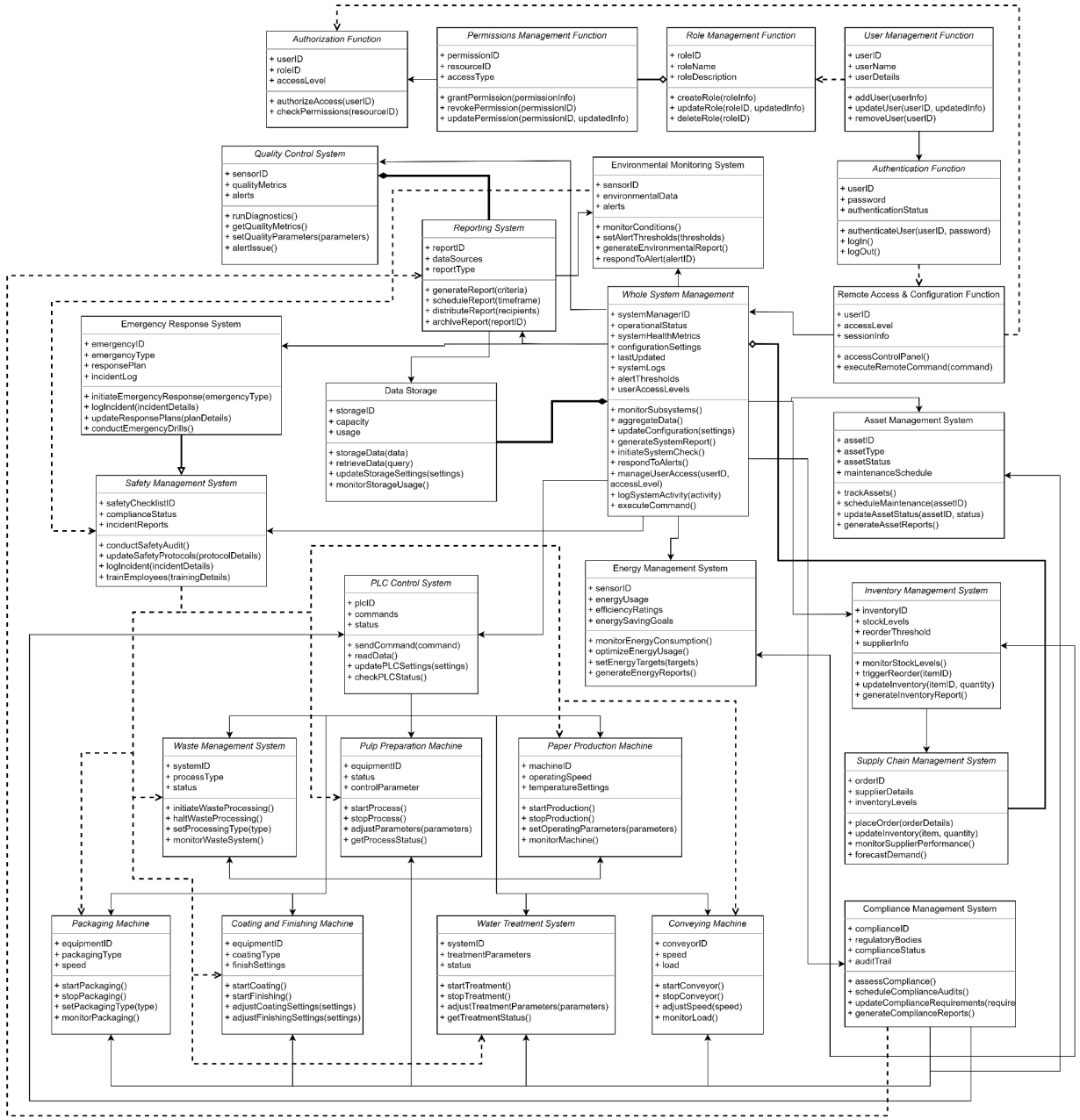
- **ProductionLine:** Each ProductionLine (1) can have multiple Machines (N)
- **Machine:** Each Machine (1) will be associated with a ConfigurationProfile (1)
- **Configuration Management:** Applies ConfigurationProfiles to multiple Configuration Profiles (1 to N) and control their settings.

- **ConfigurationProfile:** A single ConfigurationProfile (1) can encompass multiple **SettingValues** (N), each tailored for different machines or settings. Each configuration profile will be controlled and configured by a Configuration Management.
- **MonitoringService:** Monitors and provides real-time data for multiple Machines (1 to N) across different ProductionLines.

c. User Aggregate: Encompasses multiple EngineerUser (both local and remote) entities with their respective roles and permissions, as well as the user credential, authentication tokens and its associated sessions.

