

DE LA RECHERCHE À L'INDUSTRIE

cea den

# CONGRÈS D'INGÉNIERIE DES GRANDS PROJETS ET DES SYSTÈMES COMPLEXES (IGPSC)

## CYBER SÉCURITÉ DES SYSTÈMES INDUSTRIELS

PATRICK BALDIT

# LES ENJEUX DE LA CYBERSÉCURITÉ

## Risques inacceptables :

[RI 2] : Disparition de **matière nucléaire**

[RI 3] : Tensions fortes et durables dans les **relations avec les autorités de sûreté**

[RI 4] : Perte de **crédibilité** du CEA

[RI 4-2] Perte de **leadership international** dans le domaine du nucléaire civil

[RI 4-3] Perte de **reconnaissance scientifique** en recherche fondamentale

[RI 6] : Atteinte au secret de **défense nationale**

[RI 7] : Perte de confiance des décideurs (Gouvernement et Parlement)

[RI 8] : Perte de la **maîtrise du système d'information**

[RI 9] : Perte des **alliances** ou des coopérations nucléaires avec les **pays clés**

## Risques majeurs :

[RM 3] : Acte de **terrorisme** visant le CEA

[RM 9] : Mauvaise **gestion médiatique**

[RM 9-1] Attaque médiatique des activités spécifiques du CEA

[RM 9-2] Attaque médiatique imputant au CEA des préjudices issus ou occasionnés par ses recherches

[RM 16] : Arrêt brutal des **coopérations stratégiques** avec un grand partenaire industriel

## Risques forts :

[RF 1] : Prise en compte insuffisante ou trop tardive des règles de **sûreté / sécurité** dans les projets

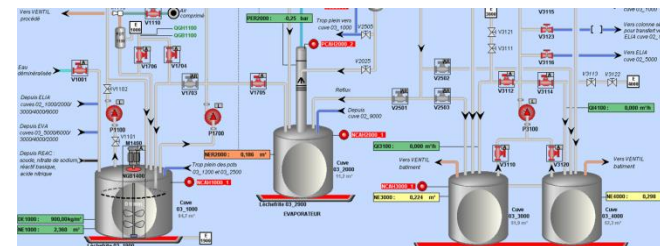
[RF 2] : Actions **d'intelligence économique** visant des technologies ou des chercheurs

[RF 5] : Développement des **contentieux**

[RF 5-1] Contentieux commerciaux et liés à la **propriété intellectuelle**

[RF 6] : Mauvaise **valorisation** des recherches

- les environnements informatisés de production, de contrôle et de sécurité ;
- les réseaux de contrôle-commande distribués ;
- les infrastructures de supervision, contrôle et acquisition de données SCADA (Supervisory Control and Data Acquisition) ;
- les systèmes de contrôle industriels ICS (Industrial Control Systems) ;
- les systèmes de contrôle de processus PCS (Process Control Systems) ;
- les systèmes de gestion des réseaux de distribution d'électricité, d'eau, de gaz, etc.
- les réseaux de relevé d'alarmes (intrusion, incendie, etc.) ;
- les réseaux de diffusion d'alertes (RDO, alarmes, etc.) ;
- les systèmes de gestion des processus industriel (salles blanches, appareils médicaux, etc.) ;
- les systèmes de contrôle des instruments de recherche ;
- les systèmes de gestion et de contrôle des installations ;
- les systèmes de contrôle d'accès.



|        | Téléalame Contrôle-accès | Contrôle-commande | Fluide | Acquisition, Mesure | Total |
|--------|--------------------------|-------------------|--------|---------------------|-------|
| Actuel | 177                      | 479               | 92     | 98                  | 846   |

