Université de Bretagne Sud

Recherche et Formation autour de la cybersécurité

Cybersécurité et industrie

7 juin 2018 - ETN

Lab-STICC « Communiquer et décider, des capteurs à la connaissance… »

Pr E. Martin

17 Bd Flandre Dunkerque BP 92116 – 56321 Lorient Cedex 02 97 87 40 22 ; eric.martin@univ-ubs.fr

La cyber, c'est quoi ?

Les rapports des spécialistes de la sécurité informatique

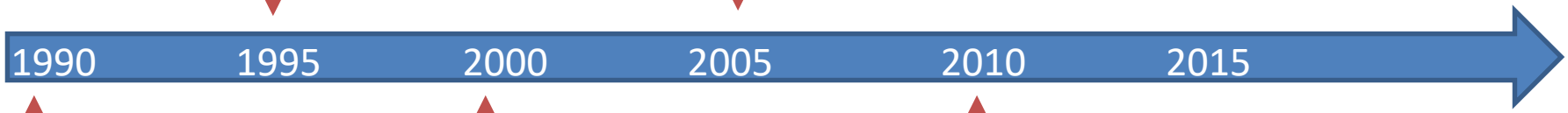
- Rapport McAfee 2018
  - 63,4 Millions de logiciels malveillants en base McAfee
    - 700 M logiciels malveillants (60 M de nouveaux)
    - 15 M logiciels de rançonnage (2 M de nouveaux)
    - 50 M de logiciels malveillants type javascript (4 M de nouveaux)
    - 10 M d'URL malveillantes
    - 350.000 URL de phishing
- F-Secure 2017 : cyberattaques recensées : 62 Millions

* 1000	GB	Fr	D	Chine	USA	Ru	Nl	Autre	Tot
GB	57	0	50	33	78	10	6	110	344
Fr	168	1	167	39	275	19	39	672	1379
D	123	0	66	973	244	51	30	269	1758
Chine	175	0	380	217	277	208	49	673	1979
USA	198	2	200	2009	564	62	116	561	3712
Ru	1015	1236	4292	209	26976	671	17224	1332	**52955**
Autres	419	12	392	62	704	80	136		
Total	2225	1259	5655	3567	35274	1142	17910		***62 M***

Menaces : Catégories d'attaques

1995 :
- outils d'intrusion des interfaces graphiques
- attaques généralisées automatisées
- attaques généralisées de déni de service
- attaques de code exécutable
- attaques généralisées d'infrastructures DNS
- attaques généralisées propagées sur NNTP protocole réseau
- technique furtive de sondage
- chevaux de Troie sur Windows

2005 :
- prise de possession massive de PC
- attaques généralisées d'applications WEB
- attaques généralisées de logiciels coté client
- hameçonnage ciblé
- **cible de systèmes de contrôle**
- infiltration de malgiciel persistant
- **compromission de chaine logistique**



1990 :
- attaques d'ingénierie sociale sur internet
- **usurpation de paquets**
- session de piratage
- sondes automatisés

Sophistication croissante

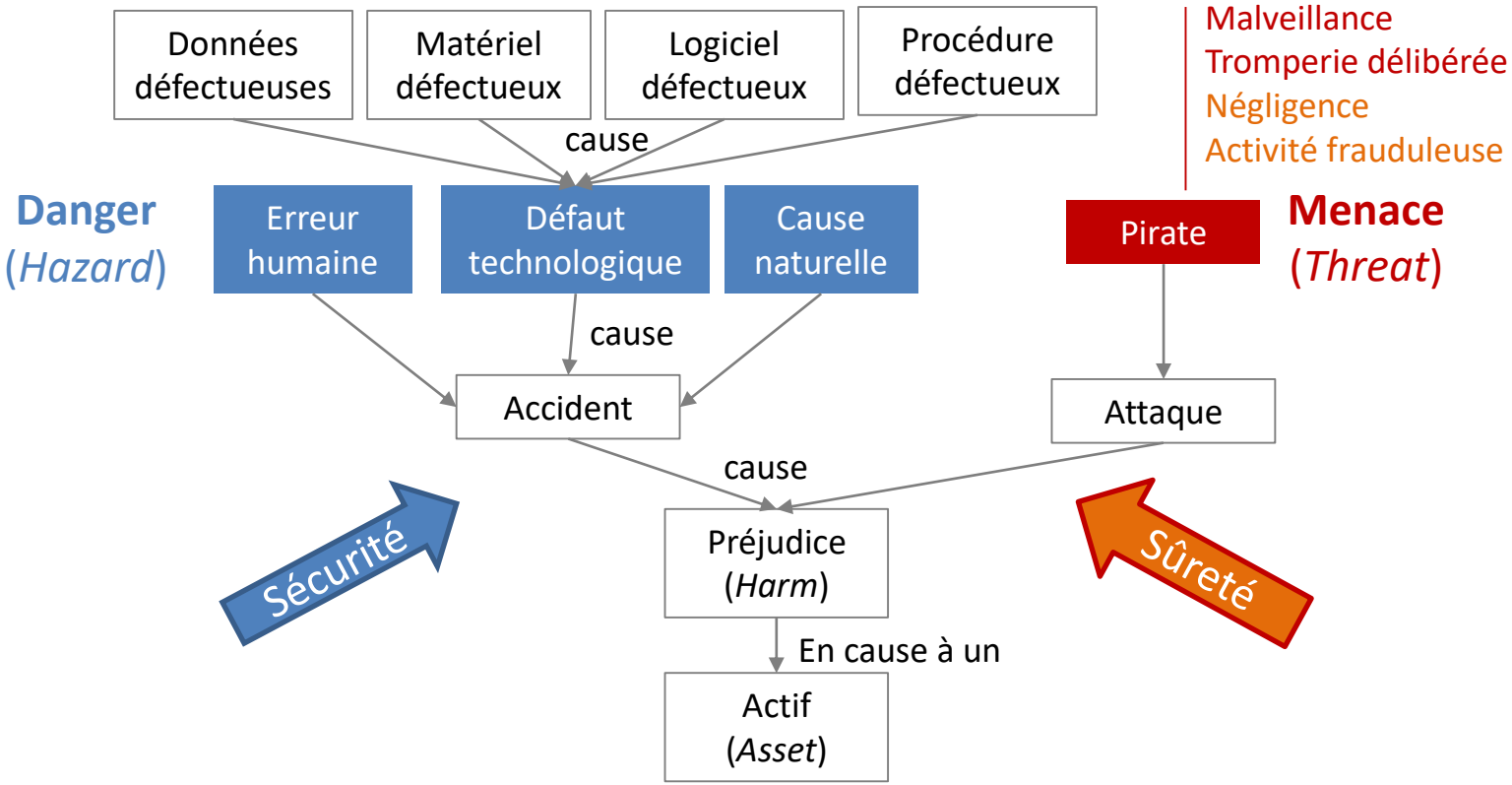
2010 :
- contrefaction malveillante de matériel
- attaques cyber physiques coordonnées
- attaque adaptative d'infrastructures critiques

