Pains, Gains and PLCs

Ben Green
Anhtuan Le
Rob Antrobus

Utz Roedig
David Hutchison
Awais Rashid

Ten Lessons from Building an Industrial Control Systems Testbed for Security Research
Testbeds
Lesson 1: Device and technology selections should be market-driven
Lesson 2: Homogeneity and heterogeneity in field sites
Siemens and Allen-Bradley PLCs

Siemens-only PLCs
Lesson 3: Process diversity is not always crucial
Diversity

Complexity

Scalability

?
Lesson 4: Hardware-in-the-Loop (HIL) is not essential in the Manufacturing Zone
Lack of exact mathematical models for representing the behaviours of sensors and actuators factors impacting simulation accuracy such as noise

Process diversity not a primary concern
hot-swap capability allows for a level of scalability with sensors and actuators, moving them between devices as and when required
Lesson 5: Simulations in the Manufacturing Zone are not favoured
Software does not provide simulations of many essential types of devices from different vendors

OR

same vendor but distinctive versions

Accuracy and reliability issues in mimicking real-life operations

Despite cost, physical equipment helps experimental rigour
Lesson 6: Virtualisation and VLANs provide ease of integration and scaling
Provide an easy and cost-effective way
To integrate new systems
OR
Scale up existing instances

Reduces technical knowledge required during experimental set up

Clean backups of known good systems should damage be caused during experimentation
Lesson 7: Employ a Management Network
**Reduces the need for pre-requisite knowledge**
Relies on all relevant research tools being in place
*Currently being addressed*

**Requires appropriate data capture points**
Capture traffic from all zones into a centralised location
*Currently being addressed*
Lesson 8: Setup Multiple Manufacturing Zones
Lesson 9: Comprehensively document as you build
Document
Communication and control processes
Known vulnerabilities in devices and software
Sample attack scenarios

Keeping documentation up-to-date is significant effort!
Lesson 10: Optimise data logging for security purposes
Contributing to open ICS datasets
Collection and distribution of data is limited
Involves a manual and time consuming process
*One for the future!*
Experimentation using the testbed


10 Lessons