Expérimentation

Procédé

Labo 1

Labo 2

Standardisation DEN

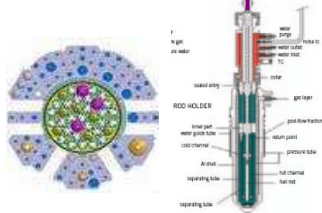
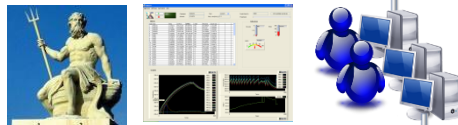
Cyber sécurité

Serveurs & Sauvegardes

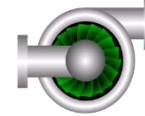
Supervisions

Automates

Procédé



Vanne



Moteur



Débitmètre

## ■ Loi de programmation militaire 2014-2019



### Que dit la loi ?

#### LOI n° 2013-1168 (18 décembre 2013) Chapitre IV

- Le Premier ministre fixe les règles de sécurité [...] des opérateurs publics ou privés [...] qui assurent la sécurité ou la capacité de survie de la Nation. Ces opérateurs sont tenus d'appliquer ces règles à leurs frais.
- Les systèmes [...] exploités sur le territoire national par des prestataires de service qualifiés en matière de sécurité de systèmes d'information, par l'ANSSI ou par d'autres services de l'Etat désignés par le Premier ministre.
- Les opérateurs [...] informent sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité des systèmes [...].
- A la demande du Premier ministre, les opérateurs [...] soumettent leurs systèmes [...] à des contrôles [...]. Le coût des contrôles est à la charge de l'opérateur.
- Pour répondre aux crises majeures [...] le Premier ministre peut décider des mesures que les opérateurs [...] doivent mettre en œuvre.
- Est puni d'une amende de 150 000 € le fait, pour les mêmes personnes, de ne pas satisfaire aux obligations [...].



Nota : aux USA le Président Obama, dans son « Executive Order », du 12 février 2013 a jeté les bases d'une politique nationale d'amélioration de la résilience des infrastructures critiques..



Procédé



Ventilation

Electricité



# LA CYBER ATTAQUE

*MYTHE OU RÉALITÉ*



## Les systèmes industriels ont à peu près 10 ans de retard par rapport au monde bureautique !

- A peu près tous les composants sont vulnérables ...,
- Pas de mécanismes de sécurité prévu dans les protocoles réseau,
- Des configurations non sécurisées,
- Des mots de passe par défaut (**Siemens - CVE-2010-2772 – Stuxnet**)

*The 'WinCCConnect' and 'WinCCAdmin' accounts have a password of '2WSXcder' which is publicly known and documented. This allows attackers to trivially access the program or system.*

- ... et codés en dur (**Turck BL20/BL67 - ICSA-13-136-01**)
- Absence de compatibilité avec les systèmes d'exploitation récents et les antivirus,
- Des services réseau (non sécurisés) ouverts (modification de firmware, etc.)
- Et toujours la menace des médias amovibles !



POLITIQUE SOCIÉTÉ MONDE ÉCONOMIE CULTURE NEXT IDÉES VIDÉO PHOTO ▼

## Un ver informatique dans le nucléaire iranien

DELPHINE MATTHIEUSSENT JÉRUSALEM, DE NOTRE CORRESPONDANTE ET JEAN-PIERRE PERRIN 29 SEPTEMBRE 2010 À 00:00



Des installations sur le site iranien gazier de South Pars en juillet 2010. (© AFP Atta Kenare)



Le virus Stuxnet a infesté un nombre important d'ordinateurs contrôlant des infrastructures du pays, notamment le centre de recherche atomique de Natanz. Téhéran soupçonne les Etats-Unis et Israël.