- **User:** Manages multiple EngineerUser and Remote EngineerUser (1 to N) authentication, authorization, and role assignments.
- **EngineerUser:** One EngineerUser (1) can have multiple roles (N)
- **Remote EngineerUser:** One Remote EngineerUser (1) can have multiple roles (N)
- **Roles:** One Role (1) can have multiple **Permissions** (N)
- **User Credential:** One User (1) can have only one User Credential (1)
- **Authentication Token:** One User (1) can have multiple Authentication Token (N) to flexibly their access
- **Session:** One Session (1) can only be associated with one Authentication Token (1)

II. Detailed UML Diagram:



This UML diagram will encompass every entity in the paper production plant and how users can interact with and control them remotely by using the application with the support of the remote access and configuration function.

1. User Management Function Class

Attributes:

- userID: Unique identifier for each user.
- userName: Name of the user.
- userDetails: Detailed information about the user.

Functions:

- addUser(userInfo): Add a new user to the system.
- updateUser(userID, updatedInfo): Update existing user information.
- removeUser(userID): Remove a user from the system.

2. Authentication Function Class

Attributes:

- userID: Unique identifier for each user.
- password: Password for user authentication.
- authenticationStatus: Status of the authentication process.

Functions:

- authenticateUser(userID, password): Verify user credentials.
- logIn(): Handle user login process.
- logOut(): Handle user logout process.

3. Role Management Function Class

Attributes:

- roleID: Unique identifier for each role.
- roleName: Name of the role.
- roleDescription: Description of the role.

Functions:

- createRole(roleInfo): Create a new role.
- updateRole(roleID, updatedInfo): Update an existing role.
- deleteRole(roleID): Delete a role.

4. Permissions Management Function Class

Attributes:

- permissionID: Unique identifier for each permission.
- resourceID: Identifier of the resource the permission applies to.
- accessType: Type of access (read, write, execute, etc.).

Functions:

- grantPermission(permissionInfo): Grant a specific permission to a role or user.
- revokePermission(permissionID): Revoke an existing permission.
- updatePermission(permissionID, updatedInfo): Update details of a permission.

5. Authorization Function Class

Attributes:

- userID: Unique identifier for each user.
- roleID: Role identifier linked to the user.
- accessLevel: Level of access granted.

Functions:

- authorizeAccess(userID): Determine access level based on user and role.
- checkPermissions(resourceID): Check if the user has permissions for a specific resource.

6. Remote Access and Configuration Function Class

Attributes:

- userID: Identifier for the user accessing remotely.
- accessLevel: Level of access granted to the user.
- sessionInfo: Information about the current remote session.

Functions:

- login(userCredentials): User login for remote access.
- logout(): Logout from the system.
- accessControlPanel(): Access the control panel for remote operations.
- executeRemoteCommand(command): Execute commands remotely.

7. Whole System Management Class

Attributes:

- systemManagerID: A unique identifier for the system management instance.

- operationalStatus: The current overall operational status of the plant.
- systemHealthMetrics: Aggregated health metrics or KPIs of all managed systems.
- configurationSettings: Settings and configurations applied across various systems.
- alertThresholds: Thresholds for various alerts across systems.
- systemUpdateLogs: Logs of system updates, changes, and configurations.
- userAccessLevels: Information about access levels for different management roles.

Functions:

- activateSystem(): Activate the systems
- deactivateSystem(): Deactivate the systems
- executeCommand(): Execute command and control the settings of each systems
- coordinateOperations(): Coordinate operations across different systems for efficiency and effectiveness.
- monitorSystemHealth(): Monitor the health and performance of all subsystems.
- updateConfigurations(configurations): Update and manage configurations across various systems.
- respondToAlerts(alertID): Respond to and manage alerts from various systems.
- aggregateReports(): Aggregate reports from different systems for an overview.
- manageSystemUpdates(): Manage and schedule updates across all systems.
- accessControlManagement(user, level): Manage access control for various system users based on roles and privileges.
- conductSystemAudits(): Conduct regular audits of all systems for compliance and performance.

8. PLC Control System Class

Attributes:

- plcID: Identifier for the PLC.
- commands: Current commands being sent to the PLC.
- status: Operational status of the PLC.

Functions:

- sendCommand(command): Send a command to PLC to control and manage machineries and systems
- readData(): Read data from the PLC.
- updatePLCSettings(settings): Update settings of the PLC.
- checkPLCStatus(): Check the status of PLC.

9. Pulp Preparation Machine Class

Attributes:

- equipmentID: Identifier for the equipment.
- status: Operational status of the equipment.
- controlParameters: Parameters controlling the process.

Functions:

- startProcess(): Start the pulp preparation process.
- stopProcess(): Stop the process.
- adjustParameters(parameters): Adjust the operating parameters.
- getProcessStatus(): Get the current status of the pulp preparation process.

10. Paper Production Machine Class

Attributes:

- machineID: Unique identifier for the paper machine.
- operatingSpeed: Current speed of operation.
- temperatureSettings: Settings for temperature control.

