NAVAL GROUP

POWER AT SEA

SYSTÈME DE DÉTECTION D'INTRUSIONS POUR LE BUS DE TERRAIN CAN, AVEC ZEEK

BarbHack 2021

28/08/2021

Inria LIG Grenoble INP UGA

1. PRÉSENTATION

Estelle HOTELLIER	Thèse CIFRE
Naval Group, NCL– INRIA, LIG, Grenoble-INP, UGA	SUJET : Détection d'anomalies par modélisation comportementale dans les systèmes cyber-physiques

ENCADRANTS :

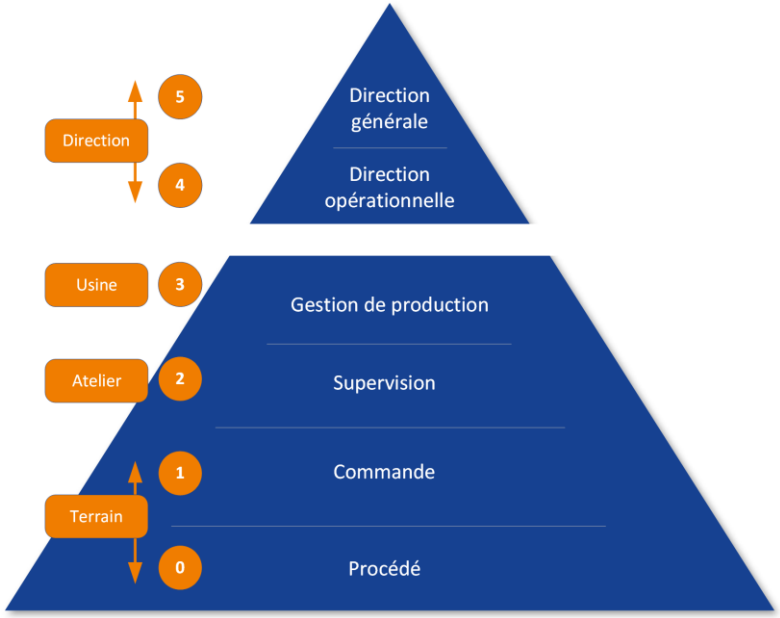
Franck SICARD	Naval Group, NCL
Julien FRANCQ	Naval Group, NCL
Stéphane MOCANU	INRIA, LIG, Grenoble-INP, UGA

SOMMAIRE

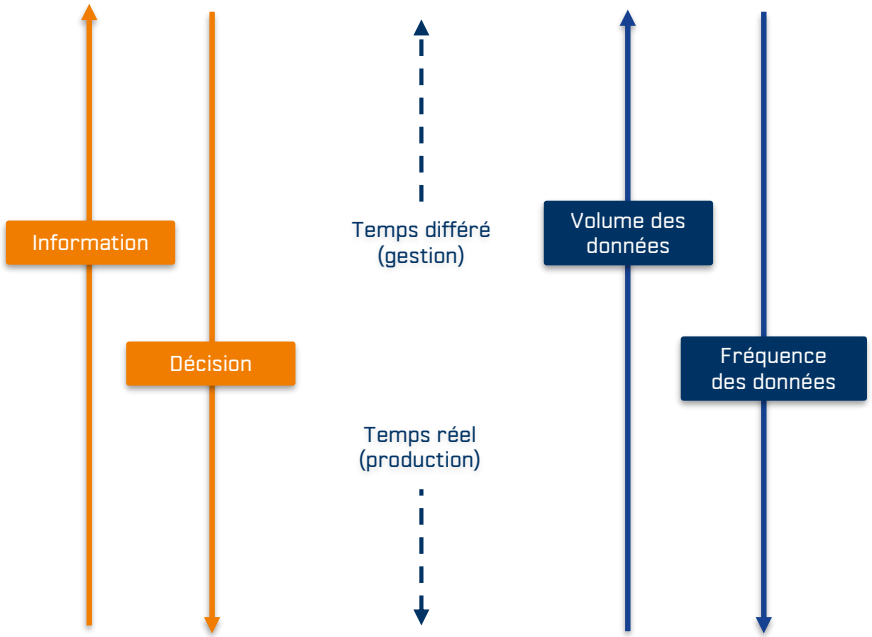
1. Les systèmes de contrôle commande industriels
2. Les bus de terrain
3. Le réseau CAN / protocole CANOpen
4. Exemples d'attaques sur le bus CAN
5. Analyse des résultats
6. Synthèse et perspectives