2000 :
- propagation de code mal intentionné par email
- chevaux de Troie à large échelle
- outils pour attaques distribuées
- attaque par DDoS
- propagation de vers
- commandes et contrôles sophistiqués

97 87 40 22 ; eric.martin@univ-ubs.fr

Dualité SSI - Cybersécurité

- Positionnement SSI et cybersécurité (projet de norme ISO34001)



Pr E. Martin
17 Bd Flandre Dunkerque BP 92116 – 56321 Lorient Cedex 02 97 87 40 22 ; eric.martin@univ-ubs.fr

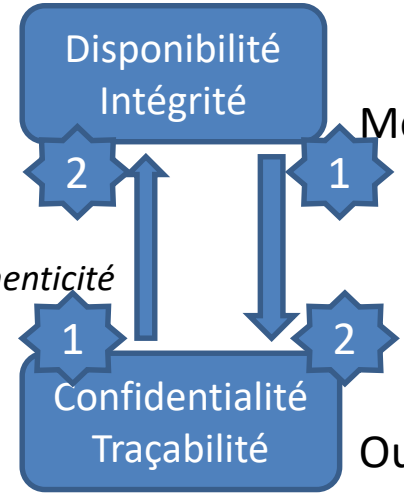
Dualité Cybersécurité – Sûreté de fonctionnement

- Cybersécurité / SSI

Mesures

- Disponibilité
- Intégrité
- Confidentialité

Imputabilité / Traçabilité , Authenticité /Non répudiation



Outils

- Management du risque
  - Approche qualitative : indicateurs, retour d'expérience, experts…
- Niveaux de sûreté
  - *Sécurity Level **SL0 à SL4***

IEC 62443-3-3

- Sûreté de fonctionnement / sûreté fonctionnelle

Mesures

- Fiabilité
- Disponibilité
- Maintenabilité
- Sécurité *intégrité physique des personnes*

Outils

- Management du risque
  - Approche quantitative

MTFB (tps moyen avant défaillance)

MTTR (durée moyenne de réparation)

TDM = MTBF / (MTBF + MTTR)

- Niveaux de fiabilité
  - *Safety integrity level **SIL0 à SIL4***

IEC 61508-1

Pr E. Martin
17 Bd Flandre Dunkerque BP 92116 – 56321 Lorient Cedex 02 97 87 40 22 ; eric.martin@univ-ubs.fr

