CLEARSY

Safety Solutions Designer

April 2023

AIX
LYON
PARIS
STRASBOURG

WWW.CLEARSY.COM

Cybersecurity Offer
Custom Protection

CONTACT@CLEARSY.COM

Positioning

- CLEARSY, designer of secure programmed systems, offers a range of services and products in the field of computer security
- This offer responds to specific cybersecurity issues encountered in Operationnal Technology (OT)
- It covers all the sectors of activity addressed by CLEARSY (railway, nuclear, defense, automotive, medical, industry, etc.)

Cybersecurity Products and Services

- Risk analysis - Prescription of requirements
  - On a system architecture
  - On software
- Critical analysis of an existing system - Detection of vulnerabilities
  - On a system architecture
  - On software
- Formal security modelling (policy and behaviour)
  - Building evidence for EAL6+ and EAL7 certification
- Implementation of protection for an industrial system
  - Custom software development
  - Development of a programmed hardware protection barrier (Cyber Gateway)
  - Integration with existing software and systems
- Development of vulnerability testing equipment

Standards – Approach

ISO 27001, IEC 62443, IEC 62645, ANSSI (LPM, EBIOS-RM), Common Criteria

References (1/4)

Cyber protection of a fire safety supervision system installed at a Vital Operator

Customers : Société du Grand Paris, ALSTOM, THALES

These activities are part of a turnkey system developed by CLEARSY for the supervision of fire equipment in Paris and Grand Paris metro stations.

The operator is identified as an Operator of Vital Importance (OIV).

Implementation of cyber protection functionalities: encryption of connections, use of VLANs, account by AD, monitoring and logging of operation and connection anomalies.

Production of the cybersecurity demonstration file, addressing the development process and the analysis of the technical devices implemented: mapping, risk analysis (EBIOS RM), traceability of contractual and normative requirements in accordance with the standards relating to the Military Planning Law (LPM).

References (2/4)

Development of a safe and cyber-secure computer board

Customer : bpifrance POLE SCS Project CASES

Development of a computer board, integrating a cyber gateway allowing both the control and the remote update of a safe computing node.

The platform aims to offer a cybersecurity level of EAL5+ (Common Criteria standard) and is based on the use of a formally proven microkernel (Proven Core from PROVENRUN).

The safety level of the computer is SIL4 according to the IEC 61508, EN50126, 128, and 129 standards.

Gateway Honeywell - Digisafe

Customer : SIEMENS

Realization of a communication gateway on a computer (Moxa) between two protocols in order to be able to safely collect remote data from a Honeywell equipment in the Budapest metro.

References (3/4)

Implementation of a test bench to qualify the robustness of classified links with regard to a denial of service

Customer : EDF

Realization of a controlled simulation of denial of service on a PLC link. Measurement of the behaviour of the PLC and its program following this request. This work is part of a C3 qualification campaign for several industrial programmable controllers (Schneider, Siemens, Hima) for nuclear power plants (CNPE).

Formal modelling of the safety policy and behaviour of electronic components

Customers : Atmel IDEMIA STMicroelectronics

Realization of the security policy formal models for the Common Criteria certification up to EAL6+ level, for microcircuit type components. Support for the presentation of the deliverables to the certification bodies (CESTI/ANSSI, TÜV).

References (4/4)

Cyber-security of a critical input/output controller for a metro

Customer : THALES

The project consists in the implementation of an SNMPv3 server (remote monitoring and diagnosis) including authentication (MD5) and encryption (AES256) in a distributed I/O management equipment.

Protection of a control system for metro platform doors for ST Engineering

Customer : ST Engineering

The project consists in securing a remote maintenance protocol for a platform management equipment, authentication of the application by login and password, authentication of the UDP link by HMAC-SHA1.