2. LES SYSTÈMES DE CONTRÔLE COMMANDE INDUSTRIELS

Système de Contrôle Commande Industriel (ICS) : « Réseau d'éléments physiques et numériques qui permet d'assurer l'exécution d'une tâche en milieu industriel. » [NIST 800-820rev2]

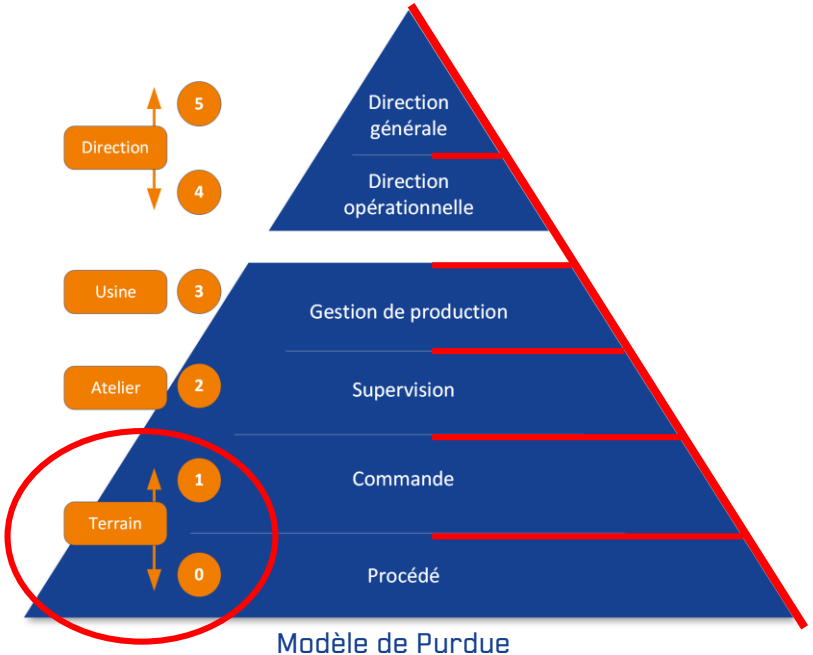


Modèle de Purdue



2. LES SYSTÈMES DE CONTRÔLE COMMANDE INDUSTRIELS

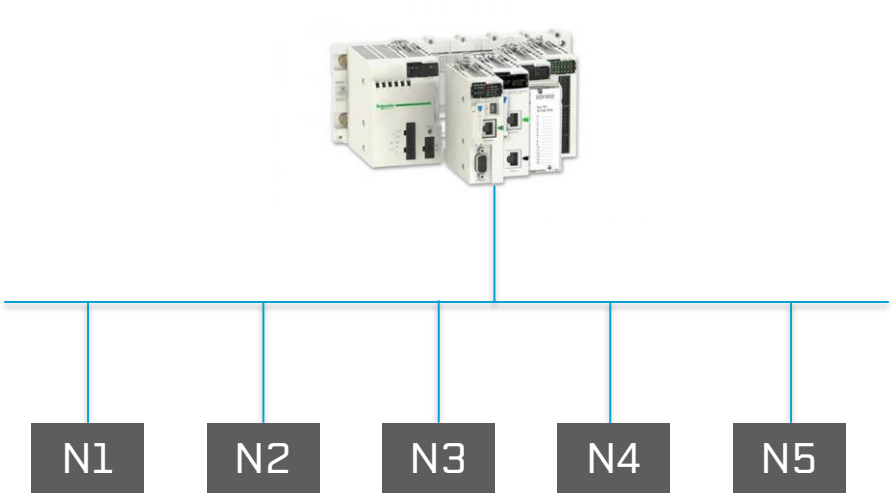
Système de Contrôle Commande Industriel (ICS) : « Réseau d'éléments physiques et numériques qui permet d'assurer l'exécution d'une tâche en milieu industriel. » [NIST 800-820rev2]



Modèle de Purdue

Surface d'attaque

3. LES BUS DE TERRAIN



Nx Nœud x

- Equipements connectés sur un support de communication unique
- Economie de câblage, diagnostic simplifié, moins de vulnérabilités, plus de flexibilité
- Architecture de communication simplifiée : couches 1, 2 (et parfois 7) du modèle OSI
- Exemples de bus terrain : Profibus, Modbus, CAN, etc.

