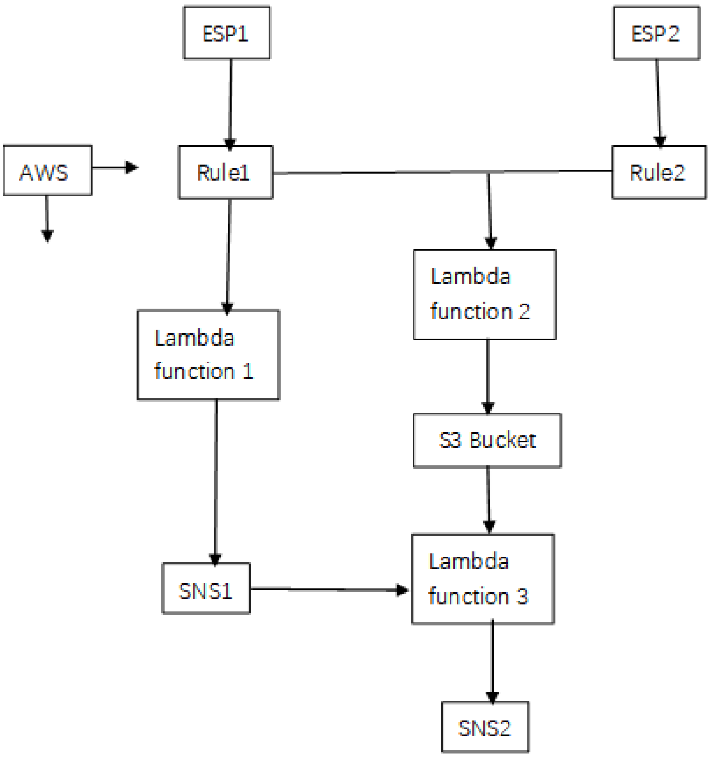
Final project report

Our Project name is Cloud-based dual inspection system for factory environment, which is a temperature and humidity alarm system designed for sensitive environments, especially factories where production is critical. Two ESPs act as temperature and humidity detectors, connected to a WIFI connection that sends a constant stream of temperature and humidity data to the AWS. When AWS receives a temperature above 70 degrees and a humidity below 30%, it sends an email warning to the manager to report the anomaly. After AWS sends out an alert, it compares the data collected by another ESP within a minute. If the difference in temperature and humidity is less than 10, It will continue to send emails alerting the factory to abnormal conditions. Judgment is made by secondary detection, thus avoiding false alarms due to certain malfunctions.

