ICBC
Capacity Building Center of the
Institute for Security and Safety

OT Security: the Demonstrator and Courses / Exercises

Institute for Security
and Safety GmbH (ISS)
at Brandenburg University
of Applied Sciences

Behlertstr. 3a/Haus B2
14469 Potsdam
Germany

Phone +49-162-7795748
Web www.uniss.org
E-Mail info@uniss.org

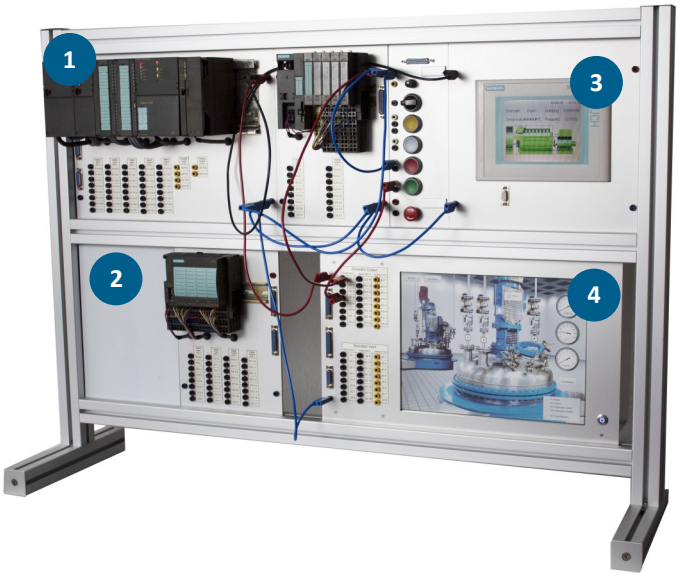
In the area of operational technology (OT), various problems arise with modernization, especially with regard to digitalization. Often, especially configured systems are used that date back to the time when cyber attacks were not perceived as a threat and are accordingly hardly, or not at all, secured. If these systems are now integrated into new networks, if possible also with the aim of remote control in digitized systems, then it is imperative to secure the OT systems against cyber attacks.

However, this requires cooperation between IT and OT managers on the one hand and communication between all players on the other. In many cases, this requires specific training that creates a common understanding of the problem situation and enables the participants to jointly develop suitable solutions by themselves.

A purely theoretical presentation is often not sufficient for a comprehensive understanding of the interrelationships between IT and OT and possibilities of harmful influence. The Institute for Security and Safety has therefore develo-ped a demonstrator that can be used to show examples of attack paths and processes, and to enable trainees to understand the effectiveness of their actions in real time.

Der ICBC Demonstrator:

1. Programmable Logic Controller (PLC) which controls the simulated environment (e.g. Siemens SIMATIC S7-300)
2. Field multiplexer PROFIBUS (de-centralized in/ output module on separate circuit board)
3. HMI: Operator display for PLC, displaying process data and controls, coupling via Profinet/Ethernet
4. Screen for scenario selection and visualization



Individual customization and development:

The demonstrator's components can be tailored to the needs and requirements of the customer.

Scenarios and exercises can be conceptualized for and integrated into the customer's specific environment.

ICBC
Capacity Building Center of the Institute for Security and Safety

Courses with the Demonstrator

Introduction to OT security:

This course offers an introduction to the world of Industrial Control Systems (ICS), the main differences between (office) IT systems and ICS, and insights into the challenges and best practices of OT security. Participant's learning goals are understanding of the characteristics of OT security, the protection of critical assets without compromising their availability, as well as an understanding of the conflict potentials between IT and OT security.

Training course content and form can be adjusted individually.