4. LE RÉSEAU CAN / PROTOCOLE CANOPEN

Caractéristiques

- Diffusion générale
- Pas d'identification d'adresses
- Identification des variables

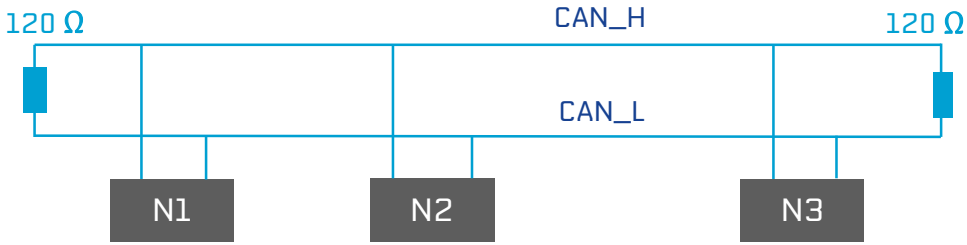
Modèle OSI

- Le bus CAN : couches 1 et 2 OSI
- Un protocole supplémentaire peut être implémenté pour la couche 7 (CANOpen par exemple)

4. LE RÉSEAU CAN / PROTOCOLE CANOPEN

Couche physique

- Câble : 2 fils blindés/non blindés
- Résistance de terminaison sur le bus
- Nombre max de nœuds <120
- Débit de 20kb/s à 1Mb/s suivant la longueur du réseau



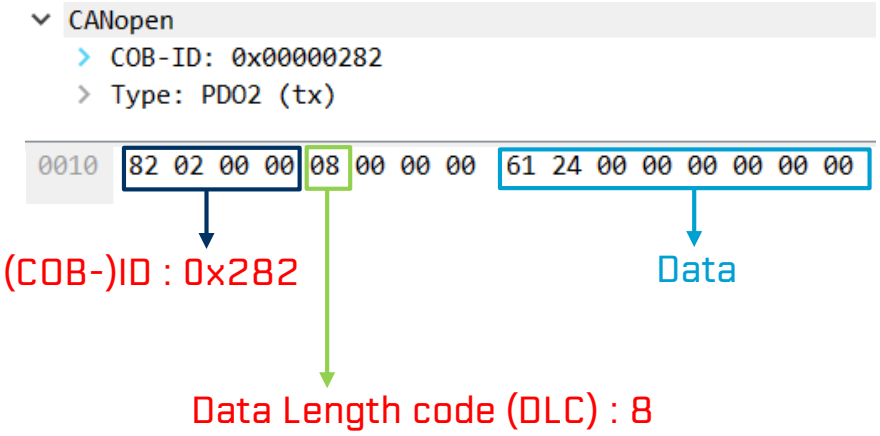
Couche liaison

- Communication multimaître
- Accès par priorité (selon l'identificateur de trame)
- Accès CSMA/CR (Carrier Sense Multiple Access / Collision Resolution), arbitrage non destructif

4. LE RÉSEAU CAN / PROTOCOLE CANOPEN

Trame de donnée

- SOF : 1 bit à 0
- (COB-)ID : 11/29 bits identification et priorité
- RTR : Remote Transmission Request (1 bit)
- Ctrl : 6 bits (2 réservés + 4 DLC)
- Data : 0 à 8 octets
- CRC/Ack : 16 bits CRC + 2 bits Ack
- EOF : 7 bits=0x7F (tous les bits à 1)



4. LE RÉSEAU CAN / PROTOCOLE CANOPEN

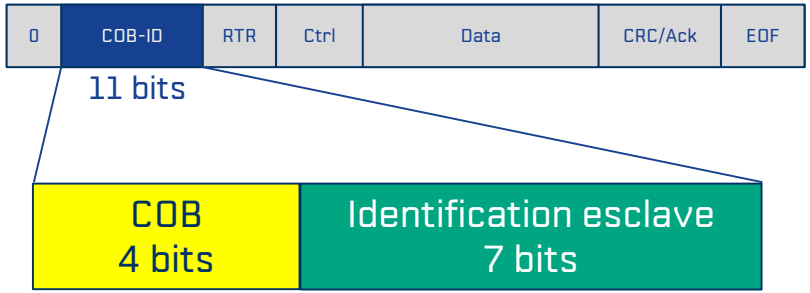
Couche application

Dictionnaire d'objets :

