HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

La loi de programmation militaire pour un petit OIV

Béatrice JOUCREAU - Christophe RENARD

Hervé Schauer Consultants

10 mars 2015

La LPM pour un petit OIV

- Introduction
- Contexte de la Loi de Programmation Militaire
  - Contexte institutionnel
  - Modèle de menaces
- Situation réglementaire
  - Définitions
  - Textes de référence et historique
  - Intervenants et interlocuteurs
  - Calendrier
- Situation technique
  - Schémas d'organisation
  - Cycles et Acteurs
  - Vulnérabilités
- Méthode de classification du guide de cybersécurité des systèmes industriels
  - Le guide
  - Méthode de classification des systèmes industriels
- Conclusion

Introduction

Sommaire

Quel est le but de cette présentation ?

- Présentation
  - Du contexte LPM/OIV
  - De ce qu'il en découle pour les petits OIV
  - Des pistes de prise en compte
- Nos objectifs
  - Partager l'expérience HSC en la matière
  - Ouvrir le débat et les échanges

Contexte de la Loi de Programmation Militaire

Sommaire

Prise en compte de la SSI par les institutions

Un long cheminement

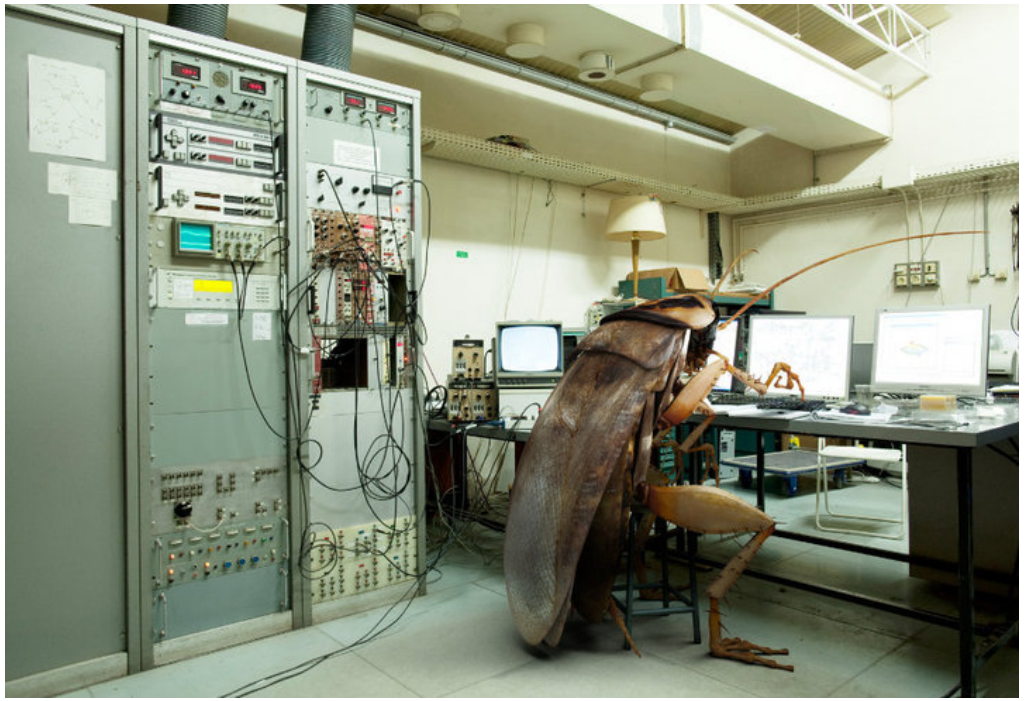
- L'informatisation précède universellement la maturation
  - Dépendance très forte sur l'informatique
  - Cadre législatif et institutionnel faibles
- Une prise en compte récente mais au pas de course
  - Livre blanc de la défense 2008: identification du besoin
  - Évolution majeure avec la création de l'ANSSI en 2009
    - Agence initialement centrée sur l'administration
    - En particulier au travers du RGS
    - Définition un processus de certification de prestataires
    - Généralisation de la démarche d'homologation
    - L'informatique "classique" reste le cœur de cible
  - Élargissement vers la protection des intérêts de la nation
    - L'ANSSI devient l'autorité nationale de cyberdéfense
    - Livre Blanc de la Défense 2013: la cyberdéfense enjeu de souveraineté
  - Passage de la LPM en fin 2013
    - L'article 22 définit la protection des systèmes critiques
    - Les Systèmes Critiques sont pris en compte
    - Création d'obligation forte de sécurisation
    - Avec des sanctions pénales lourdes à la clé

