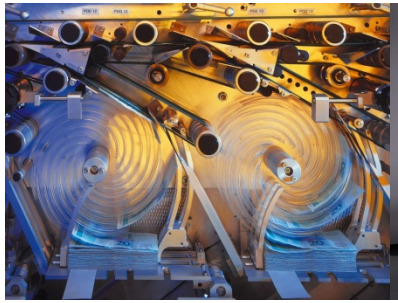
Development and Industrial Application of Multi-Domain Security Testing Technologies

Case Study Experience Sheet
Industrial Automation Case Study from Codenomicon, Metso Automation, OUSPG, VTT




ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

Industrial Automation Case Metso

Case study characterization

- The security of Industrial Control Systems (ICS) environments has traditionally not been considered as a great concern. However, especially in last decade the importance of the ICS security has become an important issue because these systems are, in addition to isolated and restricted industrial plants, also widely used in critical infrastructures, like in energy sector (power plants), petrochemical (oil and gas) and water treatment (water refineries, sewage treatment plants).
- Security is one essential issue to shield and protect ICS systems properly against evolving threats. This means that security has to be taken into account in the ICS development and maintenance and in this the testing has an important role.
- Traditionally security testing has not played very important role in ICS area. As its best security testing has been part of the overall availability, robustness and reliability testing.

Industrial Automation Case Metso
Case study characterization

- Security challenges in Industrial Control System networks:
  - ICS networks have high performance requirements in availability and response time.
  - Active testing is not possible in live networks – test are always executed to offline systems
  - Long life cycles of Industrial Control Systems (up to 30 years).
  - Very high cost of incidents, human lives may be lost due to errors
  - Software updating is challenging due to high availability requirements

Industrial Automation Case Metso

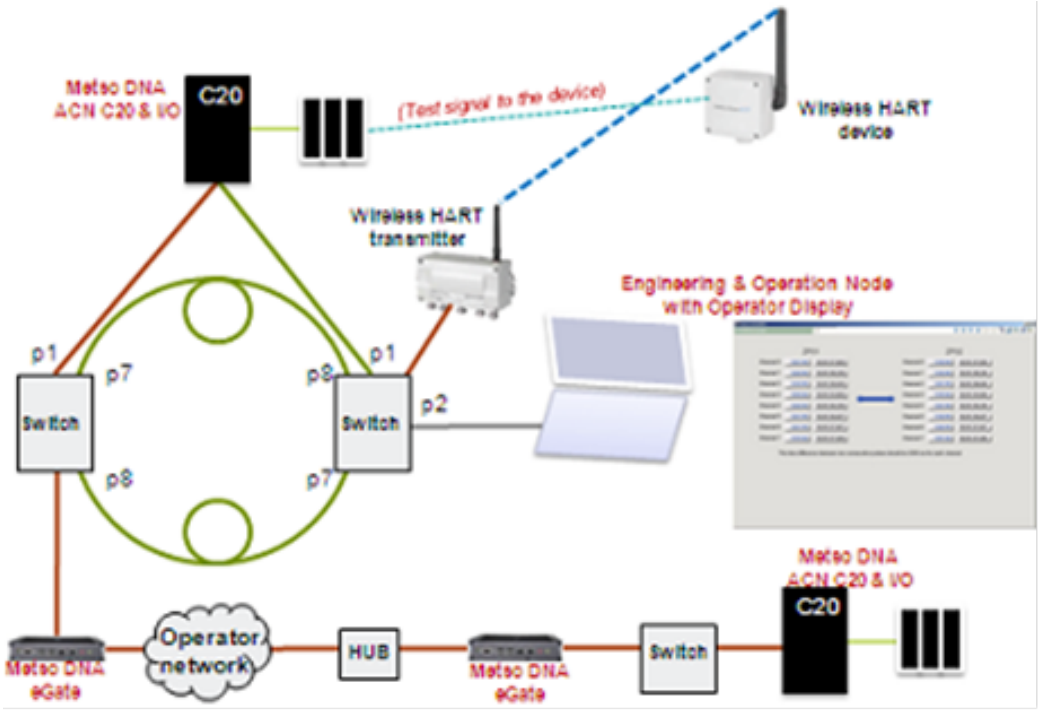
Security testing approach

The target in the industrial automation case study was to find and adapt the security testing framework (or suitable parts of it) and find practicable analysis and test techniques and methodologies to be used for industrial automation environment. Different approaches of the industrial case study include:

- **Automated code analysis (VTT)** by building up an environment and a plug-in component for gcc-compiler to produce for example a (global) control flow graph and extracting information about program structure and execution.
- **Machine learning approach to anomaly detection in ICS networks (VTT)**. Having a Network Intrusion Detection System that is able to adapt to the particular environment of an industrial site would reduce the risk of production disruptions caused by anomalous incidents on the network. Machine learning techniques are used in this approach.
- **Protocol-aware model-based fuzz testing (Codenomicon)** is investigated by using the traffic captures from real ICS environments.
- **Visual Proxy-based fuzzing** is applied to ICS environments by OUSPG.

Industrial Automation Case Metso

Security testing approach

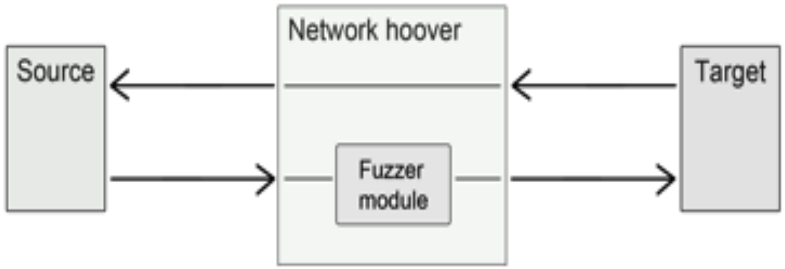


- **ICS demo environment** (Metso DNA) has been provided by Metso Automation as a target for testing the different approaches.

Industrial Automation Case Metso

Security testing approach: robustness testing

- Situation
  - Case study provider installed their setup
  - OUSPG was evaluating for potential robustness vulnerabilities
- Advances
  - New test case injection method for real time testing – Network hoover. Works as a proxy and combines robustness testing of the application level protocol.



- Results:
  - Issues were reported to case study provider, evaluated and confirmed. Improved awareness and product.

Industrial Automation Case Metso
Results and experiences

- IDS machine learning approach works well in a closed environments that include only a little noise. The challenging part is identifying and selecting features from the traffic, which is one of the most important steps in machine learning. Development of this approach is still ongoing.
- Effective test case injection lowers the bars for DIAMONDS tools to be used in ICS. Robustness testing proved (again) as an effective way to eliminate vulnerabilities.
- Codenomicon is investigating protocol-aware model-based fuzz testing based on traffic captures, and was interested in comparing the functionality to a mutation fuzzer in order to help in reproduction of the found faults.
- One of the main challenges is, that how the different approaches developed during the DIAMONDS could and should be integrated with the vendor's existing (testing) environment.

Industrial Automation Case Metso
Exploitation

- Initial results point that using machine learning approach in ICS network intrusion detection reduces the risk of production disruptions caused by anomalous incidents on the network.
- GCC-compiler plugins and OUSPG's Network hoover tool have been delivered to case study provider and are in use. The results were useful and enhanced security.
- Codenomicon has performed a robustness testing session in Metso Automation System Testing Lab where several models of Metso DNA process control devices as well as selected other network devices were tested with other Codenomicon model-based test tools. The session was successful and provided useful results.

Industrial Automation Case Metso
Summary

- **Improvement gains according to DIAMONDS STIP:**