- Liste de tous les modèles de données utilisés par le bus
- Objet = variable indiquée par un nombre

Transmission des données :

- Accès aux données du dictionnaire : COB (Communication Object)
- Code de fonction (type de message) : 16 niveaux de priorité (4 bits)
- Avec priorités + identification de l'esclave



Exemple : code fonction 0x5 de l'esclave 2

0101 000 0010

010 1000 0010

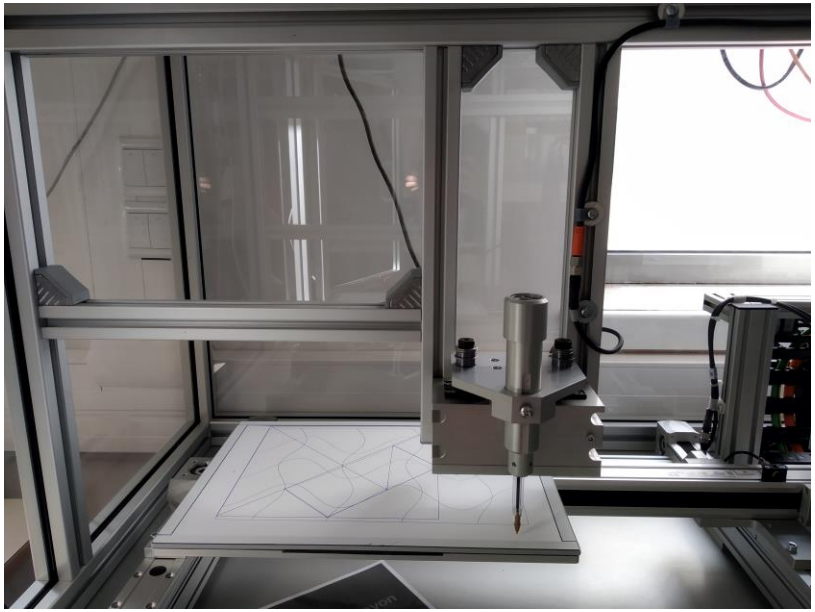
COB-ID : 0x 2 8 2

5. EXEMPLES D'ATTAQUES SUR LE BUS CAN

Etude de cas

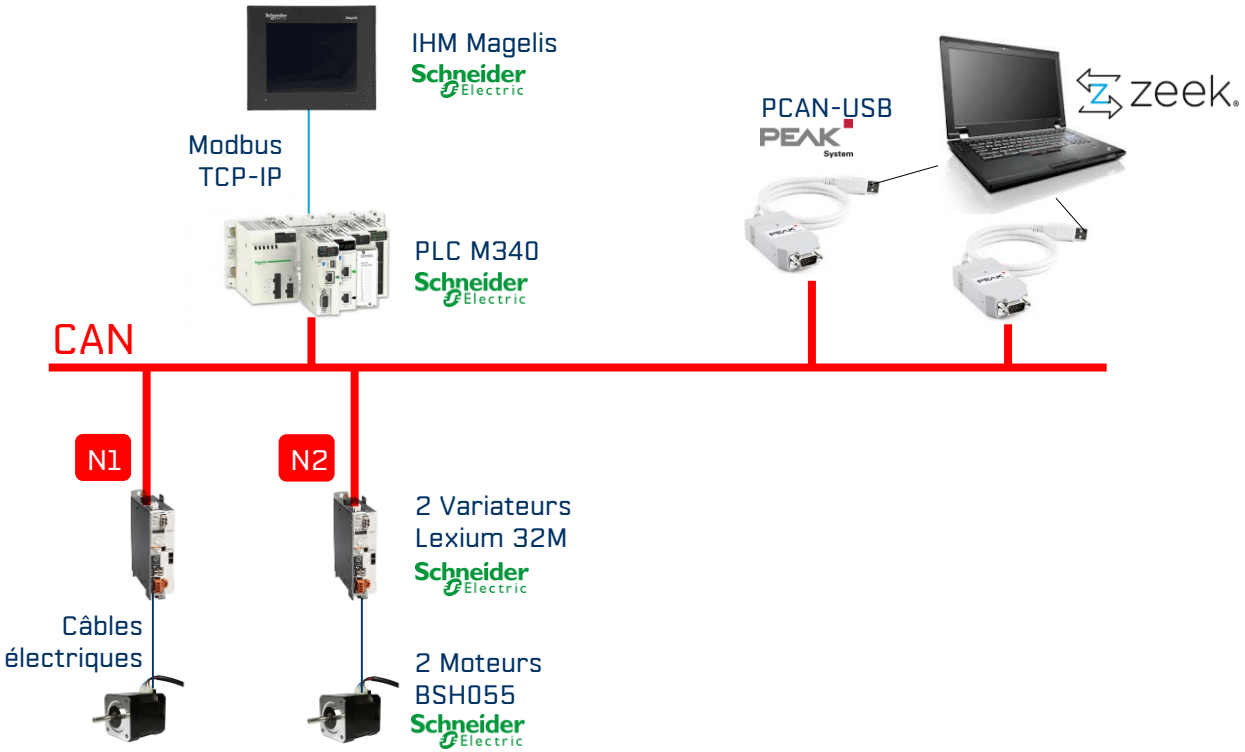
G-ICS Industrial Cybersecurity Lab [1]

