Safety Instrumentation and Management

Project 12

Description

LOGIIC conducted Project 12, Safety Instrumentation and Management, in 2019-2020. The final technical report highlights numerous consequential and reoccurring exploitable weaknesses found during the project and provides a roadmap for the short-, mid-, and long-term risk mitigations.

Download the Report

Industrial Control Systems use safety instrumented systems (SISs) to monitor operations and take automated actions to maintain a safe state when abnormal conditions occur. Instruments such as transmitters, valve controls, and fire and gas detectors provide inputs and controls to safety system function. Instruments have been modernized over time to provide smart features such as valve partial stroke testing.

The lack of security concepts in the HART protocol necessitates the use of alternative methods to protect devices from unauthorized modifications. Protections considered under Project 12 included a hardware write-protect switch on the instrument, a software-based write-protect

password or pin code on the instrument, password on the IMS/AMS (or its underlying operating system platform) that remotely manages the instrument, and a variety of dispar protections provided by various SIS solutions.

Successfully demonstrated attacks used commonly available attacker tools and exploited common-knowledge architectural weaknesses that were present in all four assessments. These attacks required a low to moderate level of effort to exploit and included effects that can significantly impact device safety function.

Project 12 exposed the risks associated with the two architectures and determined the circumstances under which each architecture poses the least risk.

Key findings include:

- Attackers can make unauthorized device changes at will and evade detection. Some changes can result in unsafe operating conditions. The risk of cyberattack directly impacts safety and must be considered along with hardware faults and other safety considerations.
- There is no simple and immediate remedy for securing safety systems; risk reduction requires a combination of protection and detection mechanisms.
- Safety systems architectures that mediate IMS/AMS and safety instrument communications using an SIS with enabled protective features pose less risk of unauthorized device modification than do architectures using a passthrough MUX. If SIS protections are not enabled, the risk is equivalent to that of using a MUX.
- Device hardware-based write protections are the only fully protective means to prevent unauthorized device configuration changes. Only 33% of sampled devices had hardware switches.
- Software-based write protections can be bypassed with little effort; therefore, they do not protect against these changes. SIS write protections effectively prevent some, but not all, changes.
- Device write-protect implementation is inconsistent, even across the same vendor products. This can lead to confusion and accidentally unprotected devices.
- HART protocol lacks basic security concepts and does not include standardized security-relevant commands, which leads to inconsistent implementation across devices using device-specific commands. This hinders the detection of attempts to circumvent device security features. The protocol provides no means to differentiate device-specific read and write commands. This makes it impossible for any SIS to block device-specific write

commands without also blocking read commands. The IMS/AMS depends on reading values to update device status in the display.
- The practiced method of distributing and installing device type manager (DTM) software opens the door to a supply chain attacks and poses significant risk to IMS/AMS platforms. These platforms are trusted and can be used as a launch point for device attacks that can negatively impact safety system function.

Because of this, we conclude that safety systems are vulnerable to malicious attacks that may be undetectable in practice. Extreme caution should be taken before introducing any software, which could insert malware into the process control environment. We cannot sufficiently emphasize the severity of this vulnerability.

We recommend a vulnerability mitigation roadmap of short-, mid-, and long-term actions. Short-term actions are things that asset owners can do immediately to reduce their exposure and risk. Mid-term actions are things that asset owners can do cooperatively with vendors. Long-term actions are things that standards bodies and vendors can do to improve the security of safety system products.

LOGIIC is a collaboration of oil and natural gas companies and the U.S. Department of Homeland Security, Science and Technology Directorate (DHS S&T). We would like to thank DHS S&T for its leadership, vision, and commitment to enhancing ICS cybersecurity. We also acknowledge the numerous vendors who cooperated in this project and provided equipment and many staff hours. This project could not have been done without this support. Finally, we would like to thank the Project 12 test team, which included Dragos and Secrabus. These two organizations provided detailed technical analyses of safety system components that were critical to the success of this project. Work performed by SRI International was funded under contract to DHS S&T.

Project Links

Project 12 Report	Download PDF
Project 12 Briefing	Download PDF
Project 12 Mitigation Action Plan	Download Spreadsheet

Project 12 Presentation at the Industrial Control System Joint Working Group (ICSJWG) Spring 2021 Meeting	Watch Video
S4 Events Project 12 discussion, May 2021	Watch Video
"Getting to the HART of the Matter: An Evaluation of Real-World Safety System OT/IT Interfaces, Attacks, and Countermeasures", published at the 14th Cyber Security Evaluation and Test (CSET) workshop.	Read Article