PÔLE D'EXCELLENCE CYBER

Bretagne : pôle d'excellence en cyber

Alliance Allistene

PEC : 8% de la recherche académique en France

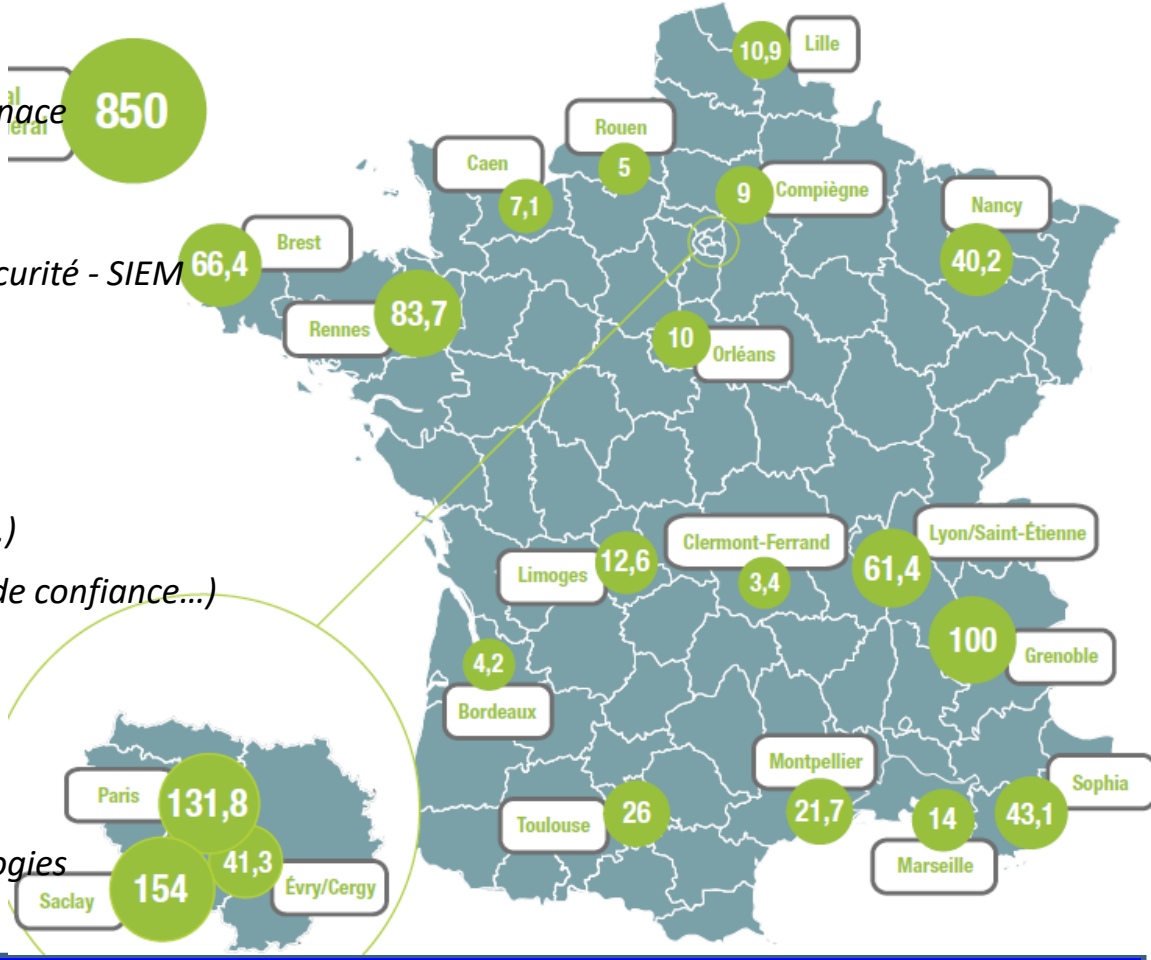
- Technologies et services

Cybersécurité

Cyberdéfense
- *Connaissance de la menace*
- *Analyses et évaluations*
- *Administration de la sécurité - SIEM*

Cyberprotection
- *Modélisations*
- *Produits (pare feu…)*
- *Technologies (info. de confiance…)*
- *Conception*
- *Test - évaluation*

Cyberrésilience
- *Méthodes*
- *Produits & technologies*
- *Services*



17 Bd Flandre Dunkerque BP 92116 – 56321 Lorient Cedex 02 97 87 40 22 ; eric.martin@univ-ubs.fr

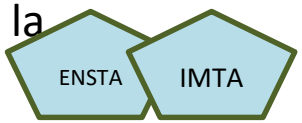
PÔLE D'EXCELLENCE CYBER

Bretagne : pôle d'excellence en cyber

- Recherches *(CPER 2015 – 2020)*

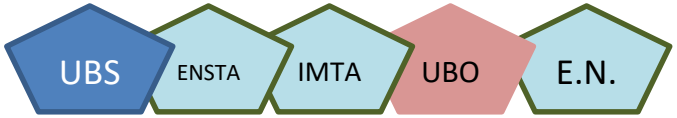
Cyber Crypto : Conception de composants matériels sûrs, implémentation matérielle et logicielle de primitives cryptographiques asymétriques

Cyber Algo : Conception d'algorithmes et de dispositifs pour l'investigation et la confidentialité (traçabilité, confidentialité, recherche de contenus cachés…)



Cyber Ubiquitous : Méthodes d'analyse de la sécurité des systèmes ubiquitaires (systèmes embarqués)

Cyber ICS (Industrial Control Systems) : Cybersécurité pour les systèmes industriels



Cyber Elec : Simulation de la détection de défaillances des systèmes physiques face aux attaques de sécurité

17 Bd Flandre Dunkerque BP 92116 – 56321 Lorient Cedex 02 97 87 40 22 ; eric.martin@univ-ubs.fr

Lab-STICC : Du capteur à la connaissance

Recherche

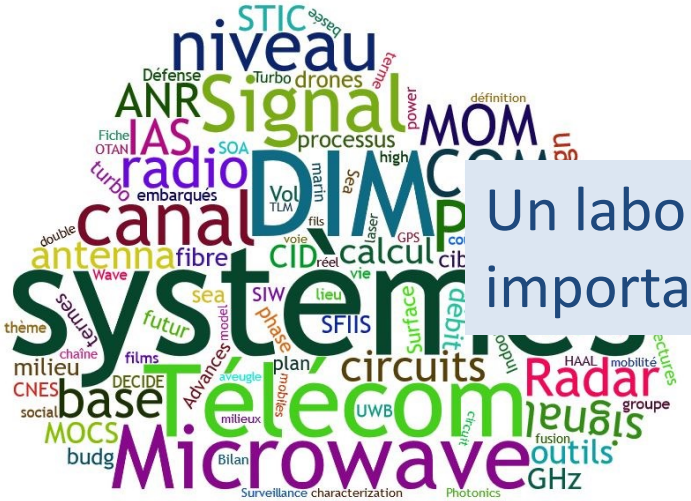
UMR 560 Membres

3 Pôles

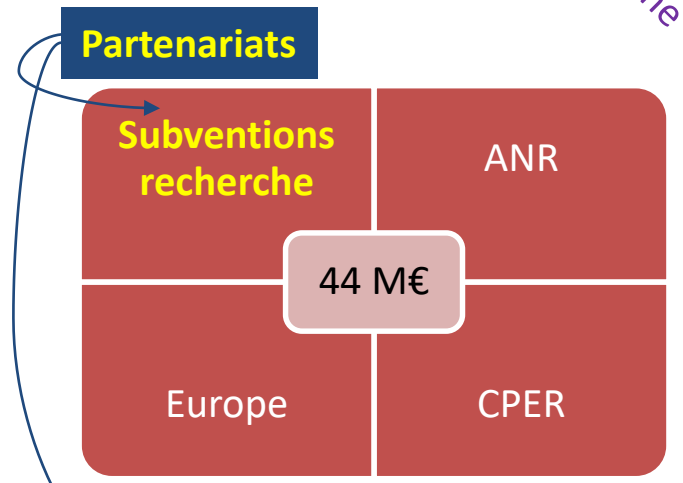
CID : Connaissance, Information, Décision

CACS : Communications, Architectures, Circuits et Systèmes

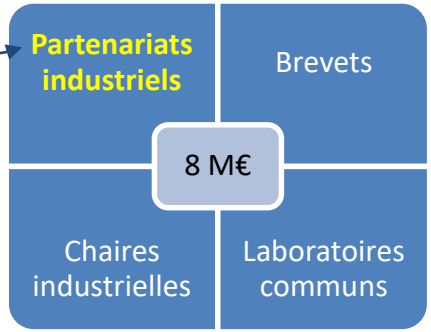
MOM : Microondes, Optoélectronique et Matériaux