- Robot traceur de traits
- Déplacement de la feuille selon deux axes (x et y)
- Boucle locale :
  - 1 PLC (Programmable Logic Controller)
  - 2 variateurs
  - 2 moteurs
  - 1 HMI (Human-Machine Interface)



[1] S. Mocanu, M. Puys, et P.-H. Thevenon, « An Open-Source Hardware-In-The-Loop Virtualization System for Cybersecurity Studies of SCADA Systems », C&esar - Virtualization and Cybersecurity, 2019.

5. EXEMPLES D'ATTAQUES SUR LE BUS CAN



- PLC maître de bus
- Identification des nœuds du bus : variateurs = N1 et N2
- Capture + Injection de données au niveau du bus CAN (en ligne)
- Utilisation de Zeek ; ajout d'un « CAN Analyzer » aux modules natifs de Zeek

5. EXEMPLES D'ATTAQUES SUR LE BUS CAN

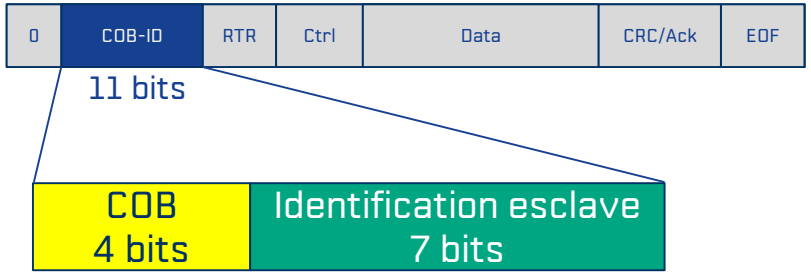
Script Zeek utilisé

DLC = Data Length Code

```
## Règles
# COB-ID autorisés avec leurs DLC possibles (2 noeuds)
global allowed : table[count] of set[count] = {
        [0x000] = set(2),
        [0x001] = set(0, 1),
        [0x07F] = set(0, 1),
        [0x080] = set(0, 1),
        [0x081] = set(8),
        [0x082] = set(8),
        [0x100] = set(6),
        [0x181] = set(0, 1, 2, 3, 4, 5, 6, 7, 8),
        [0x182] = set(0, 1, 2, 3, 4, 5, 6, 7, 8),
        [0x201] = set(0, 1, 2, 3, 4, 5, 6, 7, 8),
        [0x202] = set(0, 1, 2, 3, 4, 5, 6, 7, 8),
        [0x281] = set(8),
        [0x282] = set(0, 1, 2, 3, 4, 5, 6, 7, 8),
        [0x301] = set(0, 1, 2, 3, 4, 5, 6, 7, 8),
        [0x302] = set(0, 1, 2, 3, 4, 5, 6, 7, 8),
        [0x581] = set(8),
        [0x582] = set(8),
        [0x601] = set(8),
        [0x602] = set(8),
        [0x701] = set(1),
        [0x702] = set(1),
        [0x77F] = set(1),
};
```

DLC correspondants

COB-ID autorisés pour ce système



Code fonction 0x5 de l'esclave 2

COB-ID : 0x282

5. EXEMPLES D'ATTAQUES SUR LE BUS CAN

Cas 1

Attaques qui modifient la structure des trames :

- COB-ID non autorisés
- Longueurs de trame non autorisées (relativement au COB-ID)

Cas 2

Attaques qui modifient la payload uniquement :

- Mode de fonctionnement par pas de 30 mm
- Incréments des pas jusqu'à dépasser la butée physique