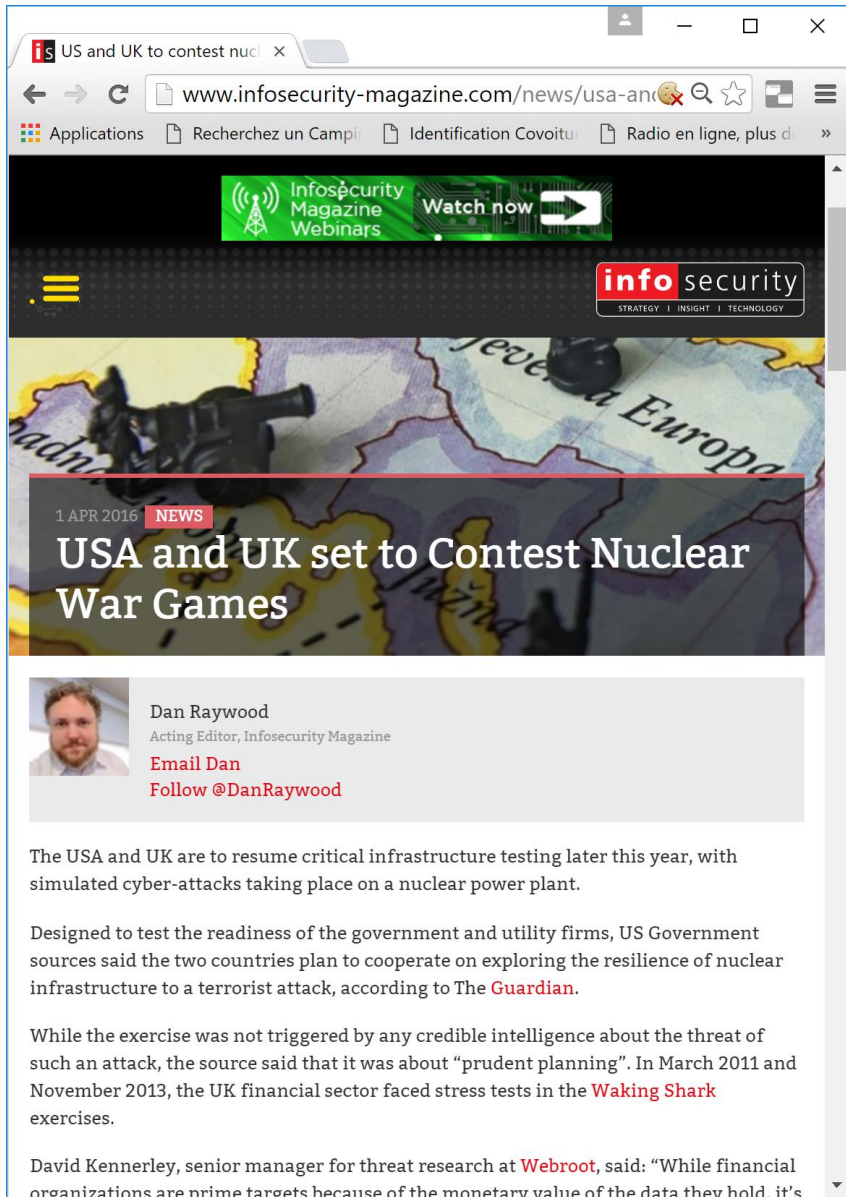
D'après les responsables iraniens, qui ont évoqué, dimanche, dans la presse une "guerre électronique", ce programme malicieux n'a toutefois pas fait de dégâts industriels majeurs et a notamment épargné la centrale nucléaire de Bouchehr, située dans le sud du pays.

Trente mille ordinateurs infectés par Stuxnet ont été jusqu'à présent dénombrés en Iran, selon Mahmoud Liayi, responsable des technologies de l'information au ministère de l'industrie. Stuxnet, découvert en juin, recherche dans les ordinateurs qu'il infecte le système de supervision de l'allemand Siemens, WinCC, qui sert au contrôle des oléoducs, des plates-formes pétrolières, des centrales électriques et d'autres installations industrielles.

Sa fonction serait d'entraîner la destruction physique des installations touchées, selon certains experts qui ont évoqué un "sabotage par informatique". D'après un responsable de la société américaine Symantec, 60 % des ordinateurs infectés par ce virus se trouvent en Iran. Mais l'Inde, l'Indonésie ou le Pakistan, seraient aussi frappés.