In the project we carried out a risk score calculation: the risk score is calculated by multiplying the likelihood (vulnerability) rating by the impact rating. The resulting score helps to prioritize risks. Likelihood (vulnerability) rating and impact rating are from 1-5 in descending order The security challenges included in the project are physical risks (risks related to physical damage or theft of IoT devices); communication risks (risks related to data transfer between devices and servers); cybersecurity risks (risks related to unauthorized digital access to the system), and Operational Risks. We have analyzed a total of 15 possible risks and labeled them with a serial number beginning with R. Of the physical risks, R1 is a power outage, which indicates a real risk of system outage or failure with an assessed likelihood of occurrence of 2. If such an event were to occur, the impact on plant operations would be considerable, with an impact score of 5. The total risk score is 10, which indicates that there is an urgent need for a robust contingency plan and back-up power solution to minimize operational disruption. The resulting total risk score of 10 indicates the critical need for robust contingency planning and backup power solutions to minimize operational disruption. R2 is sensor deterioration, a recurring risk that could result in operational damage with a likelihood of 2. This event, while unlikely, has a potential impact of 5 due to the criticality of the sensor data during double-checking. This equates to a risk score of 10. The risk score emphasizes the importance of preventive maintenance and regular evaluation of sensors to prevent failures from occurring. R3 for Physical Security Vulnerability: The likelihood of physical theft or tampering (especially of the ESP32 circuit boards) is low, with a total of 1. The impact of this security vulnerability, however, would be a risk of 1. However, the impact of such a security breach is high, i.e. a risk score of 5. Although the likelihood is low, the high impact requires strong physical security protocols to protect critical hardware components. Of the communication risks, R4 is Man-in-the-middle attack. This risk has a likelihood of 2, an impact of 4, and a risk score of 8, highlighting the vulnerabilities in the transmission of data to AWS. Mitigations may include the use of advanced encryption protocols and continuous monitoring of network traffic. R5 is SNS message spoofing. Since spoofed messages have the potential to compromise the integrity of the communication, this risk has a likelihood and impact of 2 and 3, respectively, for a risk score of 6. R6 is data corruption in transit. Data in transit may be corrupted due to unreliable communication links. The likelihood of this scenario is higher at 3, but the impact is comparable to R5, resulting in a risk score of 9. R7 is Wi-Fi Security Vulnerability. the vulnerability of Wi-Fi networks to attack is a significant issue, with a likelihood of 3 and an impact of 4, for an overall risk score of 12. Of the cybersecurity risks, R8 is a protocol encryption issue. A protocol encryption vulnerability could lead to a data leakage with a likelihood of 3 but an impact of 4, giving a risk score of 12. This requires the use of secure communication methods that are compliant with industry standards. R9 is unencrypted Lambda function calls. Unencrypted Lambda function calls can lead to data leakage, a risk with a likelihood of 2, but with an impact level of 5, resulting in a risk score of 10. This highlights the need to encrypt all serverless compute processes. R10 for Unauthorized IoT Access. Unauthorized access to AWS IoT rules can lead to data mishandling, with a likelihood of 3, an impact of 4, and a risk score of 12. It underscores the critical need for strict access controls and regular auditing of IoT configurations. R11 for S3 Storage Bucket Compromise. A compromise of an S3 storage bucket can have serious consequences, with an impact score of 5. With a likelihood of 3 and an impact score of 15, this risk is the highest of the cybersecurity risks, demonstrating the urgency of secure storage practices and vulnerability detection systems. R12 for DDoS Attacks. The threat of a DDoS attack is assessed as a likelihood and impact of 3 and 4, respectively, with a risk score of 12. Defending against this type of attack requires a multilayered security strategy. For Operational Risk, R13 is Lambda Function Error. An incorrect Lambda function could result in data loss with a likelihood of 2, an impact of 3, and a risk score of 6. R14 is S3 container backup failure. Lack of a proper S3 storage bucket backup process could result in data loss, which has a low probability of 1 but a high impact of 4, resulting in a risk score of 4. R15 is AWS service outage. Information overload could result in an AWS service outage with a likelihood of 2 and an impact of 3, giving a risk score of 6. The above risks must be countered accordingly

To manage or address these risks, we use the following three approaches: Risk mitigation, Risk transference and Risk acceptance. Mitigation measures for R1 include uninterruptible power supply (UPS) and standby generators, as well as periodic testing. Risks are transferred through business interruption insurance. Residual risk is recognized and accepted. R2 is addressed through regular maintenance and lifecycle management, with risk outsourced to the supplier under liability terms. Inherent wear and tear of sensors is accepted as a residual risk. R3 Enhanced physical security measures and equipment tracking, along with theft and damage insurance, accept the residual risk of such events. R4-R7 risk reduction focuses on authentication protocols and secure transport using end-to-end encryption and redundancy. Risk is transferred through service agreements and indemnification clauses. Acceptance of residual risk is based on the robustness of implemented controls and the perception of low impact of potential breaches. R9-R11 focuses on the latest encryption standards, least privilege access and multi-factor authentication to protect critical data. Transfer is achieved through cyber liability insurance and partnerships with security firms. After rigorous security measures and reviews, residual risk was accepted, while recognizing that no system is completely watertight. R12-R15 enhances operational stability with detailed logging, automatic rollback, regular data backups, and strict access controls. Risks are mitigated through proactive response strategies with the help of third-party managed services and highly durable cloud storage. Acceptable risks are those that can be quickly addressed through the flexibility of existing protocols and cloud-based infrastructure.

Now you see all risks can be ameliorated in all three ways. The reason we decided to use the above measures is to keep the system as stable as possible. This way the system can respond quickly to most emergencies to meet real needs Below is our proposed solutions which matches the functional description of our project



In response to the question mentioned in the Q&A session in the final presentation. If we want both ESPs to publish to one topic at the same time and only to one topic, we may need to change the AWS policy, the code in PlatformIO regarding the publication of the topic, and the AWS rule used for alerts and difference comparisons. The reason we are using two boards to publish to different topics is because we want to differentiate the data as much as possible so that we can do functionality extensions later on.

Written by Xianyao Li