Inclusion du contexte industriel

Une tendance mondiale

- La sécurité informatique industrielle n'est pas récente
  - Certains acteurs ont commencé dès les années 80
  - Pas d'engagement global
  - Une perception de la menace inégale
- Après 2001: beaucoup de travaux aux États-Unis
- Et dans les communautés "sécurité" :
  - Blackhat, Defcon, CCC
  - Beaucoup d'attaques présentées
  - Peu de défense
- En 2010 Stuxnet donne une exposition majeure aux risques informatiques industriels

Modèle de menaces



- Sources de menace
  - États
  - Terroristes
  - *Insiders*
  - Criminels et non ciblé

États

Le pipeline BTC

- Le 7 août 2008 à 23h, le pipeline BTC explose
  - Pipeline concurrent de ceux opérés par les entreprises d'Etat russes
  - Traversant la Géorgie (et donc y contribuant financièrement)
  - La veille de l'intervention russe en Ossétie
  - Une attaque sophistiquée
    - Sur le territoire turc
    - Désactivation des sécurités industrielles et de la surveillance par piratage informatique
    - Intrusion physique et manipulation manuelle des vannes
    - Nécessite un haut niveau: logistique, d'entrainement, de connaissance de la cible

États

Récapitulatif

- Objectifs
  - Neutralisation d'un processus vital
  - Nuisance économique pour faire pression dans une négociation
  - Sabotage d'un effort de guerre
- Moyens:
  - Connaissance des processus
  - Capacité à monter des simulations complexes
  - Accès à des 0-days et des codes offensifs complexes
- Motivation à frapper un OIV
  - Fait maintenant partie de l'arsenal standard des relations inter-étatiques

Terrorisme

Le Pakistan dans le noir

- 26 janvier 2015 : 80% du Pakistan privé d'électricité pendant plus de 2 jours
  - Un attentat fait sauter 2 pylônes électriques
  - Résultant en une défaillance du système d'échelle nationale
  - 3ème tentative par les rebelles du Balouchistan depuis début 2015
  - Les 2 premières n'avaient causé que des pannes mineures

Terrorisme

Récapitulatif

- Objectifs
  - Frapper les esprits : moyens d'obtenir des concessions, de la visibilité ou de provoquer une répression impopulaire
  - Objectifs symboliques ou effrayants
- Moyens
  - Variables : de la petite organisation peu financée et disposant de peu de compétences au terrorisme à support étatique
  - La *commoditization* des technologies joue en leur faveur
- Motivation à frapper un OIV
  - Incertaine : les frappes sur des sites industriels peuvent faire l'objet d'une communication contrôlée (populations limitées, identification des causes longues)
  - La mise en défaillance d'un service, même critique, frappe rarement les opinions

Insiders

Exemple

- Le 15 août 2012, Saudi Aramco était victime d'un malware virulent
  - Tente d'exfiltrer des informations et écrase le MBR
  - Approximativement 30000 postes et 3000 serveurs contaminés
  - Revendiqué par un groupe inconnu *Cutting Sword of Justice*
  - Il faudra plus de 3 semaines pour maitriser la situation
  - A la source, un administrateur système à volontairement introduit le malware

Insiders

Récapitulatif

- Objectifs
  - Vengeance, nuisance à l'organisation
- Moyens
  - Accès privilégiés
  - Connaissance des processus
  - Accès physique
- Motivation à frapper un OIV
  - Forte suivant tensions sociales, ou locales (géopolitiques et religieuses dans le cas d'Aramco)

Criminels et non ciblé

Exemple

- Janvier 2003, la centrale de Davis-Besse dans l'Ohio a perdu la supervision informatique de ses processus
  - Le vers Slammer s'est infiltré sur le réseau via l'accès d'un sous-traitant
  - La perte de supervision a entrainé un passage en analogique
  - Alors que le personnel de l'usine traitait déjà un incident majeur (percement d'un réacteur)

Criminels et non ciblé

Récapitulatif

- Objectifs
  - Nuisance et gain financier
- Moyens
  - Codes non ciblés mais pouvant échapper aux antivirus
  - Dénis de service locaux
  - Chiffrement de données sensibles ?
- Motivation à frapper un OIV
  - Peut cibler un industriel pour des raisons indépendantes de son rôle stratégique
  - A quand la prise d'otage façon Cryptolocker d'un site industriel ?