Example agenda for a 5-day training course on OT security:

	Day 1	Day 2	Day 3	Day 4	Day 5
Training resources		up to 4 ISS ICS simulators	up to 4 ISS ICS simulators	Demonstrator	Demonstrator
Morning 1	Assembly and launch of the exercise environment	Introduction III - Control systems (communication, protocols)	Introduction V - Typical ICS vulnerabilities	Other PLC and bus systems (i.a. ModBus / Modbus TCP)	Development of the necessary elements for the awareness event in groups (procedure plan, software-tools, documents)
	Break				
Morning 2	Introduction I - Control systems (types, functions, deployment, use)	Introduction IV - Control systems (project planning/ programming)	Introduction VI - Attack vectors against ICS	Other PLC and bus systems (i.a. ModBus / Modbus TCP)	Coordination of the results
	Break				
Afternoon 1	Introduction II - Control systems (composition, elements)	Introduction IV - Control systems (project planning/ programming)	Exercise - Attacks against ICS - Part 1	Protection and Detection: Technical and organizational protection measures for ICS and their work environment	Simulation of the developed awareness event, role play with speakers and decision maker level
	Break				
Afternoon 2	Exercise - Identification and Classification of ICS (example-based)	Exercise - Handling of ICS	Exercise - Attacks against ICS - Part 2	Introduction to the simulation software of the Demonstrator	Wrap-up, course evaluation and farewell
					Dismantling of the exercise environment

Target groups:

- Technical employees in digitization,
- OT specialists with the desire to expand their existing knowledge in OT security with a view to future developments in the connected infrastructure,
- Engineers for industrial controls and control systems,
- ICS personnel,
- Security architects,
- ISOs, CISOs.

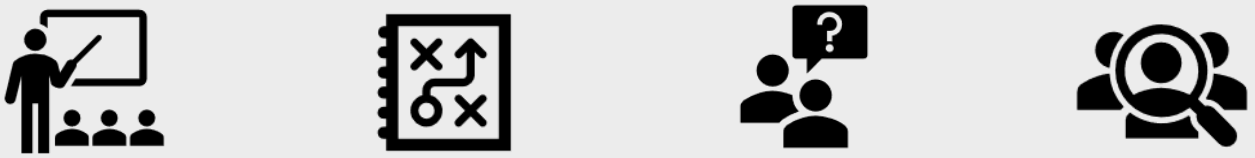
ICBC
Capacity Building Center of the Institute for Security and Safety

Cyber Exercises:

Cyber exercises provide a pragmatic way to understand and assess the impact of a cybersecurity incident. In the field of IT security, these exercises are often in the form of penetration testing based on various scenarios. The ICBC Demonstrator allows for the implementation of Cyber Exercises for Operational Technology. By actively 'playing' through the scenarios, the participants gain a basic understanding of the possibilities of influencing Programmable Logic Controllers and technical processes. Depending on the level of knowledge of the participants, they can use various scenarios to learn how to recognize attack routes, practice cyber defense and learn to carry out forensic analyzes. In this way, the participants gain a basic understanding of the vulnerability of their assets and information on how they can protect them. The scenarios and exercises can be customized.

Structure of the Exercises:

Introductory Training (optional) ➡ **Question-led Task** ➡ **Support during the Exercise** ➡ **Reflection/ Feedback after the Exercise**



Offensive Exercises:

Exercise 1: Reconnaissance
PLC will not be damaged, but the attacker obtains useful information

Exercise 2: Denial of Service
PLC communication will be interrupted, but recovers upon termination of the attack

Exercise 3: Send STOP command
PLC is permanently disrupted, manual reboot of the system is necessary

Exercise 4: Destruction of the system
Depending on the scenario, the aim is to achieve permanent damage to the system controlled by the PLC by manipulating the PLC.

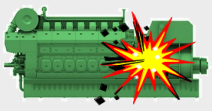
Defensive Exercises:

(for each of the exercises above)

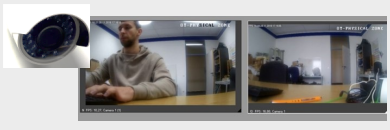
- **Organisational measures for prevention**
- **Technical measures for prevention**
- **Detection of attacks**
- **Forensic analyses**

Scenario Examples:

Electricity generator
Goal of attack: Destruction of the generator via manipulation of values, e.g. in the HMI



Video surveillance
Goal of attack: Tapping, manipulation, oder disruption of video feeds



Door opening systems
Goal of attack: Manipulation of databases (alteration of access rights), permament opening or closing of the installation