**Stuxnet est devenu la référence en terme de cyberarme.**

**Sa complexité et sa technicité implique des mois de développement et des moyens très importants**



US and UK to contest nuclear war games


www.infosecurity-magazine.com/news/usa-and-uk-to-contest-nuclear-war-games

Infosecurity Magazine Webinars Watch now

info security  
STRATEGY | INSIGHT | TECHNOLOGY

1 APR 2016 NEWS

## USA and UK set to Contest Nuclear War Games

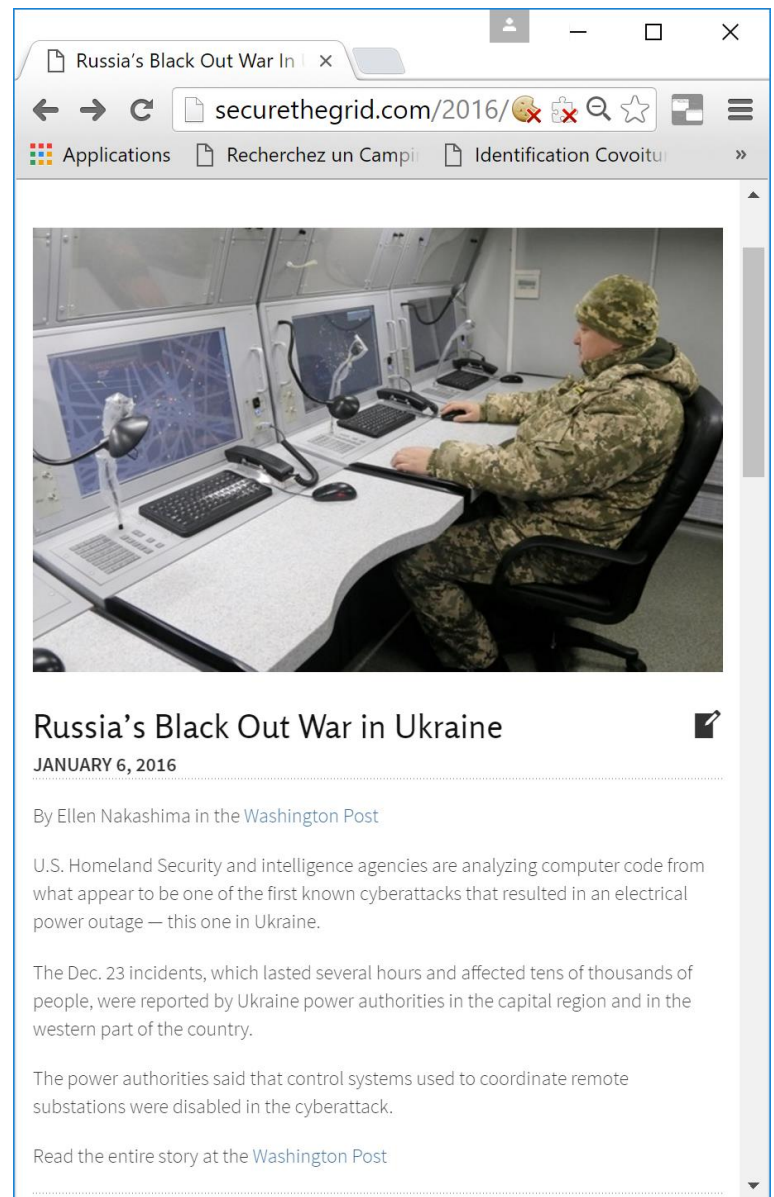
 Dan Raywood  
Acting Editor, Infosecurity Magazine  
[Email Dan](#)  
[Follow @DanRaywood](#)

The USA and UK are to resume critical infrastructure testing later this year, with simulated cyber-attacks taking place on a nuclear power plant.