Réalisme des attaques 1/2

L'ordinaire

- Les *insiders* sont la menace la plus banale
  - En particulier les acteurs à privilèges : administrateurs systèmes et réseau
  - La résilience face à un sabotage intelligent d'un acteur privilégié est complexe
  - Un acteur individuel peut avoir des effets à une échelle macroscopique
- Les malware non-ciblés sont un risque permanent
  - A considérer sous un angle épidémiologique
  - Mais la plupart des systèmes industriels ont un système immunitaire déficient
  - Et des pratiques douteuses propices à la contagion

Réalisme des attaques 2/2

L'extra-ordinaire

- Les attaques inter-étatiques se sont déjà produites
  - Il y aura d'autres Stuxnet
  - Les médias américain évoquent des pré-positionnements chinois depuis plusieurs années
  - Réalité ou sensationnalisme ?
  - Des attaques combinant cinétique et informatique ont eu lieu lors d'opérations russes
- Aucune attaque informatique terroriste n'est connue
  - Peu d'appels à ce genre d'attaque dans la littérature jihadiste (Inspire ou sites)
  - Mais des tentatives auront certainement lieu tôt ou tard
  - Cibles attractives pour des acteurs terroristes compétents ?

Niveau des impacts

Une évaluation complexe

- Le monde industriel maitrise la sûreté de fonctionnement
  - Fiabilité face aux menaces non intentionnelles
  - Fonctionnements par défaut sûrs
- La disponibilité de l'informatique est rarement prise en compte
  - Combien d'organisations peuvent encore fonctionner sans informatique ?
  - A quel coût et combien de temps ?
- Étudier les risques d'un OIV est complexe
  - Lien entre études de risques informatiques et de sûreté de fonctionnement complexe à établir
  - Le lien entre sureté et intérêt de la nation ?

Situation réglementaire

Sommaire

Qu'est-ce qu'un SAIV ?

Définition

- SAIV : Secteurs d'Activité d'Importance Vitale
  - Ensemble d'activités concourant à un même objectif
  - Qui ont trait à la production et la distribution de biens ou de services indispensables :
    - A la satisfaction des besoins essentiels pour la vie des populations
    - Ou à l'exercice de l'autorité de l'État
    - Ou au fonctionnement de l'économie
    - Ou au maintien du potentiel de défense
    - Ou à la sécurité de la Nation
    - Dès lors que ces activités sont difficilement substituables ou remplaçables
  - Ou peuvent présenter un danger grave pour la population
- Liste des SAIV définie par le Premier Ministre
- Un ministre coordonnateur défini pour chaque SAIV

Qu'est-ce qu'un SAIV ?

Liste des SAIV

Secteur	Ministre coordonnateur
Activités civiles de l'État	Ministre de l'Intérieur
Activités judiciaires	Ministre de la Justice
Activités militaires de l'État	Ministre de la Défense
Alimentation	Ministre chargé de l'agriculture
Communications électroniques, audiovisuel et information	Ministre chargé des communications électroniques
Énergie	Ministre chargé de l'énergie
Espace et recherche	Ministre chargé de la recherche
Finances	Ministre chargé de l'économie et des finances
Gestion de l'eau	Ministre chargé de l'écologie
Industrie	Ministre chargé de l'industrie
Santé	Ministre chargé de la santé
Transports	Ministre chargé des transports

Qu'est-ce qu'un OIV ?

Définition

- OIV : Opérateur d'Importance Vitale
  - Exerce des activités [...] comprises dans un secteur d'activités d'importance vitale
  - Gère ou utilise au titre de ces activités un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement :
    - D'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation
    - Ou de mettre gravement en cause la santé ou la vie de la population

Qu'est-ce qu'un OIV ?

Désignation

- Les OIV sont désignés parmi
  - Opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation
  - Gestionnaires d'établissements comprenant une installation nucléaire ou autres et dont la destruction ou l'avarie peuvent présenter un danger grave pour la population
- Sont désignés par arrêtés, eux-mêmes non publiés et non communicables

Liste des OIV

- 218 OIV, liste réputée classifiée Confidentiel Défense
- Une partie est connue via le Comité National des secteurs d'activité d'importance vitale (abrogé)
  - Comprenait dix personnalités désignées parmi les dirigeants des OIV
- Désignés par le ministre coordonnateur du secteur d'activité
  - Sur avis de la Commission interministérielle de défense et de sécurité des SAIV
  - Comprend des représentants de la Défense et de l'Économie
- Ou par le préfet du département dans laquelle se situe l'établissement
  - Sur avis de la Commission zonale de défense et de sécurité des SAIV
  - Présidée par le préfet de zone