Functions:

- startProduction(): Start paper production.
- stopProduction(): Stop paper production.
- setOperatingParameters(parameters): Set parameters like speed, temperature.
- monitorMachine(): Monitor the status and performance of the machine.

11. Coating and Finishing Machine Class
Attributes:
- equipmentID: Identifier for coating and finishing equipment.
- coatingType: Type of coating being applied.
- finishSettings: Settings for the finishing process.

Functions:
- startCoating(): Begin coating process.
- startFinishing(): Begin finishing process.
- adjustCoatingSettings(settings): Adjust settings for coating.
- adjustFinishingSettings(settings): Adjust settings for finishing.

12. Conveying Machine Class
Attributes:
- conveyorID: Identifier for the conveyor system.
- speed: Conveyor speed.
- load: Current load on the conveyor.

Functions:
- startConveyor(): Activate the conveyor system.
- stopConveyor(): Deactivate the conveyor system.
- adjustSpeed(speed): Adjust the speed of the conveyor.
- monitorLoad(): Monitor the load on the conveyor system.

13. Packaging Machine Class
Attributes:
- equipmentID: Identifier for packaging equipment.
- packagingType: Type of packaging being used.
- speed: Speed of the packaging process.

Functions:
- startPackaging(): Start the packaging process.
- stopPackaging(): Stop the packaging process.
- setPackagingType(type): Set the type of packaging.
- monitorPackaging(): Monitor the ongoing packaging process.

14. Water Treatment Machine Class
Attributes:
- systemID: Identifier for the water treatment system.
- treatmentParameters: Parameters for water treatment.
- status: Operational status of the system.

Functions:
- startTreatment(): Start water treatment process.
- stopTreatment(): Stop water treatment process.
- adjustTreatmentParameters(parameters): Adjust water treatment parameters.
- getTreatmentStatus(): Get the status of water treatment systems.

15. Waste Management System Class
Attributes:
- systemID: Identifier for the waste management system.

- processType: Type of waste processing being used.
- status: Operational status of the system.

Functions:

- initiateWasteProcessing(): Start the waste management process.
- haltWasteProcessing(): Stop the waste management process.
- setProcessingType(type): Set the type of waste processing.
- monitorWasteSystem(): Monitor the waste management systems.

16. Data Storage Class

Attributes:

- storageID: Unique identifier for the data storage system.
- capacity: Total capacity of the storage system.
- usage: Current data usage.

Functions:

- storeData(data): Store data in the system.
- retrieveData(query): Retrieve data based on a query.
- updateStorageSettings(settings): Update storage settings.
- monitorStorageUsage(): Monitor the usage of the storage system.

17. Quality Control System Class

Attributes:

- sensorID: Identifier for quality control sensors.
- qualityMetrics: Metrics for paper quality.
- alerts: Alert status for quality issues.

Functions:

- runDiagnostics(): Perform quality control diagnostics.
- getQualityMetrics(): Retrieve current quality metrics.
- setQualityParameters(parameters): Set parameters for quality control.
- alertIssue(): Trigger an alert in case of quality issues.

18. Emergency Response Class

Attributes:

- emergencyID: Unique identifier for each emergency situation.
- emergencyType: Type of emergency (e.g., fire, mechanical failure).
- responsePlan: Planned response for different types of emergencies.
- incidentLog: Log of all incidents and responses.

Functions:

- initiateEmergencyResponse(emergencyType): Activate the emergency response plan for a specific type of emergency.
- logIncident(incidentDetails): Log details of the incident for review and analysis.
- updateResponsePlans(planDetails): Update and refine emergency response plans.
- conductEmergencyDrills(): Conduct regular emergency response drills for preparedness.

19. Reporting System Class

Attributes:

- reportID: Unique identifier for each report.
- dataSources: Data sources used for the report.
- reportType: Type of the report (e.g., performance, quality).

Functions:

- generateReport(criteria): Generate a report based on specified criteria.
- scheduleReport(timeframe): Schedule regular report generation.
- distributeReport(recipients): Distribute the report to specified recipients.

- archiveReport(reportID): Archive reports for future reference.

20. Safety Management System Class
Attributes:
- safetyChecklistID: Identifier for safety checklists.
- complianceStatus: Compliance status with safety regulations.
- incidentReports: Reports of safety incidents.

Functions:
- conductSafetyAudit(): Conduct a safety audit of the facility.
- updateSafetyProtocols(protocolDetails): Update safety protocols and procedures.
- logIncident(incidentDetails): Log a safety incident.

21. Compliance Management System Class
Attributes:
- complianceID: Unique identifier for each compliance requirement.
- regulatoryBodies: Information about relevant regulatory bodies.
- complianceStatus: Current compliance status for various regulations.
- auditTrail: Records of compliance audits and findings.