Un laboratoire ayant l'un des plus importantes activités partenariales



2010-2015, hors salaires état



Plateforme

Lab-STICC-SCAP

Industrie du Futur

Digital Manufacturing

Digital Factory

Chaires industrielles

Chaire cyber naval

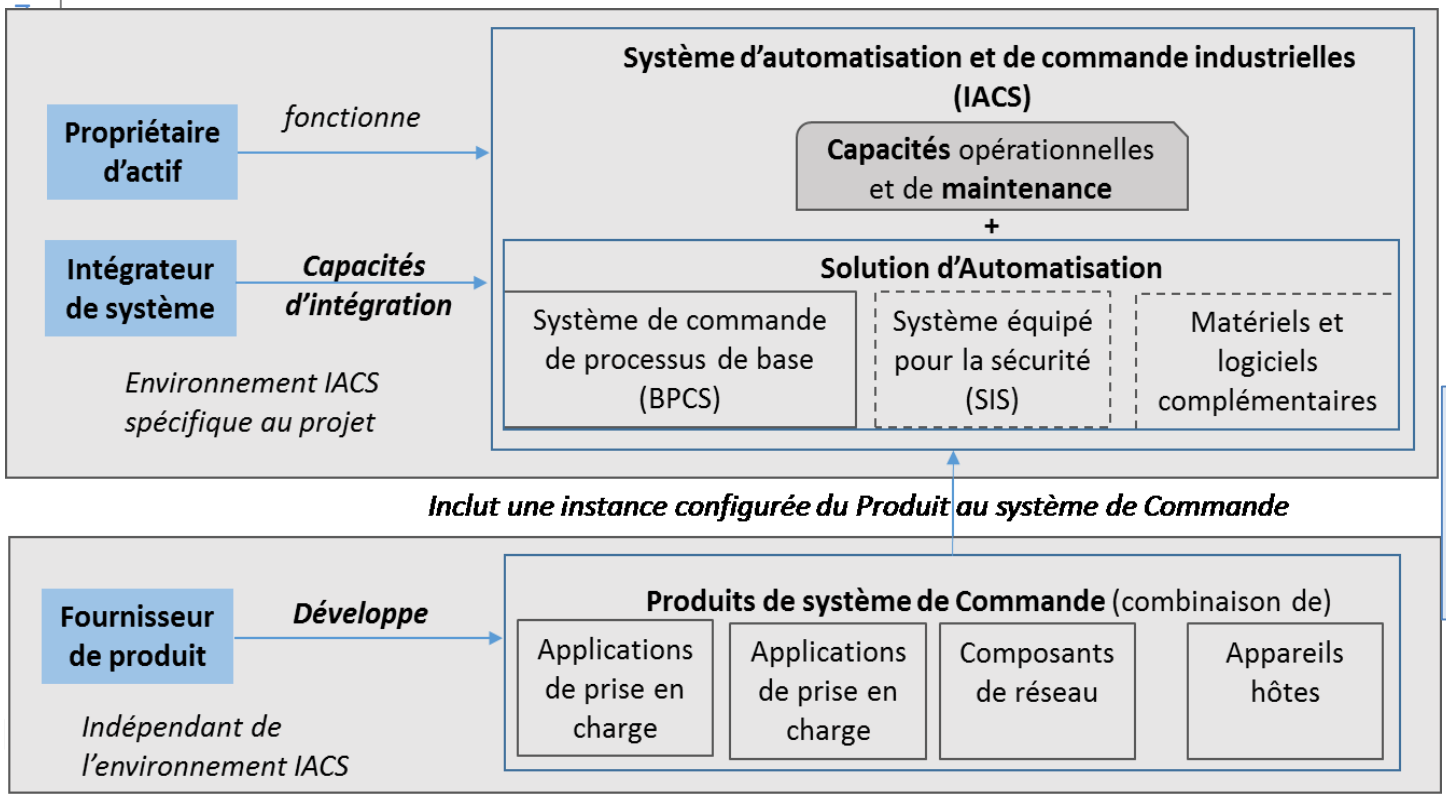
En projet :

Chaire jumeau numérique

Chaire cybersécurité

Cybersécurité industrielle

- les IACS Systèmes d'automation et de commande industrielles
  - Le cadre des systèmes d'automation et de commande industrielle