La jungle des sigles : PIV, ZIV

- PIV : Point d'importance vitale - Établissement, installation ou ouvrage vital
  - Arrêtés de désignation classifiés Confidentiel Défense
- ZIV : Zone d'importance vitale - Aire dans laquelle sont implantés plusieurs PIV relevant d'OIV différents

Les textes qui définissent les mesures de sécurité applicables aux OIV

- A l'échelle d'un SAIV
  - DNS : Directives nationales de sécurité : une par SAIV
  - Classifiées Confidentiel Défense
  - Contient un rappel des mesures du plan Vigipirate applicables au SAIV
- A l'échelle d'un OIV
  - PSO : Plan de Sécurité Opérateur (classifiés CD)
  - Un par OIV, non obligatoire si un seul PIV
  - Analyse de risques propre à l'OIV (pas orientée SI uniquement)
  - Instanciation pour l'OIV des mesures de la DNS applicable
  - Politique de sécurité/sûreté à l'échelle de l'OIV dans son ensemble
- A l'échelle d'un PIV
  - PPP : Plan Particulier de Protection et PPE : Plan de Protection Externe (classifiés CD)
  - Un PPP par PIV
  - Éventuellement un PPP par ZIV
  - PPP : rédigé par l'opérateur. Mesures de protection du PIV prévues par l'OIV
  - PPE : rédigé par le préfet de département. Mesures prévues par les pouvoirs publics. De manière générale, non connu par l'opérateur

La loi de programmation militaire 2014-2019

LOI 2013-1168 du 18 décembre 2013, article 22

- A modifié le Code de la Défense
- Relative à la protection des infrastructures vitales contre la cybermenace
- Règles de sécurité fixées par le Premier Ministre
- Détection des événements : systèmes et prestataires qualifiés
  - PDIS : prestataires de détection d'incidents de sécurité
  - PRIS : prestataires de réponse aux incidents de sécurité
- Obligation de remonter les incidents
- Contrôle d'évaluation du niveau de sécurité et du respect des règles : prestataires qualifiés
  - Extension potentielle du champ d'action des PASSI : prestataires d'audit de la sécurité des systèmes d'information

Historique

- Première liste des SAIV fixée par arrêté en juin 2006
- IGI 6600 : 1ère version en septembre 2008, 2e version en janvier 2014
  - Objectif : anticiper et réagir à la menace terroriste
  - En particulier, menaces liées à la sécurité des systèmes d'information
- En 2014 : loi de programmation militaire
  - Une partie concerne directement la SSI des OIV
- Pour les systèmes industriels :
  Guide de cybersécurité des systèmes industriels (ANSSI)

La loi de programmation militaire

Applicabilité

- Systèmes d'information des OIV ou supportant les OIV et pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation
  - Systèmes dits d'importance vitale (SIV)
  - Plus de notion de danger grave envers populations
- Conditions et limites d'applicabilité attendues dans un (ou plusieurs) décret, non encore publié(s)
- Précisions dans des arrêtés

Types d'interlocuteurs

- FSSI : Fonctionnaire de Sécurité des Systèmes d'Information
  - Un par ministère
  - Point de contact SSI de son ministère
- AQSSI : Autorité Qualifiée en Sécurité des Systèmes d'Information
  - Nommée dans une entité (de l'Etat ou un OIV),
  - Point de contact du FSSI

Correspondants

A qui parler ?

- Pour les OIV
  - Le FSSI au ministère coordonnateur, relayé par l'AQSSI
  - Le coordinateur sectoriel (du SAIV correspondant) à l'ANSSI (bureau coordination sectorielle)
- Pour les prestataires
  - Le bureau Politique Industrielle et Assistance de l'ANSSI

Calendrier

- Décret précisant les conditions de mise en application de la LPM
  - Devait paraître à l'automne 2014
  - Probablement en cours de validation
- Règles de sécurité
  - Devaient paraître en décembre 2014
  - Impossible de déterminer des règles génériques s'appliquant à tous les secteurs
  - Règles sectorielles : arrêtés
  - Potentiellement intégrées dans les DNS
  - Classification de ces arrêtés ?
- Phase expérimentale
  - Des OIV contactés par l'ANSSI
  - Doivent établir un inventaire de leurs SIV, approuvé ensuite par l'ANSSI
  - Secteurs prioritaires : Energie, communications électroniques
  - Objectif: permettre de définir les arrêtés sectoriels