Functions:
- assessCompliance(): Assess current operations against compliance standards.
- scheduleComplianceAudits(): Schedule regular compliance audits.
- updateComplianceRequirements(requirements): Update system with new or changed compliance requirements.
- generateComplianceReports(): Generate reports for internal use and regulatory submissions.

22. Environmental Monitoring System Class
Attributes:
- sensorID: Identifier for environmental sensors.
- environmentalData: Data related to environmental conditions.
- alerts: Environmental alerts and warnings.

Functions:
- monitorConditions(): Monitor environmental conditions.
- setAlertThresholds(thresholds): Set thresholds for environmental alerts.
- generateEnvironmentalReport(): Generate reports on environmental conditions.
- respondToAlert(alertID): Respond to environmental alerts.

23. Energy Management System Class
Attributes:
- sensorID: Identifiers for energy consumption sensors.
- energyUsage: Current energy usage data.
- efficiencyRatings: Efficiency ratings of various plant processes.
- energySavingGoals: Set goals for energy savings.

Functions:
- monitorEnergyConsumption(): Monitor real-time energy consumption across the plant.
- optimizeEnergyUsage(): Optimize energy usage to improve efficiency.
- setEnergyTargets(targets): Set and adjust energy-saving targets.
- generateEnergyReports(): Produce reports on energy usage and savings.

24. Inventory Management System Class
Attributes:
- inventoryID: Unique identifier for each type of inventory item.
- stockLevels: Current stock levels of various items.

- reorderThreshold: Threshold levels at which reordering is triggered.
- supplierInfo: Information about suppliers for each inventory item.

Functions:

- monitorStockLevels(): Continuously monitor and report current stock levels.
- triggerReorder(itemID): Automatically trigger reordering of items that fall below threshold.
- updateInventory(itemID, quantity): Update inventory levels after receiving or consuming stock.
- generateInventoryReport(): Generate reports on inventory status, trends, and forecasts.

25. Asset Management System Class

Attributes:

- assetID: Unique identifier for each physical and digital asset.
- assetType: Type of the asset (e.g., machinery, software).
- assetStatus: Current status (e.g., operational, under maintenance).
- maintenanceSchedule: Scheduled maintenance activities for assets.

Functions:

- trackAssets(): Keep track of all assets within the organization.
- scheduleMaintenance(assetID): Schedule regular maintenance for assets.
- updateAssetStatus(assetID, status): Update the status of each asset.
- generateAssetReports(): Generate reports on asset utilization, status, and maintenance.

26. Supply Chain Management System Class

Attributes:

- orderID: Unique identifier for supply orders.
- supplierDetails: Information about suppliers.
- inventoryLevels: Current levels of inventory.

Functions:

- placeOrder(orderDetails): Place an order for supplies.
- updateInventory(item, quantity): Update the inventory levels.
- monitorSupplierPerformance(): Monitor and evaluate supplier performance.
- forecastDemand(): Forecast future supply needs.

E. Threat Modelling Technique and Security Framework:

I. Threat Modelling (STRIDE):

STRIDE on the Remote Access Solution for Paper Production Plant

The following STRIDE threat modelling apply to the Remote Access Solution for Paper Production Plant

STRIDE	Identified Threats
Spoofing	**Spoofing Threat 1:** The remote application needs to be accessible to engineers from different geographical locations. Therefore, the login feature, and its related features (i.e., password reset, etc.), need to be easy to use. However, the ease of use must not introduce a threat which allows an adversary to circumvent or misuse login features (and thus gain access to user credentials). ● **Risk Assessment:** ○ Likelihood: Moderate, as user-friendly systems can often have vulnerabilities. ○ Impact: High, as unauthorized access could lead to significant security breaches. ○ Priority: High, due to the potential for widespread system compromise. ● **Mitigation strategies:** ○ Implement multi-factor authentication (MFA) to enhance login security. ○ Regularly update and patch authentication systems. ○ Conduct user education on secure password practices. **Spoofing Threat 2:** Adversary exploits captured or guessed credentials to impersonate an authorised remote engineer, compromising the integrity of production line settings. ● **Risk Assessment:** ○ Likelihood: High, especially if credential management is weak. ○ Impact: High, as it could compromise the integrity of critical production settings. ○ Priority: High, considering the direct threat to operational integrity. ● **Mitigation strategies:** ○ Enforce strong password policies and credential rotation. ○ Utilize advanced authentication mechanisms like biometrics or hardware tokens. ○ Monitor for unusual login patterns or locations. **Spoofing Threat 3:** Adversary resorts to intimidation or coercion, pressuring a user to disclose valid credentials or comply with activities dictated by the attacker, potentially leading to unauthorized modifications in production parameters. ● **Risk Assessment:** ○ Likelihood: Moderate, depends on social engineering tactics and user awareness. ○ Impact: High, could lead to unauthorized changes in production. ○ Priority: Moderate to High, depending on user training and security culture. ● **Mitigation strategies:** ○ Provide training on recognizing and reporting social engineering attacks. ○ Establish a protocol for verifying identity in high-risk situations. ○ Implement an incident response plan specifically for credential compromise.

