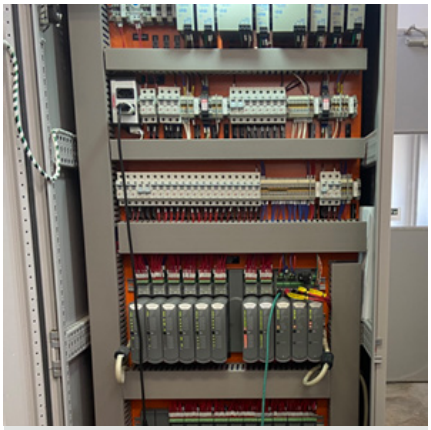
SENSIA
Rockwell Automation + SLB

+ CASE STUDY

Successful AADvance firmware upgrade at a leading gas terminal in Brazil

Enhancing safety and cybersecurity through strategic firmware modernization



Key Highlights

+ Resolved legacy hardware/ cybersecurity risks via firmware upgrade to Windows 10.
+ Zero-downtime upgrade on critical gas unit.
+ Ensured SIL-3 compliance through rigorous testing and real-time monitoring.
+ Scalable framework created for future upgrades (50% capacity expansion).

A major natural gas processing terminal in Brazil, vital to over a third of the country's energy production, faced recurring hardware failures, cybersecurity vulnerabilities, and risks of unplanned shutdowns. To address these issues, a critical firmware upgrade was implemented, along with a migration to a secure Windows 10-based environment. This modernization eliminated operational risks, enhanced cybersecurity, ensured compliance with safety standards, and established a scalable framework for future upgrades—safeguarding current operations and supporting long-term capacity expansion.

Challenges

+ **Aging Infrastructure:** A legacy safety system (SIL-3 certified) experienced intermittent failures in I/O modules and PLC communications, triggering production downtime.
+ **Cybersecurity Gaps:** Outdated firmware relied on obsolete software (Windows 7), exposing critical infrastructure to vulnerabilities.
+ **Operational Criticality:** The upgrade required zero disruption to a processing unit handling 1,600 m^3/h of natural gas, with plans to increase capacity by 50%.
+ **Legacy System Constraints:** Limited spare parts and documentation increased risks during the upgrade.
+ **Reversibility Demands:** A fail-safe rollback plan was mandatory to revert to the original system if critical issues arose.

Solutions

The upgrade was meticulously planned and executed in two phases. During preparation, spare I/O modules and a legacy CPU were secured to address potential failures, while SIL-3 safety loop documentation was validated to ensure testing accuracy. Collaborative risk assessments with cybersecurity experts ensured the Windows 10-based SIS Workstation met industry standards. The execution phase involved deploying updated firmware, migrating to the modernized development environment, and conducting enhanced diagnostic tests on PLC communications to preempt interoperability issues. Real-time monitoring tools were employed during the upgrade to detect anomalies, while a staged rollback protocol ensured operational continuity. Post-upgrade, cross-functional teams validated SIL-3 compliance through simulated failure scenarios, ensuring no residual risks to safety or production.

Results

The upgrade resolved critical hardware and cybersecurity issues, eliminating unplanned shutdowns and ensuring SIL-3 compliance. A subsequent network failure highlighted the modernized system's resilience, as only upgraded components maintained uninterrupted operations. The project's success secured approval to modernize remaining systems during planned maintenance windows, minimizing operational disruption. By addressing legacy risks and establishing a replicable upgrade framework, the terminal enhanced long-term reliability, cybersecurity posture, and scalability to meet future production demands.