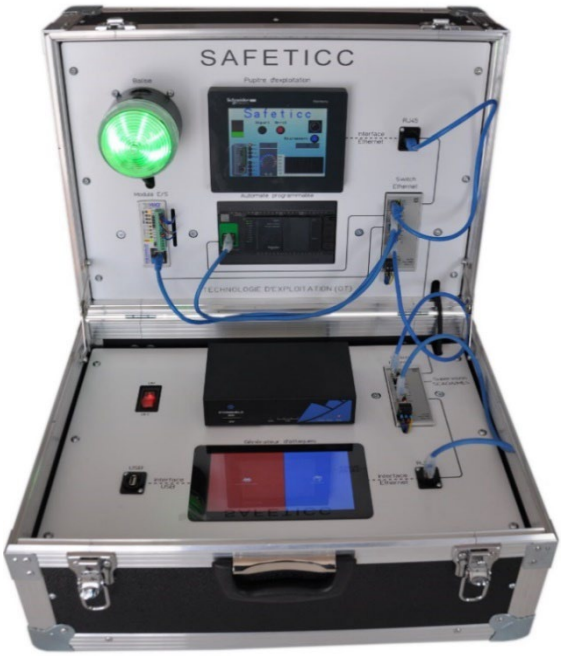
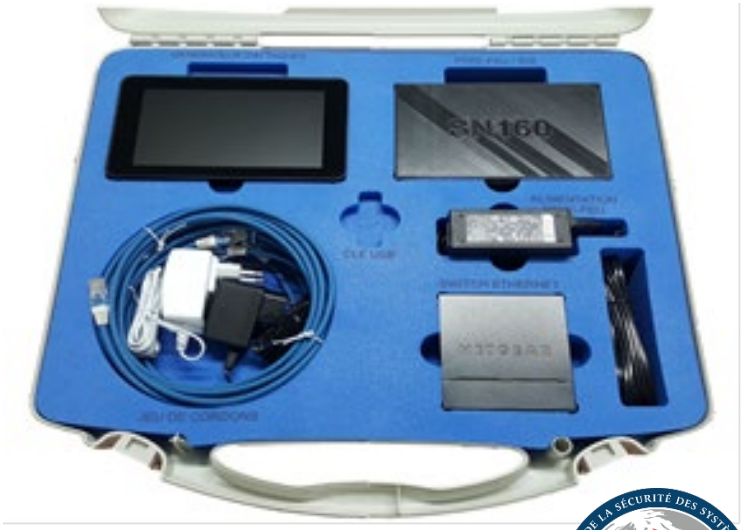
Safeticc

Experimental kit and kit to integrate for concrete learning about cybersecurity





***SAFETICC* is a cybersecurity experimentation set whose central element is an ANSSI* certified firewall. The concept is available in two perfectly distinct pieces of equipment: an experimental kit to simulate an automated system subject to a cyberattack and equipped with firewall protection, and a component kit for the deployment of the cybersecurity solution on various systems of the technical platform.**
Both solutions include an attack generator that ensures fault scenarios.

**French National Agency for the Security of Information Systems*

Like a real system, the *SAFETICC* experimental kit includes an OT *(Operation Technology)* section and an IT *(Information Technology) section*.
The OT presents the core of a classic automated system with PLC, HMI, status beacon and Ethernet switch. IT is about the digital layer of exchange between OT and the outside world. It integrates the cyberattack device and the system protection firewall. All of these components are accompanied by network cables required for communication.
An operating part can be connected to the briefcase, which then becomes a real automated system. The kit includes the attack generator and the firewall protection components.

Educational activities:
- Principles of cybersecurity,
- Implementation of a LAN and connection of the elements of a digital information chain,
- Implementation of a cyberattack scenario,
- Analysis of digital frames before and after an attack,
- Firewall programming.

Main sectors concerned:
- Digital systems (Bac, BTS and BUT)
- Industrial maintenance (improvement of an asset),

Rev. D – May 21, 2024

ASTRIANE

1884 Saint Maurice Avenue
04100 MANOSQUE
FRANCE

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

Safeticc

Experimental kit and kit to integrate for concrete learning about cybersecurity

In view of the attacks that target all economic fields of industrial societies, the protection of digital data has become a priority area for improvement in many companies. The deployment of firewalls extends to workshops where machines often remain a weak link in digital security. Our range, with several production lines, lends itself particularly well to the implementation of a digital protection solution.

Equipment presentation

The **SAFETICC** equipment is available in 2 solutions:
- an experimental kit designed to understand an industrial "firewall" device, its configuration and operation, - a kit that brings together all the technical elements required to implement the industrial "firewall" on the existing equipment in the range.
Both solutions include an attack generator that ensures faults by DoS (Deny of Service) and causes the saturation of normal communication with incessant requests.
The "Man-in-the-Middle" technique defines a cyberattack following a phase of observation of digital exchanges. A defective code then replaces the sound code of the machines' programs.
This case is staged on systems in our range.

Functional features

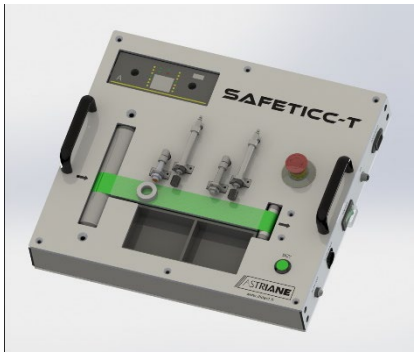
SAFETICC integrates an interface allowing to have a personalized menu for each application:
A universal mode, allows the customization of the targets (typically PLC / HMI / I/O module) and the variables to be perturbed. "SAVONICC" and "RECYCLICC" modes, with the line automatons preconfigured, as well as the instructions that may be disturbed (temperature setpoints, cutting setpoints, etc.)

Associated systems

The ASTRIANE range offers several systems that are compatible with the cybersecurity scenario. This is the case of the SAVONICC and RECYCLICC production lines.

A simpler application is also available. It is implementing a motorized belt conveyor for the sorting of parts whose operation is jeopardized by the cyberattack. This PO includes a set of sensors and a conveyor belt speed drive.

Illustration of the PO 100% electric sorting conveyor



Educational exploitation

- Setting up the LAN: use of Machine Expert, configuration of the HMI and configuration of remote peripherals.
- Ethernet frame analysis with Wireshark,
- DoS attacks and effects on the automated system,
- Frame analysis during a DoS attack: principle of denial of service,
- Disturbance attack or exit forcing: effects on the system,
- Setting up the firewall and checking the operation against different types of attacks,- Analysis of the frames upstream and downstream of the firewall during a DoS attack.
- ''Man in the middle'' application (advanced level):

a) "Spy" mode with monitoring of the frames exchanged between 2 devices.
b) Output of an actionable log on Wireshark to identify frames of interest for an attack.
c) Switching from the ''Man in the middle'' application to ''Spy'' mode to ''Modifying'' the identified frames.

- Firewall rule settings (advanced level).

General characteristics

Experimental case:
- LxWxH = 400x500x300 mm
- Weight: 18 kg- Energies: 230V - 50Hz
- P consumed = max 500W

Operational part:
- LxWxH = 500x450x135 mm
- Mass: 9 kg
- Electrical energies: 230V-50Hz
- P consumed: 100 W

ASTRIANE

1884 Saint Maurice Avenue
04100 MANOSQUE
FRANCE

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