

# Club EBIOS

Risque « cyber » sur les SI Industriels  
Une approche de sensibilisation



Réunion courante du 22/03/2018



LE CHOIX DE L'EXPERTISE



# L'USINE DE PRODUCTION

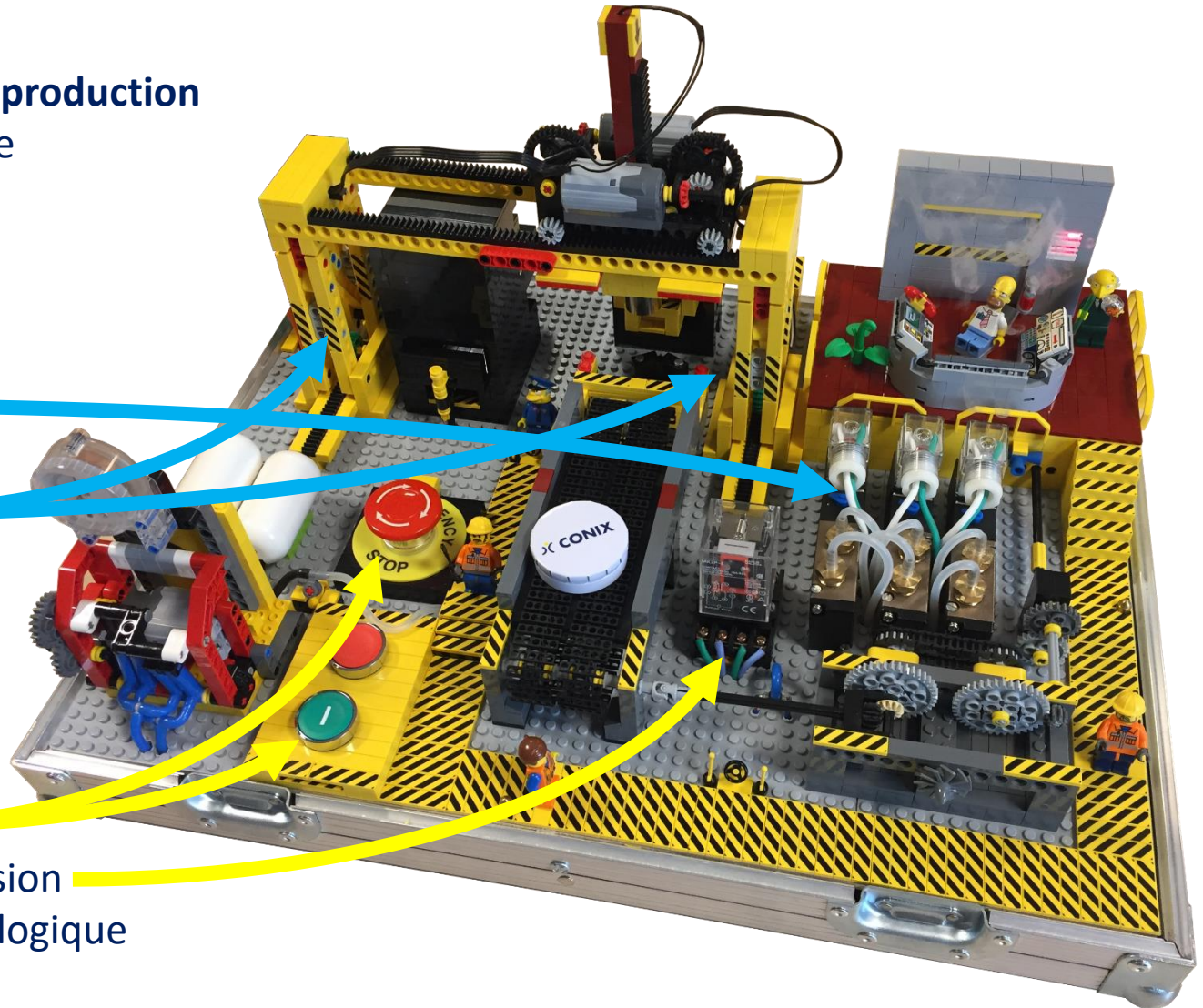
1 environnement de production  
1 circuit pneumatique

