CLEARSY

Safety Solutions Designer

Avril 2023

AIX
LYON
PARIS
STRASBOURG

WWW.CLEARSY.COM

Offre Cyber
Custom Protection

CONTACT@CLEARSY.COM

Positionnement

- CLEARSY, concepteur de systèmes programmés sûrs propose une offre de services et de produits dans le domaine de la sécurité informatique
- Cette offre répond à des problématiques de cybersécurité spécifiques rencontrées en informatique industrielle
- Elle couvre l'ensemble des secteurs d'activité adressés par CLEARSY (ferroviaire, nucléaire, défense, automobile, médical, industrie…)

Offre Cyber CLEARSY

- Analyse de risques – Prescription des exigences
  - Sur une architecture système
  - Sur un logiciel
- Analyse critique d'un existant – Détection de vulnérabilités
  - Sur une architecture système
  - Sur un logiciel
- Modélisation formelle de sécurité (politique et comportement)
  - Constitution d'éléments de preuve pour une certification EAL6+ et EAL7
- Réalisation de protection pour un système industriel
  - Développement de logiciel sur mesure
  - Développement de barrière de protection matérielle programmée (Gateway Cyber)
  - Intégration au sein de logiciels et systèmes existants
- Développement d'équipement de test de vulnérabilité

Normes - Démarche

ISO 27001, IEC 62443, IEC 62645, ANSSI (LPM, EBIOS-RM), Critères Communs

Références (1/4)

Protection cyber d'un système de supervision incendie sécuritaire installé chez un Opérateur d'Importance Vitale

Clients : Société du Grand Paris, ALSTOM, THALES

Ces activités s'inscrivent dans le cadre d'un système clés en main développé par CLEARSY pour la supervision des équipements incendie des stations de métro de Paris et du Grand Paris.

L'exploitant est identifié en tant qu'Opérateur d'Importance Vitale (OIV).

Mise en œuvre de fonctionnalités de protection cyber : chiffrement des connexions, utilisation de VLAN, de compte par AD, surveillance et log du fonctionnement et des anomalies de connexion.

Réalisation du dossier de démonstration de la cybersécurité, abordant le processus de développement et l'analyse des dispositifs techniques mis en œuvre : cartographie, analyse de risque (EBIOS RM), traçabilité des exigences contractuelles et normatives selon les normes relatives à la Loi de Programmation Militaire (LPM).

Références (2/4)

Réalisation d'une carte calculateur sûr de fonctionnement et cyber sécurisé

Client : bpifrance POLE SCS Project CASES

Réalisation d'une carte calculateur, intégrant une passerelle cyber permettant à la fois le contrôle et la mise à jour à distance d'un nœud de calcul sûr de fonctionnement.

La plateforme vise à offrir une sécurisation cyber d'un niveau EAL5+ (norme Critères Communs) et repose sur l'utilisation d'un micro-noyau formellement prouvé (Proven Core de PROVENRUN).

Le niveau de sécurité du calculateur est SIL4 selon les normes 61508, EN50126, 128, et 129.

Passerelle Honeywell - Digisafe

Client : SIEMENS

Réalisation d'une passerelle de communication sur un calculateur (Moxa) entre deux protocoles afin de pouvoir collecter en sécurité des données distantes d'un équipement Honeywell dans le métro de Budapest.

Références (3/4)

Réalisation d'un banc de test pour qualifier la robustesse de liaisons classées en regard d'un déni de service

Client : EDF

Réalisation d'une simulation maitrisée de déni de service sur une liaison automate. Mesure de comportement de l'automate et de son programme suite à cette sollicitation. Ce travail s'inscrit dans le cadre d'une campagne de qualification C3 de plusieurs automates programmables industriels (Schneider, Siemens, Hima) à destination de centrales nucléaires (CNPE).

Modélisation formelle de la politique et du comportement de sécurité de composant électronique

Clients : Atmel, IDEMIA, STMicroelectronics

Réalisation des modèles formels de la politique de sécurité pour la certification Critères Communs jusqu'à un niveau EAL6+, pour des composants de type microcircuits.

Accompagnement à la soutenance des livrables auprès des acteurs de certification (CESTI/ANSSI, TÜV).

Références (4/4)

Cybersécurisation d'un contrôleur d'entrées/sorties critiques de métro

Client : THALES

Le projets consiste en la mise en place d'un serveur SNMPv3 (surveillance et diagnostic à distance) incluant authentification (MD5) et chiffrement (AES256) dans un équipement de gestion d'entrées/ sorties distribuées.

Protection d'un système de contrôle-commande de portes palières de métro

Client : ST Engineering

Le projet consiste en la sécurisation d'un protocole de maintenance à distance pour un équipement de gestion de quai, authentification de l'application par mot de passe login, authentification de la liaison UDP par HMAC-SHA1.