Sécurité fonctionnelle

Danger (accidentel)
E->S Robustesse
S->S Fiabilité
S->E Résilience

E : externe
S : système

Menace (Malveillance)
E->S Résistance
S->S Intégrité
S->E Confinement

Cybersécurité

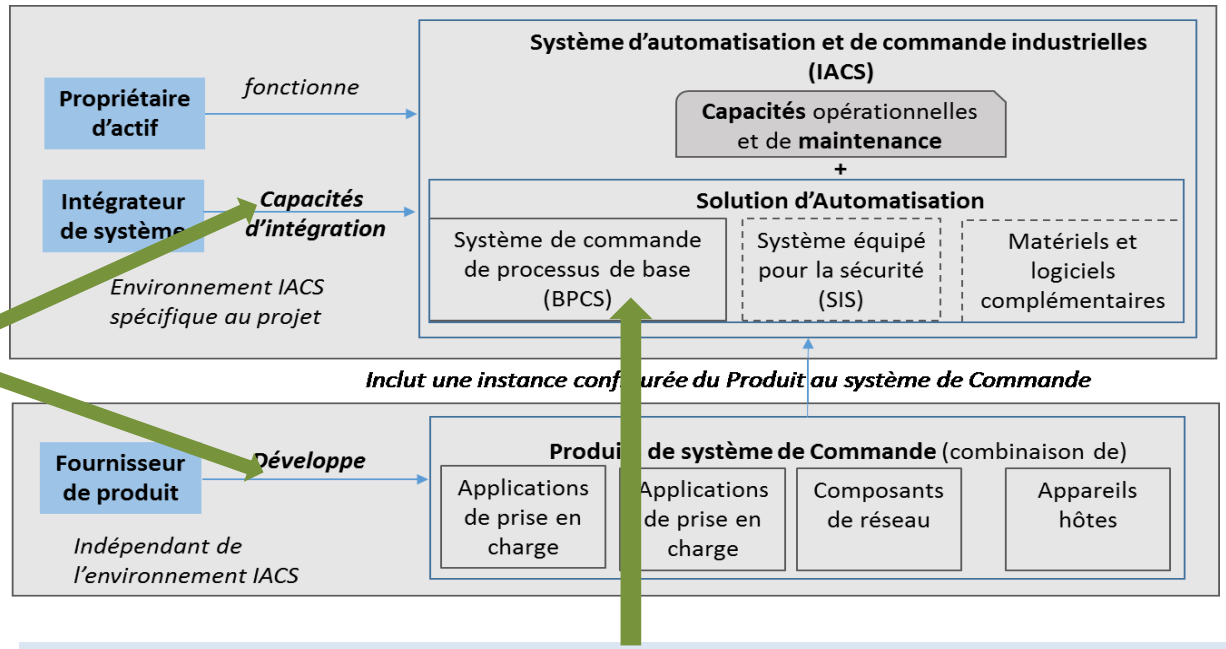
Cybersécurité industrielle

- La détection d'intrusion dans les IACS
  - Le cadre des systèmes d'automation et de commande industrielle

Nx de management de sécurité

- Affectation en personnel pour la solution
- Assurance
- Architecture
- Sans fil
- SIS
- Gestion de la reconfiguration
- Accès distant
- Gestion des évènements
- Gestion des comptes
- Protection contre les logiciels malveillants
- Gestion des correctifs
- Sauvegarde /restauration

62443 : Niveaux de protection



Niveaux de sécurité SL

a) Contrôle d'identification et d'authentification (**IAC**) b) Contrôle d'utilisation (**UC**),
c) Intégrité du système (**SI**), d) Confidentialité des données (**DC**),
e) Transfert de données limité (**RDF**), f) Réponse appropriée aux événements (**TRE**),
g) Disponibilité des ressources (**RA**).

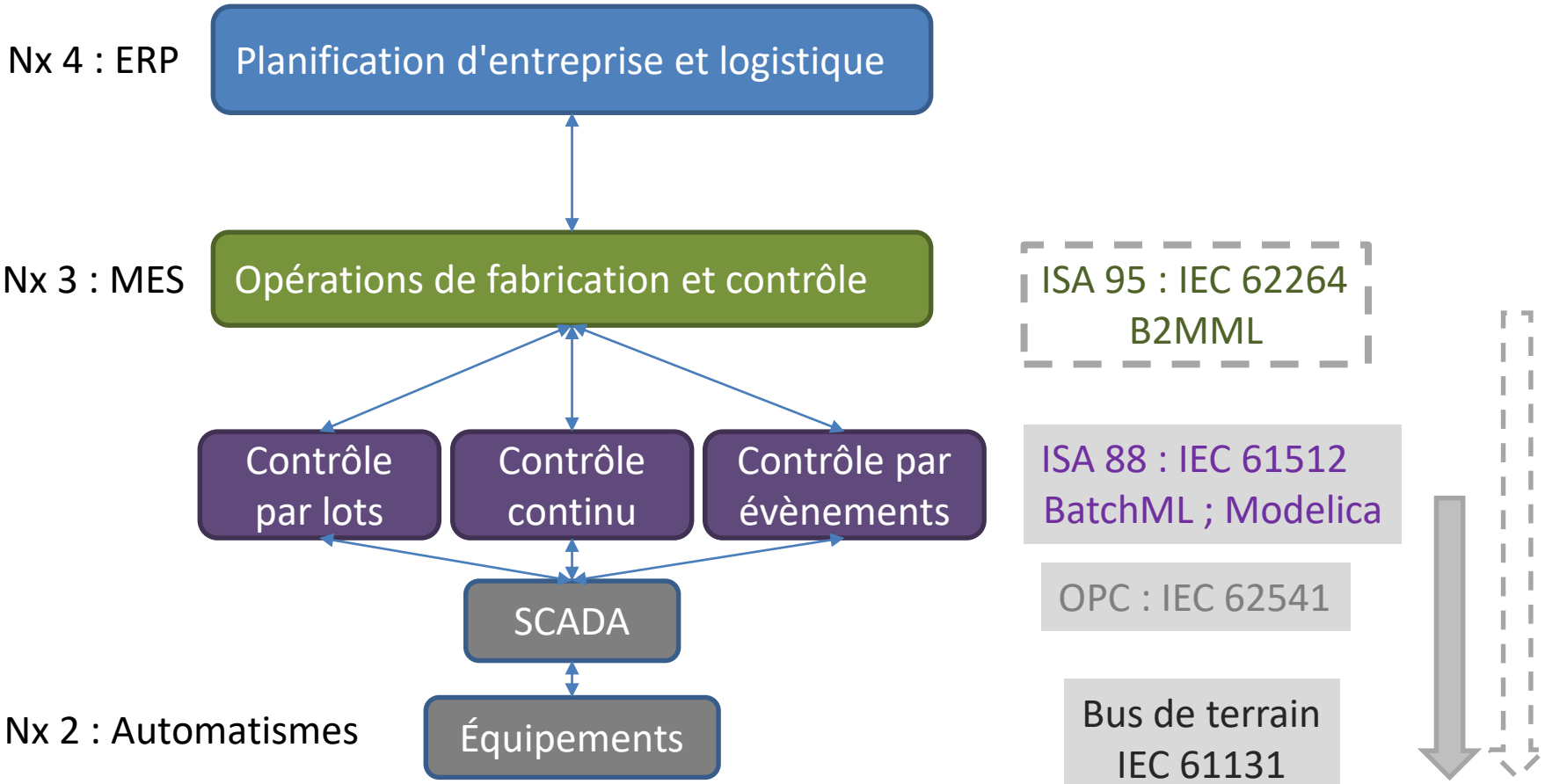
Cybersécurité industrielle - IDS

- Recommandations
  - IEC 62443-4-2 : Exigences de sécurité technique des composants IACS
    - CR 3.3 – Vérification de la fonctionnalité de sécurité
    - CR 6.2 – Surveillance continue
  - NIST 800-82 : Guide to Industrial Control Systems (ICS) Security
    - 6.2.17.2 Intrusion Detection and Prevention
    - Déploiement efficace de l'IDS :
      - NIDS : Entre le réseau de contrôle et le réseau d'entreprise conjointement avec un pare-feu ;
      - HIDS : Sur les ordinateurs (OS), des applications telles que les IHM, les serveurs SCADA et les stations de travail d'ingénierie.
      - La surveillance de la sécurité du réseau et la **compréhension de l'état normal du réseau ICS** peuvent aider à distinguer les attaques des conditions transitoires, et à la fois déclencher et fournir des informations dans des événements qui sont en dehors de l'état normal.
  - NIST 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)
    - Performances : Configuration (par défaut ou avancée) ; Complexe et robuste ou sobre en calcul et mémoire ; Généraliste ou basé sur le matériel ; Conditions de test de performance.