6. RÉSULTATS

Cas 1

```
ubuntu@ubuntu-HP-Pavilion-Notebook:~$ cansend can1 283#d827feff00000000
ubuntu@ubuntu-HP-Pavilion-Notebook:~$ cansend can1 080#5045
ubuntu@ubuntu-HP-Pavilion-Notebook:~$
```

```
listening on can0

Can object 283 len 8 payload d8 27 fe ff 00 00 00 00
Can object 80 len 2 payload 50 45 00 00 00 00 00 00
```

Attaque 1 :

COB-ID = 0x283 ; mais nœud 3 n'existe pas dans le système

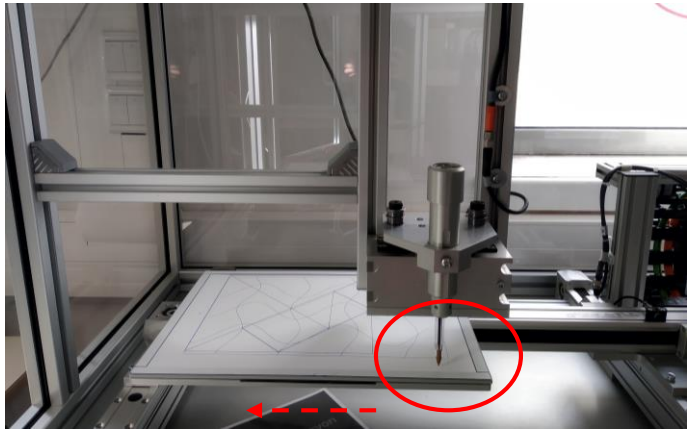
Attaque 2 :

DLC de 2 ; n'existe pas pour le SYNC protocol (0x80)

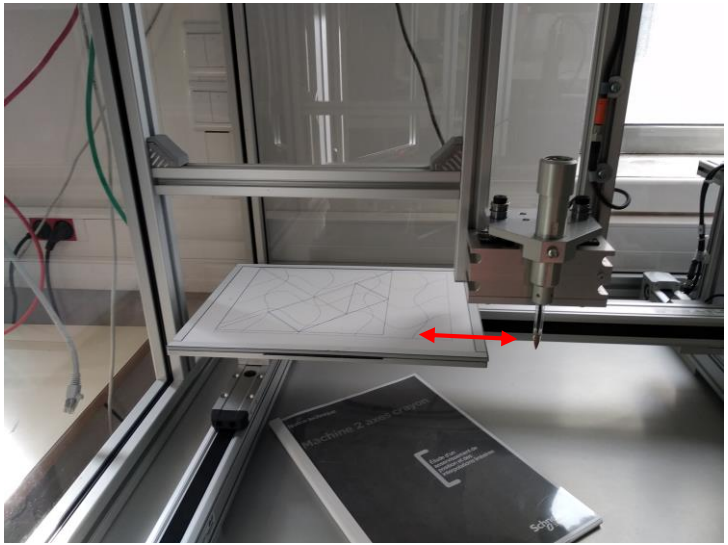
Détectées et loggées

6. RÉSULTATS

Cas 2 Attaque 3 : modification de la payload



```
cansend can0 202#c142f40171720000
sleep 0.5
cansend can0 202#4142f40171720000
sleep 0.5
cansend can0 202#c142f40171720000
sleep 0.5
cansend can0 202#4142f40171720000
```



Attaque non détectée

Variateurs en erreur

7. SYNTHÈSE ET PERSPECTIVES

Implémentation de 2 types d'attaques sur le bus CAN :

1. Attaques qui violent la structure des trames du protocole CAN
2. Attaques qui respectent la structure des trames

Attaques "process aware" :

- Attaques qui peuvent dégrader le système physique de façon directe
- Non détectables au niveau de la structure des trames
- Nécessité d'avoir une approche comportementale
- Utilisation de Zeek

NAVAL GROUP

POWER AT SEA

SYSTÈME DE DÉTECTION D'INTRUSIONS POUR LE BUS DE TERRAIN CAN, AVEC ZEEK

Estelle Hotellier - Naval Group, NCL– INRIA, LIG, Grenoble-INP, UGA
Franck Sicard - Naval Group, NCL
Julien Francq - Naval Group, NCL
Stéphane Mocanu – INRIA, LIG, Grenoble-INP, UGA

28/08/2021

Inria LIG Grenoble INP UGA