Designed to test the readiness of the government and utility firms, US Government sources said the two countries plan to cooperate on exploring the resilience of nuclear infrastructure to a terrorist attack, according to [The Guardian](#).

While the exercise was not triggered by any credible intelligence about the threat of such an attack, the source said that it was about “prudent planning”. In March 2011 and November 2013, the UK financial sector faced stress tests in the [Waking Shark](#) exercises.


David Kennerley, senior manager for threat research at [Webroot](#), said: “While financial organizations are prime targets because of the monetary value of the data they hold, it’s



Russia's Black Out War in Ukraine

securethegrid.com/2016/01/06/russias-black-out-war-in-ukraine

Applications Recherchez un Campi Identification Covoitu Radio en ligne, plus d



## Russia's Black Out War in Ukraine

JANUARY 6, 2016

By Ellen Nakashima in the Washington Post

U.S. Homeland Security and intelligence agencies are analyzing computer code from what appear to be one of the first known cyberattacks that resulted in an electrical power outage — this one in Ukraine.

The Dec. 23 incidents, which lasted several hours and affected tens of thousands of people, were reported by Ukraine power authorities in the capital region and in the western part of the country.

The power authorities said that control systems used to coordinate remote substations were disabled in the cyberattack.

[Read the entire story at the Washington Post](#)



Une centrale nucléaire alle...

www.lepoint.fr/societe/une-centrale-nucleaire-allemande-victir

Applications Recherchez un Campi Identification Covoitu Radio en ligne, plus d Sites suggérés

Services Newsletters Montres Automobile Vin Le Point Pop f g t Q

MENU **Le Point**

## Une centrale nucléaire allemande victime d'une cyberattaque

Des pirates informatiques ont tenté de prendre le contrôle à distance de plusieurs serveurs gérant une installation sensible outre-Rhin.  
**PAR BAUDOIN ESCHAPASSE**  
 Modifié le 29/04/2016 à 19:13 - Publié le 29/04/2016 à 18:36 | Le Point.fr



ABONNEZ-VOUS À PARTIR DE 1€

L'information a été confirmée au lendemain du **trentième anniversaire de la catastrophe de Tchernobyl**. Mais la rumeur circulait depuis plusieurs jours dans le petit monde de la cybersécurité. Une centrale nucléaire allemande a bel et bien été visée par plusieurs attaques informatiques d'ampleur. Révélée par le quotidien britannique *The Telegraph*, la nouvelle a de quoi faire frémir, d'autant que les services de renseignements européens RETOUR

L'impréparation domine f...

www.lemagit.fr/actualites/450281562/Limpreparation-domine-face-au-risque

Applications Recherchez un Campi Identification Covoitu Radio en ligne, plus d Sites suggérés

MENU **LEMAGIT** Q

## L'impréparation domine face au risque de cyberattaque sur des infrastructures critiques

par  
**Valéry Marchive**  
 Rédacteur en chef adjoint  
 Publié le 18 avr. 2016

[t](#) [g+](#) [in](#) [✉](#)

Les parlementaires américains s'inquiètent du manque de préparation à une éventuelle panne électrique de longue durée causée par une cyberattaque.

La commission aux transports et aux infrastructures du parlement américain semble inquiète, au moins point de se saisir de la question de la préparation des Etats-Unis au risque d'attaque informatique sur son réseau de distribution électrique. Dans un discours d'introduction à la réunion organisée la semaine dernière sur le sujet, Lou Barletta, président de la sous-commission du développement économique, des édifices publics et de la gestion des urgences, relève un nombre élevé d'audiences consacrées à la cybersécurité et « à comment arrêter les méchants ». Mais il estime

f t g+ in

Le 24 Décembre 2014

## Le géant du nucléaire coréen victime de cyber-pirates



L'opérateur nucléaire sud-coréen KHNP a de nouveau été victime de cyber-pirates. (Crédit D.R.)