17 Bd Flandre Dunkerque BP 92116 – 56321 Lorient Cedex 02 97 87 40 22 ; eric.martin@univ-ubs.fr

Modélisation des IACS & IDS

- Les modèles en vigueur

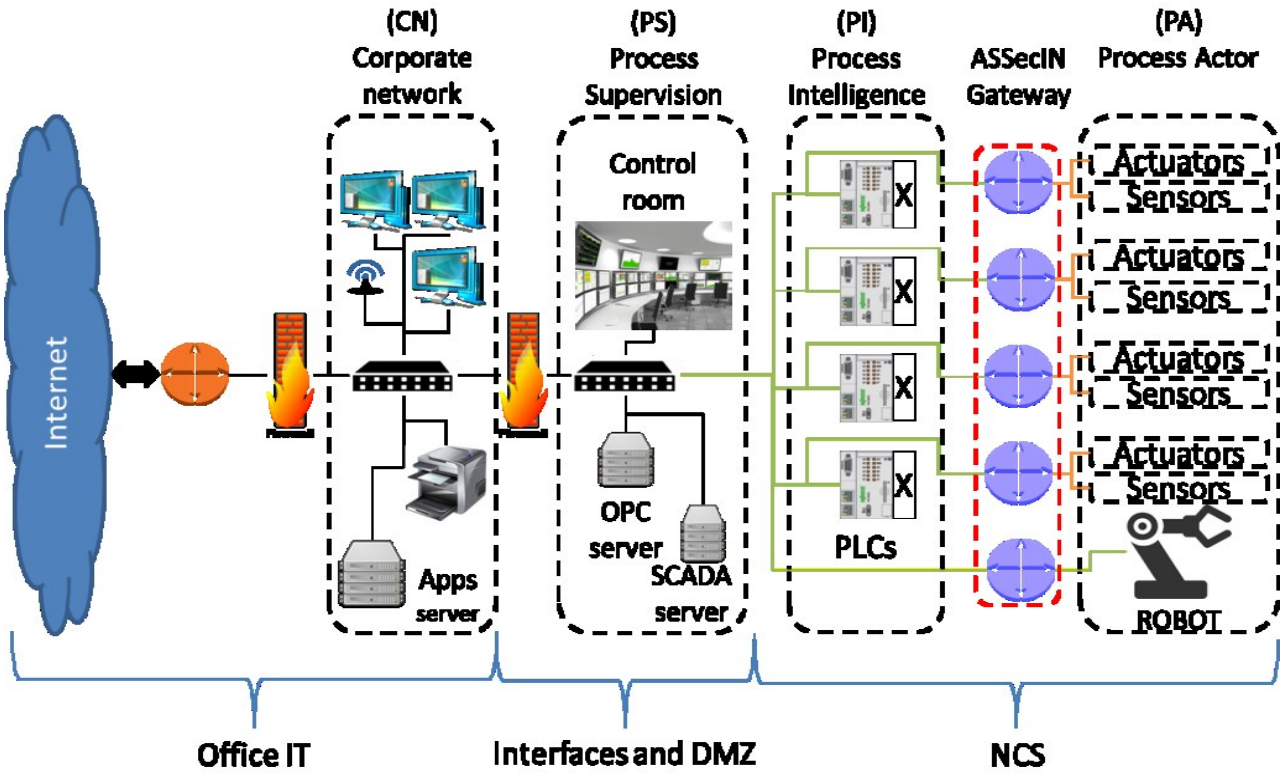


17 Bd Flandre Dunkerque BP 92116 – 56321 Lorient Cedex 02 97 87 40 22 ; eric.martin@univ-ubs.fr

Th : Sécurisation matérielle de capteurs/actionneurs distribués sur des réseaux industriels

Recherche

- ## Principe
  - Observation des variables du système sur le réseau de terrain
- ## Solution
  - Une passerelle sur le réseau de terrain transmet l'information tout en l'interprétant.
  - Elle intègre des principes de détection et des mécanisme de réaction.



