Safeticc

Experimental toolkit and integration kit for hands-on cybersecurity learning

SAFETICC is a cybersecurity experimentation kit, centered around an ANSSI*certified firewall. The concept is divided into two distinct pieces of equipment: an experimental kit designed to simulate an automated system under cyberattack, protected by a firewall, and a component kit for deploying the cybersecurity solution across various technical platform systems.
Both solutions include an attack generator that enables failure scenarios.

**French National Cybersecurity Agency*

Similar to a real-world system, the *SAFETICC* experimental kit includes both an OT (*Operational Technology*) section and an IT (*Information Technology*) section.
The OT section represents the core of a traditional automated system, featuring a PLC, HMI, status beacon, and Ethernet switch. The IT section involves the digital communication layer linking the OT to the external environment, integrating both the cyberattack device and the system's protective firewall.
All components are provided with the necessary network cables for communication. An operational unit can be connected to the kit, transforming it into a fully functional automated system. The kit includes an attack generator as well as firewall-protected components.

Educational Activities:

-Principles of cybersecurity
-Setting up a LAN and connecting elements in a digital information chain
-Implementing a cyberattack scenario
-Analyzing digital packets before and after an attack
-Firewall programming

ASTRIANE Didact
A brand of Ai Didact

1884, avenue Saint Maurice
04100 MANOSQUE
FRANCE

+33 (0)4 92 75 87 80
Fax : +33 (0)4 92 74 08 20
www.didact.fr

Safeticc

Experimental toolkit and integration kit for hands-on cybersecurity learning

Given the increasing frequency of attacks targeting all economic sectors of industrial companies, digital data protection has become a priority improvement area for many businesses.

The deployment of firewalls now extends to workshops, where machines often remain a weak link in digital security. Our product line, which includes multiple production lines, is particularly well-suited for implementing a digital protection solution.

Equipment Overview

The **SAFETICC** equipment is available in two solutions:

- An experimental case designed for understanding an industrial firewall device, its configuration, and operation.
- A kit that includes all the technical components necessary to deploy the industrial firewall on existing equipment in the product line.

Both solutions incorporate an attack generator that enables failure scenarios through DoS (Denial of Service) attacks, overwhelming normal communication with continuous requests.
The "Man-in-the-Middle" technique illustrates a cyberattack that follows an initial phase of observing digital exchanges, allowing malicious code to replace the clean code in machine programs.
This scenario is demonstrated on systems within our product line.

Functional characteristics

SAFETICC includes an interface with a customizable menu for each application:

- A universal mode allows for target customization (typically PLC, HMI, I/O modules) and selection of variables to disrupt.
- Preconfigured modes, "SAVONICC" and "RECYCLICC," feature pre-set PLCs for the line along with adjustable setpoints that can be modified (such as temperature settings, cutting parameters, etc.).

Associated systems

The ASTRIANE product line offers several systems compatible with the cybersecurity scenario. This includes the SAVONICC and RECYCLICC production lines.
A simpler application is also available, featuring a motorized conveyor whose operation is jeopardized by a cyberattack. The conveyor (OT) includes all the components required for its control and is connected to the control switch (IT) via a simple RJ45 Ethernet cable.

Here is an illustration of the motorized conveyor system and its connected control cabinet.

Pedagogical use

-LAN setup: using Machine Expert, configuring the HMI and remote device setup.
-Ethernet frame analysis with Wireshark.
-DoS attacks and their effects on the automated system.
-Frame analysis during a DoS attack: the principle of denial of service.
-Disruption or forced shutdown attack: effects on the system.
-Firewall setup and testing its functionality against different types of attacks.
-Analyzing frames before and after the firewall during a DoS attack.
-"Man in the Middle" attack (advanced level):
a) "Spy" mode with monitoring of frames exchanged between two devices.
b) Exporting a usable log on Wireshark to identify interesting frames for an attack.
c) Switching the "Man in the Middle" application from "Spy" mode to "Modify" mode for identified frames.
-Configuring advanced firewall rules.

General characteristics

Toolkit :
- LxWxH = 400x500x300 mm
- Weight : 8 kg
- Power : 230V - 50Hz
- power consumption = max 500W

Operative part:
- Lxlxh = 1000x150x100 mm
- Masse : 5 kg
- Power : 230V – 50Hz
- power consumption : 100W

ASTRIANE Didact
A brand of Ai Didact
1884, avenue Saint Maurice
04100 MANOSQUE
FRANCE
+33 (0)4 92 75 87 80
Fax : +33 (0)4 92 74 08 20
www.didact.fr