**Pour la cinquième fois, des cyber-pirates ont publié en ligne des documents volés dans les systèmes informatiques de l'opérateur sud-coréen de centrales nucléaires KHNP.**

Mardi, une nouvelle série de documents internes volés à l'opérateur de centrales nucléaires sud-coréen Korea Hydro and Nuclear Power (KHNP), ont été publiés sur Internet. Lors d'une réunion ministérielle, le président Park Geun-hye a reconnu la gravité de ces fuites, précisant que la situation relevait de la sécurité nationale. Dans un message posté à 15 h, heure locale, un pirate anonyme affichant l'ID Twitter @John\_kdfifj1029, a conseillé aux citoyens coréens de se tenir à l'écart des centrales nucléaires et s'est moqué de

l'exercice organisé lundi par l'opérateur KHNP pour répondre à la cyberattaque. « Le 9 décembre est une date qui restera dans l'histoire », dit-il dans son message. Le 9 décembre étant le jour où l'opérateur Korea Hydro and Nuclear Power a détecté pour la première fois la présence de code malveillant dans le courriel de ses employés.

# QUELQUES EXEMPLES

*CHEZ NOUS ...*

*..... PAS ENCORE D'ATTAQUES MAIS DES PROBLEMES DE  
SECURITÉ INFORMATIQUE ÉVIDENTS*

- 04/2013 : Découverte d'un trafic réseau anormal sur le PC de réception des colis en entrée d'une installation (activité de type malware)
- J+1 : Un disque dur externe USB a été connecté sur ce poste et sur d'autres postes de l'installation par l'opérateur industriel (prestataire)
- J+2 : Analyse complète des postes industriels
  - *6 postes sur 13 sont infectés*
- J+4 : Découverte d'un malware sur le poste de l'opérateur industriel (prestataire) qui intervient sur plusieurs installations du centre ...





**ET ALORS ?**

***QUE DOIT ON FAIRE POUR NOS INSTALLATIONS  
INDUSTRIELLES***

## Impacts :

- Médiatique

- Programmes (perte de disponibilité)

  - Ex : Attaque en ukraine : « Les attaquants ont tout d'abord utilisé les IHM Scada identifiés auparavant pour lancer des commandes d'ouverture des disjoncteurs dans au moins sept postes haute tension et vingt-trois postes moyenne tension au sein des trois distributeurs. Cela a eu pour conséquence de couper la distribution électrique de ces parties du réseau »

- Sûreté

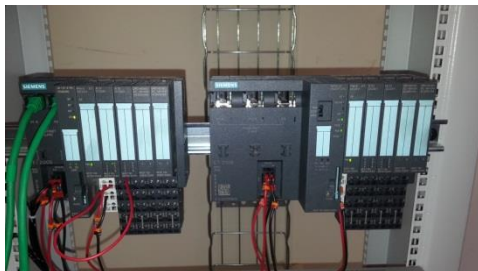
**Décret d'application de la LPM (avril 2017 pour le nucléaire) :**