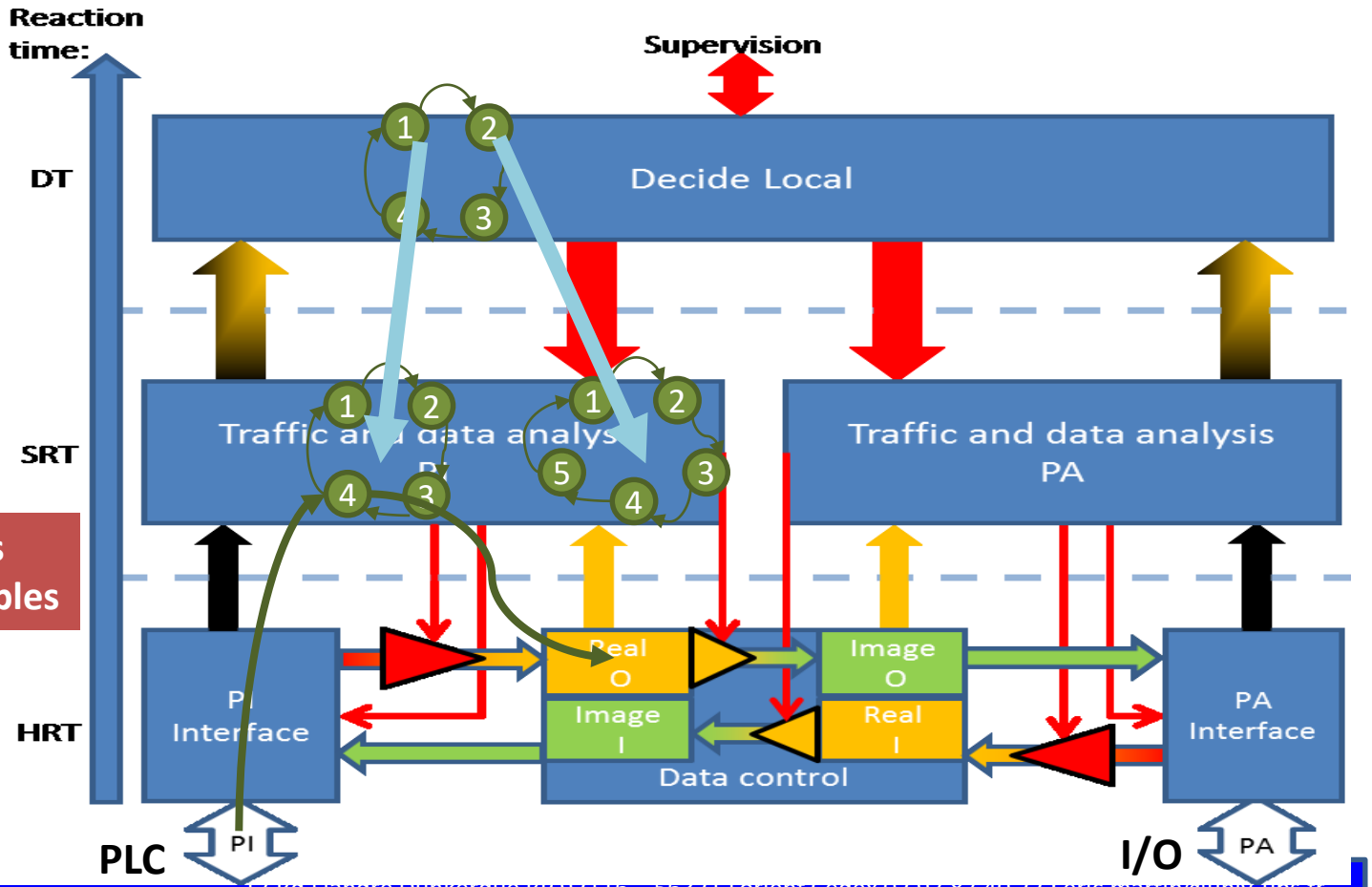
17 Bd Flandre Dunkerque BP 92116 – 56321 Lorient Cedex 02 97 87 40 22 ; eric.martin@univ-ubs.fr

Th : Sécurisation matérielle de capteurs/actionneurs distribués sur des réseaux industriels

- Passerelle à 2 niveaux de modèles

Modèle : Machine à états des configurations

Modèle : L/E des variables
Machine à états des variables



17 Bd Flandre Dunkerque BP 92116 – 56321 Lorient Cedex 02 97 87 40 22 ; eric.martin@univ-ubs.fr

Th : Sécurisation matérielle de capteurs/actionneurs distribués sur des réseaux industriels

Recherche

Simulateur de Partie Opérative

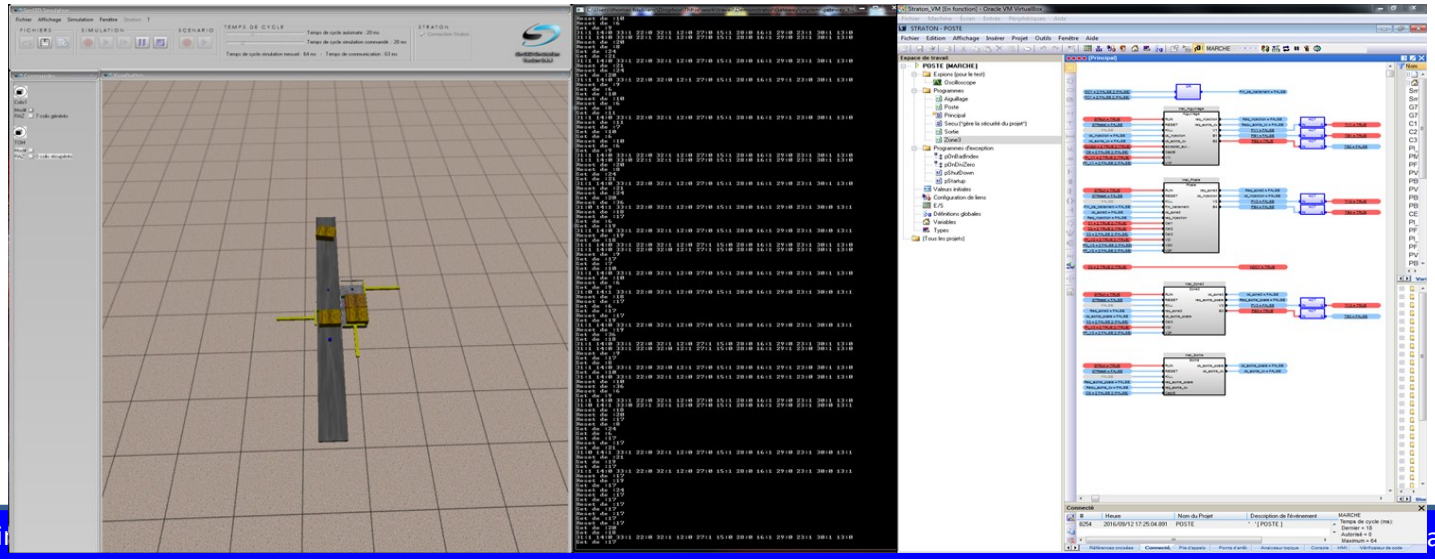
- simule le comportement physique du système
- agit comme un client
- Approche composant

Passerelle

- 3 parties majeures :
  - communication
  - détection
  - réaction
- Le but est de tester :
  - Principes de détection
  - Mécanismes de réaction

Emulateur de Partie Commande

- un runtime émule l'automate
- agit comme un serveur



artin@univ-ubs.fr

Lab-STICC

Th : Cybersécurité des équipements connectés industriels: Modélisation, détection et performances temporelles en présence d'intrusions des systèmes cyber-physiques de l'usine du futur