	Spoofing Threat 4: If the user's access device (such as a laptop for example) becomes a target for attack and compromise, allowing unauthorized access to the control system network, thereby risking unauthorized alterations in production line settings. ● **Risk Assessment:** ○ Likelihood: High, as personal devices are common targets. ○ Impact: High, due to the potential control over production settings. ○ Priority: High, given the direct risk to the production control system. ● **Mitigation strategies:** ○ Ensure secure, encrypted channels for remote access. ○ Implement endpoint protection and regular security audits on user devices. ○ Enforce strict access controls based on the principle of least privilege.
Tampering	**Tampering Threat:** The remote access solution has restricted certain modification features for enhanced security. For instance, the majority of the production line settings are configured as read-only, preventing unauthorized alterations. However, there remains a potential threat wherein individuals other than the designated remote engineering team, particularly the current user, may attempt to tamper with critical production parameters like speed, temperature, and pressure, leading to potential disruptions in the paper plant's operations. ● **Risk Assessment:** ○ Likelihood: Moderate to High. While the system restricts modification features, the potential for tampering still exists, especially if there are any system vulnerabilities or user privileges that can be exploited. ○ Impact: High. Unauthorized alterations to production parameters like speed, temperature, and pressure can lead to significant disruptions, safety hazards, and financial losses. ○ Priority: High, due to the potential severe impact on the paper plant's operations and safety. ● **Mitigation strategies:** ○ Regularly review and update access permissions to reflect current roles and responsibilities. ○ Introduce multi-factor authentication for users accessing sensitive controls, adding an extra layer of security against unauthorized access.
Repudiation	No Repudiation threats identified.

Information Disclosure	**Information Disclosure Threat 1:** Company's production chain is unique and all production settings are confidential. There is a threat that some engineers working remotely may access confidential settings, through lack of access controls. ● **Risk Assessment:** ○ Likelihood: High. Without adequate access controls, the possibility of remote engineers or others accessing confidential information is significantly increased. ○ Impact: High. The disclosure of unique production chain settings can lead to competitive disadvantage, intellectual property theft, and potentially compromise production integrity. ○ Priority: High, due to the critical nature of the confidential information and its impact on the company's competitive positioning and operational security. ● **Mitigation strategies:** ○ Strict Access Controls: Implement role-based access control (RBAC) systems to ensure that only authorized personnel have access to confidential settings. ○ Regularly review and update access rights to ensure they align with current job roles and responsibilities. ○ Use multi-factor authentication for accessing sensitive systems to add an additional layer of security. ○ Encrypt sensitive data both during transmission and while stored to prevent unauthorized access and ensure data integrity. ○ Segregate sensitive information and systems from less critical systems to minimize the risk of unauthorized access. ○ Implement network segmentation and firewalls to control data flow.
Denial of Service	**Denial of Service Threat:**An attacker floods the Authentication Function with excessive authentication requests, causing a denial-of-service. This can end up in disruption in the authentication process, preventing legitimate users (remote engineer group) from accessing the production line settings. ● **Risk Assessment:** ○ Likelihood: High. DoS attacks are common, especially if the authentication system is exposed to the internet and not adequately protected. ○ Impact: High. A successful DoS attack could disrupt the authentication process, preventing legitimate users from accessing critical production line settings, which could lead to significant operational disruptions. ○ Priority: High, given the potential for operational paralysis and the relative ease with which such attacks can be executed. ● **Mitigation strategies:** ○ Rate Limiting and Throttling: Implement rate limiting on the number of authentication requests a user can make in a given period to prevent flooding. ○ Design the authentication system to handle high loads and to segregate authentication traffic from other critical services. ○ Employ DDoS Protection Tools and Services:that can detect and filter out malicious traffic.
Elevation of Privilege	**Elevation of Privilege Threat 1:** If the Authorization Function does not adequately validate access requests, an attacker could manipulate accessLevel. Unauthorized elevation of privileges within the Remote Access & Configuration Function, enabling the attacker to gain control over production line settings. ● **Risk Assessment:**

	○ Likelihood: Moderate to High. If there are weaknesses in the authorization process, it's feasible for an attacker to exploit these vulnerabilities. ○ Impact: High. Unauthorized control over production settings can lead to significant operational disruptions, safety issues, and financial losses. ○ Priority: High, given the potential severe consequences of an attacker gaining elevated privileges. ● **Mitigation strategies:** ○ Strict Access Controls: Implement role-based access control (RBAC) systems to ensure that only authorized personnel have access to confidential settings. ○ Regularly review and update access rights to ensure they align with current job roles and responsibilities. ○ Ensure that the Authorization Function has rigorous validation checks to prevent unauthorized elevation of privileges. ○ Use MFA for critical functions, adding an extra layer of security to prevent unauthorized access. ○ Adhere to the principle of least privilege, ensuring users are given the minimum level of access necessary to perform their job functions.