**impact sur les sous-traitants des OIV**

Probabilité d'occurrence d'une attaque cyber

>>>

aléa sismique



## INFRASTRUCTURE

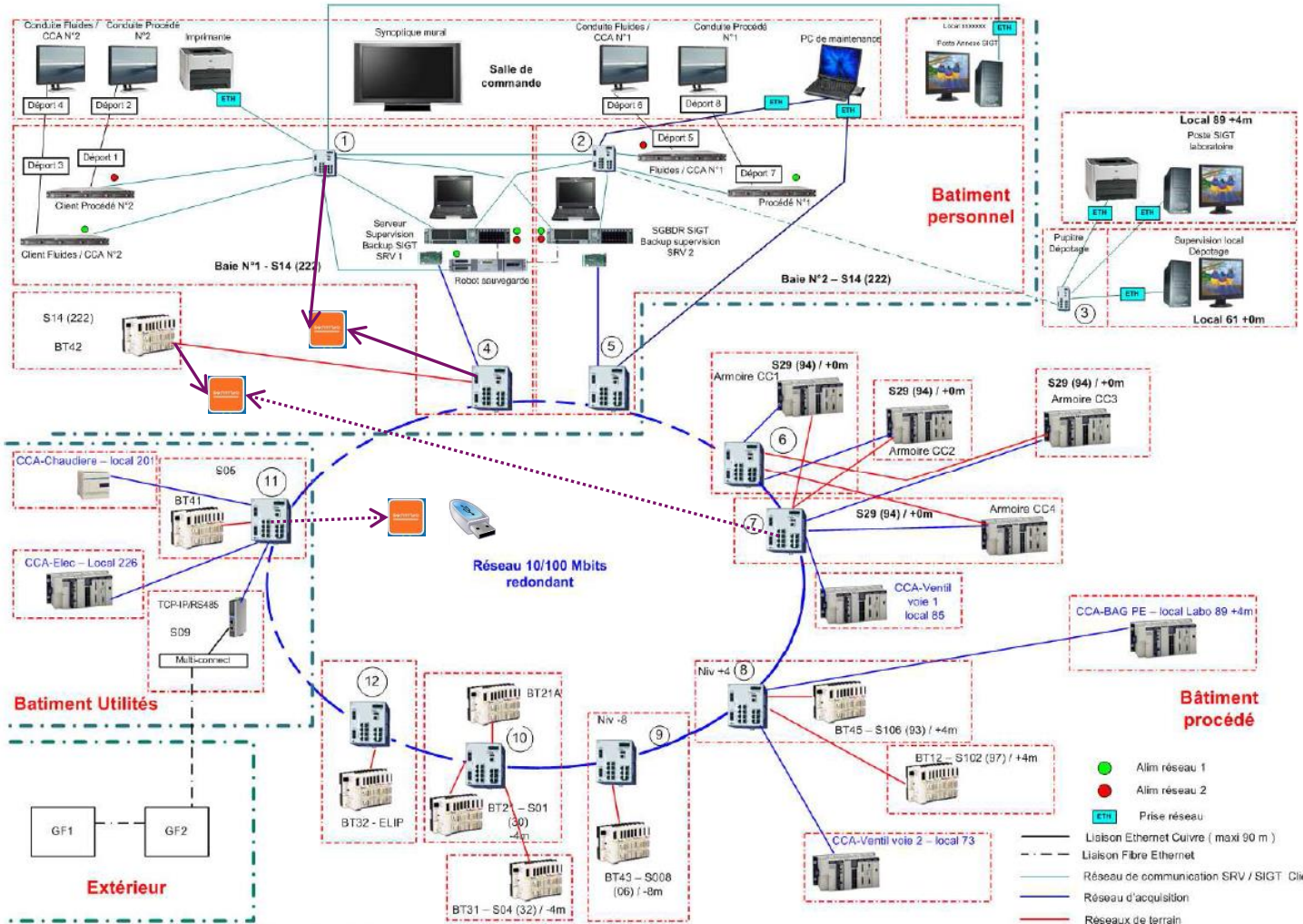
- Validation des “produits de sécurité”, dédiés SCADA
- Définition de standards (CYBERGUIDES)
- Validation des évolutions avant mise en production
- Tests de nouvelles infrastructures

## ANALYSE & DETECTION

- Scénarios d'attaques
- Qualification de solutions d'analyses et de détection
- Conception de solutions de supervision Cyber (correlation de données et analyse comportementale)



# COLLECTES DES FLUX INFORMATIQUES



Architecture réseau Infirnie 00 - Ma 13a 2011/12

Mirroring de ports sur commutateurs du procédé

Les ports en mirroring ne prennent pas en compte les flux entrants → Les sondes ne peuvent agir sur le procédé

Limitations  
 – Version OS switch pour port mirroring  
 - Positionnement sonde vis-à-vis des flux

# du boulot en perspective.....