Recherche

« … et décider, des capteurs à la connaissance… »

Process segment | Product def. | Production Capa | Production Schedul | Production Perform | KPI

Physical assest | Operation def. | Operation Capa | Operation Schedul | Operation Perform

Equipment

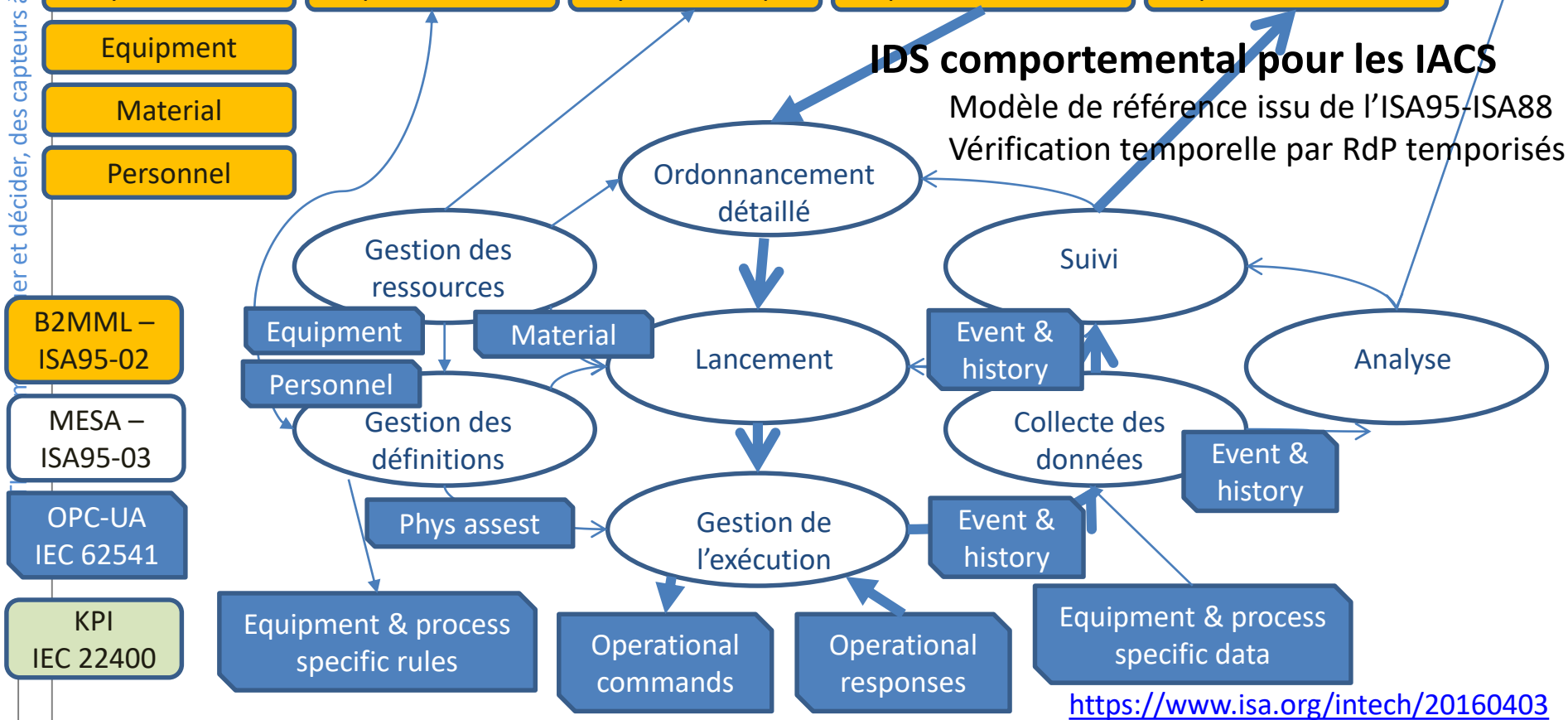
Material

Personnel

IDS comportemental pour les IACS

Modèle de référence issu de l'ISA95-ISA88

Vérification temporelle par RdP temporisés



B2MML – ISA95-02

MESA – ISA95-03

OPC-UA IEC 62541

KPI IEC 22400

https://www.isa.org/intech/20160403

Pr E. Martin

17 Bd Flandre Dunkerque BP 92116 – 56321 Lorient Cedex 02 97 87 40 22 ; eric.martin@univ-ubs.fr

SCAP industrie du futur

- Formation
  - Cybersécurité industrielle
- Prestation de service
  - Hygiène numérique

  Êtes vous cybervulnérable ?
  https://usinedufuturblog.wordpress.com/2018/01/24/etes-vous-cyber-vulnerable/
- Recherche
  - Détection d'intrusion en systèmes industriels

17 Bd Flandre Dunkerque BP 92116 – 56321 Lorient Cedex 02 97 87 40 22 ; eric.martin@univ-ubs.fr

ENSIBS

- École d'ingénieurs
  - 330 étudiants
  - 4 spécialités
    - Cyberdéfense : *Former des ingénieurs capables de cyberdéfendre les Opérateurs d'Importance Vitale français*
    - Génie industriel : *Former des ingénieurs à la maîtrise des organisations et la maitrise de la complexité industrielle en intégrant le management du risque et une forte composante digitale.*
    - Informatique de confiance : *Former des ingénieurs en cybersécurité du logiciel*.
    - Mécatronique : *Former des ingénieurs à la conception systèmes en intégrant l'électronique, la mécanique et l'informatique*

ENSIBS

- La place de la cybersécurité
  - Cyberdéfense : *Aspects humains (cyber ethique ; cyber droit ; cyber crise) ; Aspects techniques (Internet et télécommunication ; électromagnétisme et électronique ; Systèmes d'information ; IoT ; mathématiques du numérique)*
  - Génie industriel : *Management de la cybersécurité des installations industrielles IACS.*
  - Informatique de confiance : *Analyser, spécifier, concevoir et déployer les besoins fonctionnels et extra fonctionnel des systèmes logiciels*.

Merci de votre attention

- Document :

https://usinedufuturblog.wordpress.com/