II. Security Framework (NIST CSF):

To strengthen the security maturity of the remote access solution for the paper production plant, implementing the NIST cybersecurity framework is an excellent approach. The NIST cybersecurity framework is structured around five key domains: Identify, Protect, Detect, Respond, and Recover. Each domain contains specific standards, guidelines, and practices.

Rationale:

The decision to adopt the NIST cybersecurity framework for the project, with a focus on remote access and configuration in an industrial automation setting, is driven by its industry-wide recognition, comprehensive coverage, and alignment with regulatory requirements. The framework's adaptability to the complexities of the system components ensures its relevance to the unique challenges presented. Furthermore, its risk management focus is crucial for identifying and prioritizing potential threats in the system, particularly as it involves the remote engineering team modifying production line settings. The continuous improvement cycle inherent in the NIST framework aligns well with the commitment to staying ahead of evolving cybersecurity threats. By adhering to this framework, a structured and globally respected approach is established that not only enhances cybersecurity practices but also facilitates compliance with industry standards like GDPR and ISO/IEC 27002. Ultimately, the choice of the NIST cybersecurity framework is a strategic decision aimed at ensuring the integrity, reliability, and long-term security of industrial automation processes.The NIST cybersecurity framework provides a robust and adaptable approach to address the unique challenges presented by industrial automation context.

NIST Cybersecurity Framework Pillars and Implementation:

a. Identify:

Asset Management:

- Catalog and manage all physical and software assets to support other cybersecurity framework functions.
- List all hardware, software, data, and network assets.

Business Environment Understanding:

- Understand the business context, resources, and risk tolerance to effectively prioritize efforts.
- Define the role of the remote access system in the business context.

Risk Assessment:

- Conduct a comprehensive risk assessment for the system.
- Identify, document, and analyze risks based on the inventory and business context.

Risk Management Strategy:

- Develop and implement a risk management strategy in line with the business's requirements, risk tolerance, and resources.

b. Protect:

Access Control:

- Limit access to assets and associated facilities to authorized users, processes, or devices.
- Restrict access to critical functionalities through role-based access controls (RBAC).

Data Security:

- Protect data integrity, confidentiality, and availability.
- Encrypt sensitive data and apply DLP measures.

Policy Development:

- Develop comprehensive security policies, including incident response and business continuity.

Regular System Maintenance:

- Schedule and conduct regular system maintenance.

Deploy Protective Technologies:

- Utilize firewalls, antivirus software, and intrusion detection systems.

c. Detect:

Monitor Network and Systems:

- Implement advanced monitoring tools for real-time analysis.
- Detect anomalous activity and potential cybersecurity events.
- Maintain detection processes and procedures.

d. Respond:

Response Planning:

- Make a response plan during or after a cybersecurity event.
- Outline steps and responsibilities for addressing cybersecurity incidents.

Communications:

- Manage internal and external communications during and after a cybersecurity incident.

Analysis:

- Analyze the impact and scope of incidents.

Mitigation:

- Implement procedures for incident analysis and mitigation.

Post-Incident Reviews:

- Conduct reviews after incidents to improve response strategies.

e. Recover

Recovery Planning:

- Develop and implement recovery processes to restore systems and assets affected by cybersecurity incidents.
- Implement recovery planning improvements based on lessons learned.
- Coordinate restoration activities with internal and external parties.

By implementing the NIST cybersecurity framework, the paper production plant will significantly strengthen its cybersecurity posture, ensuring that the remote access system is robust, secure, and resilient against potential cyber threats.

F. GDPR - Data Privacy concern:

a. Identification of Personal Data:

- Employee Information: Names, employee ID numbers, contact information, job titles.
- Biometric Data: Fingerprints or facial recognition data
- Access Logs: Information about system access.
- Configuration Data: Production line settings and parameters.
- User Authentication Data: Usernames, passwords, authentication logs.
- Communication Data: System-related messages, alerts, and notifications.
- Maintenance and Support Data: Information related to system maintenance and support.

b. Identification of data sources and destinations:

- Remote Access and Configuration Function Class:
    - Data Sources: Remote user input during login, configuration changes.
    - Destinations: Remote system, configuration database.
- User Management Function Class:
    - Data Sources: User input during the registration process, user profile updates.
    - Destinations: User database, authentication process.
- Authentication Function Class:
    - Data Sources: User input during login.
    - Destinations: Authorization process, user session data.
- Role Management Function Class:
    - Data Sources: Admin input for role creation and updates.
    - Destinations: Role database, permission assignment.
- Permissions Management Function Class:
    - Data Sources: Admin input for permission assignment.
    - Destinations: Permission database, authorization process.
- Authorization Function Class:
    - Data Sources: User roles, permissions.
    - Destinations: Access control decisions, authentication process.
- PLC Control System Class:
    - Data Sources: Commands from the system, sensor data.
    - Destinations: Machineries and systems, status updates

c. Legal Basis for Processing:

- **Employee Information:** Contractual necessity (art 6(1)(b)) and compliance with legal obligations (art 6(1)(c)).
- **Biometric Data:** Explicit consent (art 9(2)(a)) or potentially contractual necessity.
- **Access Logs, Configuration Data, User Authentication Data, Communication Data, Maintenance and Support Data:** Contractual necessity and legitimate interests (art 6(1)(b) and art 6(1)(f)).

d. Data Minimization:

Processing of only the data necessary for the specific purposes identified.

e. Security Measures:

This automation system will have implementation of robust security measures, including encryption and pseudonymization, to ensure the confidentiality, integrity, and availability of personal data (art 32).

g. Data Protection Impact Assessment (DPIA):

Conduction of a DPIA, especially for the processing of sensitive data like production line setting parameters, to assess and mitigate potential risks (art 35).

h. Consent and Transparency:

Obtaining explicit consent where necessary, and ensuring transparent communication with employees about data processing activities.

i. Data Subject Rights:

Respecting and facilitating the exercise of data subject rights, including the right to access, rectification, erasure, and data portability.

k. Documentation:

Maintaining centralised and regularly updated records of all processing activities, implementing automated tools for efficient tracking, and integrating data protection impact assessments. Enforce access controls, maintain audit trails, and conduct regular reviews, fostering transparency and compliance with GDPR (art 30).

l. Data Breach Response:

Promptly detecting and isolating incidents, activating a designated response team, assessing and mitigating data breaches. Complying with GDPR, notify authorities and affected individuals, and continuously train and refine response protocols for effective incident management. (art 33 and art 34).

G. Find on vulnerability and explain how it can be handled:

The following part demonstrates how vulnerabilities were found in a remote access solution by following a systematic approach which consists of identifying system assets, defining security objectives and potential threats, including attack tree.

System Assets:

- Hardware Assets: This includes servers, network devices, PLCs, and other machinery involved in paper production.
- Software Assets: The remote access application, operating systems, and any other software used for control and monitoring.
- Data Assets: Operational data, including production parameters, quality metrics, and user data. Compliance-related data for GDPR and NIST cybersecurity framework.
- Network Assets: LANs and WANs, along with associated infrastructure like routers and switches.

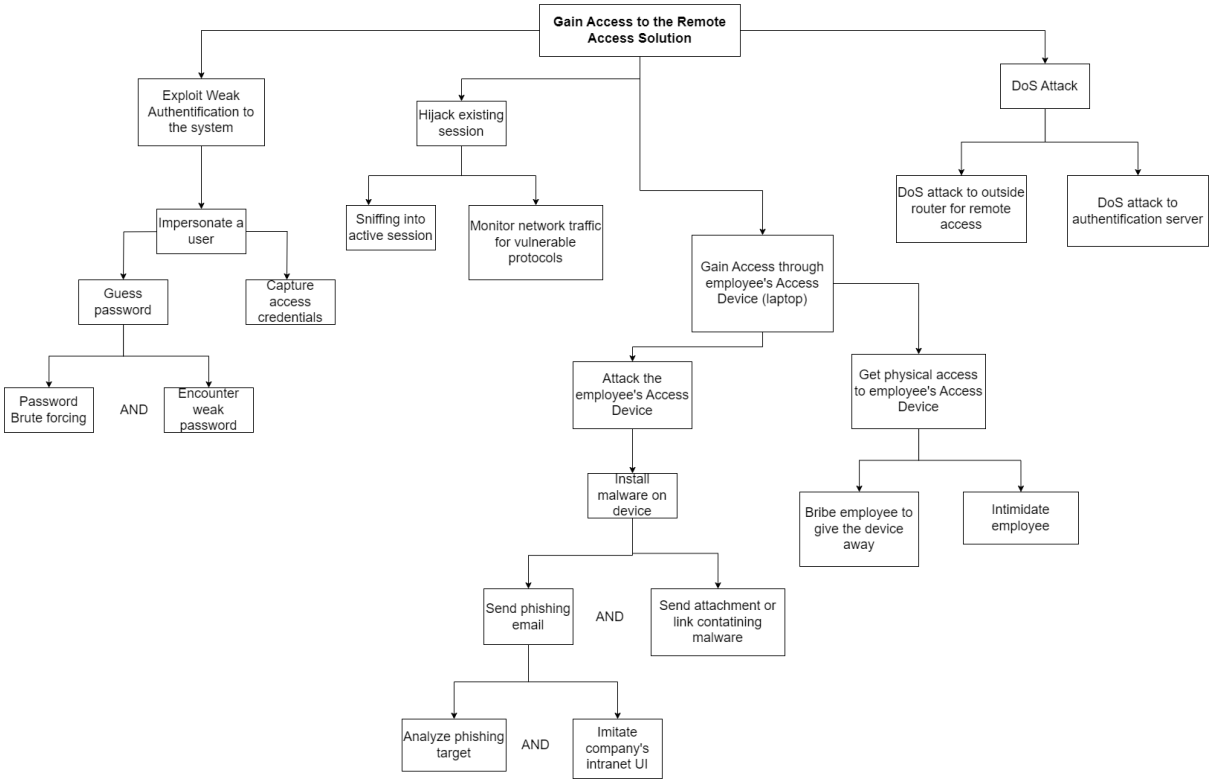
Security Objectives:

- Confidentiality: Ensuring that sensitive information is accessible only to authorized individuals.
- Integrity: Safeguarding the accuracy and completeness of data and preventing unauthorized data modification.
- Availability: Ensuring that the system and its data are available to authorized users when needed.
- Compliance: Adhering to legal and regulatory standards, particularly GDPR and NIST CSF.
- Safety: Ensuring the physical safety of the plant, machinery, and personnel.

Potential Threats:

- Unauthorized Access: Due to weak authentication or compromised credentials.
- Data Breach: Leading to the exposure of sensitive operational data.
- System Tampering: Unauthorized changes to system configurations or PLC settings.
- Denial of Service: Attacks that could render the remote access system unavailable.
- Malware: Including ransomware that could disrupt operations.

Attack Tree Analysis:
An attack tree provides a visual representation of the potential threats and the paths an attacker might take to exploit vulnerabilities.
Note: For the following attack tree all attacks were based on CAPEC library.



Handling Identified Vulnerabilities:

- Strong Authentication Protocols: Implement multi-factor authentication and enforce strong password policies.
- Regular Software Updates: Keep all systems updated to patch known vulnerabilities.
- Employee Training: Conduct regular training on identifying phishing attacks and following security best practices.
- Network Security Measures: Use firewalls, intrusion detection/prevention systems, and network segmentation.
- Access Control: Implement role-based access controls to limit access based on user roles and responsibilities.
- Physical Security: Secure physical access to critical infrastructure and hardware.

Threat Analysis:

- Perform Regular Threat Assessments: Continuously assess the threat landscape to identify new and emerging threats.
- Penetration Testing: Conduct regular penetration tests to uncover vulnerabilities.
- Security Audits: Regular audits to ensure compliance and identify security gaps.

By systematically identifying assets, security objectives, potential threats, and analyzing them through an attack tree, vulnerabilities can be better understood and addressed. This comprehensive approach ensures a robust security posture for the paper production plant's remote access system.

H. Security requirement based on that vulnerability

Based on the identified vulnerabilities and the security objectives in the scenario of the remote access solution for a paper production plant, it can be seen that improvements should be done to the following aspects - Authentication and Access Control, Network Security, Data Protection and Privacy. Thus, new security requirements can be formulated. These requirements are designed to address potential threats and ensure the integrity, confidentiality, availability, and compliance of the system.

Authentication and Access Control:

- In the context of security considerations, the system shall require multi-factor authentication (MFA) for all users accessing the system, ensuring an additional layer of security beyond just passwords.
- In the context of security considerations, the system shall implement role-based access control (RBAC) to ensure that users have access only to the resources necessary for their specific roles and responsibilities, enhancing security and operational efficiency.
- In the context of security considerations, the system shall enforce regular password updates and adhere to strong password policies, requiring users to frequently change passwords and use complex, hard-to-guess passwords.

Network Security:

- In the context of security considerations, the system shall deploy firewalls to control incoming and outgoing network traffic based on predetermined security rules, thereby preventing unauthorized access and safeguarding network integrity.
- In the context of security considerations, the system shall implement network segmentation to segregate the network, limiting the spread of attacks and reducing the overall attack surface.
- In the context of security considerations, the system shall utilize secure Virtual Private Networks (VPNs) for remote access, ensuring that all data transmitted during remote access sessions is encrypted and secure.

Data Protection and Privacy:

- In the context of security considerations, the system shall encrypt sensitive data both in transit and at rest, safeguarding confidential information against unauthorized access and breaches.
- In the context of security considerations, the system shall implement Data Leakage Prevention (DLP) tools to prevent unauthorized access.

These detailed security requirements, when implemented, will address the vulnerabilities identified in the threat analysis, thereby enhancing the overall security posture of the remote access solution for the paper production plant. Regular review and updating of these requirements are also essential to adapt to evolving threats and technological changes.