## Des actionneurs :

- 3 valves
- 4 moteurs
- 2 pistons
- 1 électro aimant

## Des capteurs :

- 3 boutons
- 1 capteur de pression
- 1 manomètre analogique



# L'USINE DE PRODUCTION

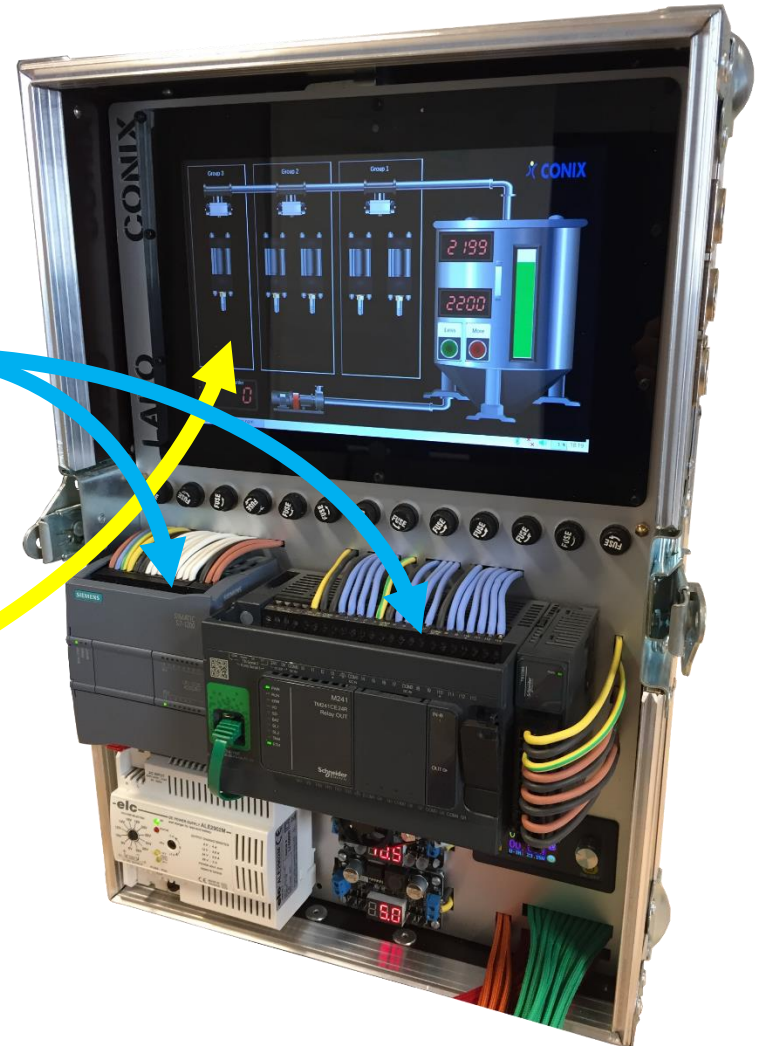
**1 environnement de contrôle-commande**  
**1 circuit électrique**

**De l'intelligence (programmée) :**

- 2 PLC (Programmable Logic Controllers)

**Des éléments d'interface :**

- 1 IHM
- 1 port USB
- 1 port ethernet



## MENACES

### Les vecteurs

- Phishing mail
- Phishing USB

### Les « charge utiles »

- 1 fichier bureautique (+ VBScript)
- 1 lien Internet
- 1 script (+ clef USB auto exécutable)

## VULNÉRABILITÉS

### Sur le service HTTP

- Identifiant par défaut du service HTTP
- Cookie de session rejouable

### Sur les protocoles

- Protocole non chiffré
- Protocole décodable

**Déni de service sur l'automate** → **Arrêt de la production**

**Déni de service sur l'IHM** → **Compromission du procédé**

**Compromission PLC (man in the middle)** → **Explosion**

**Compromission PLC (reprogrammation)** → **Dysfonctionnement de l'arrêt d'urgence**

## ÉVÉNEMENTS REDOUTÉS

## IMPACTS

## MENACES

### Les vecteurs

- Phishing mail
- Phishing USB

### Les « charge utiles »

- 1 fichier bureautique (+ VBScript)
- 1 lien Internet
- 1 script (+ clef USB auto exécutable)

## VULNÉRABILITÉS

### Sur le service HTTP

- Identifiant par défaut du service HTTP
- Cookie de session rejouable

### Sur les protocoles

- Protocole non chiffré
- Protocole décodable

Déni de service sur l'automate

Déni de service sur l'IHM

Compromission PLC (man in the middle)

Compromission PLC (reprogrammation)

## ÉVÉNEMENTS REDOUTÉS

**Arrêt** de la production

**Compromission** du procédé

**Explosion**

**Dysfonctionnement** de l'arrêt d'urgence

## IMPACTS



## POURQUOI ÇA MARCHE ?

---

-  **Parce qu'il y a de la fumée (= risque HSE)**
-  **Parce que c'est coloré et ce sont des briques lego**

## POURQUOI Ç'EST INTÉRESSANT ?

---

-  **Parce que ça met en scène le digital dans l'industrie**
-  **Parce que ça matérialise le risque (HSE)**