Questions en suspens

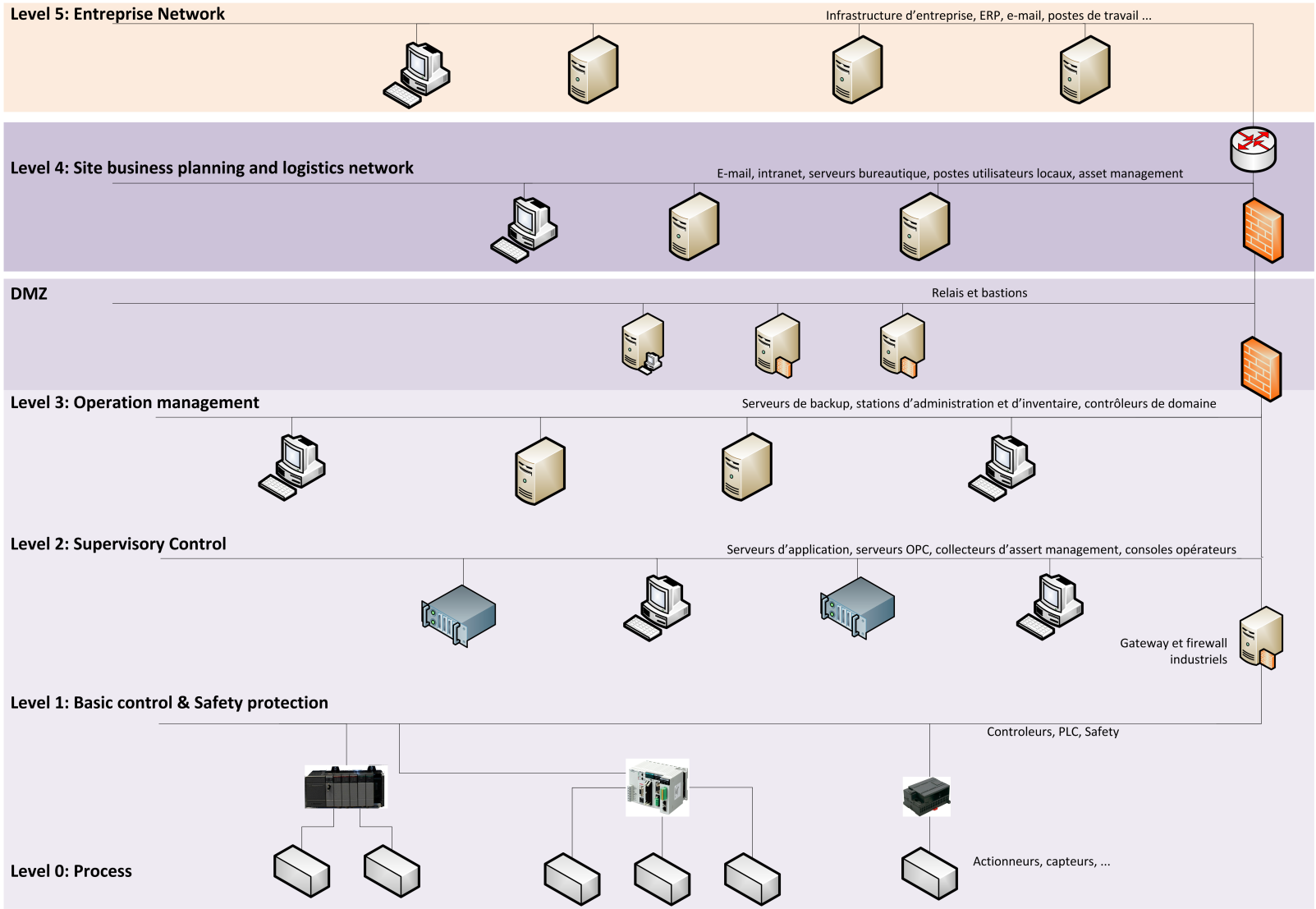
- Périmètre SIV
  - Identifier les SIV
  - Méthode de définition des SIV
  - Quid des systèmes ”supports” des SIV ?
- Mise en oeuvre
  - Application des règles sur l’ensemble du SIV de manière homogène ou par paliers
  - Délais de mise en oeuvre
- Impacts opérationnels des règles de sécurité sur l’activité

Situation technique

Sommaire

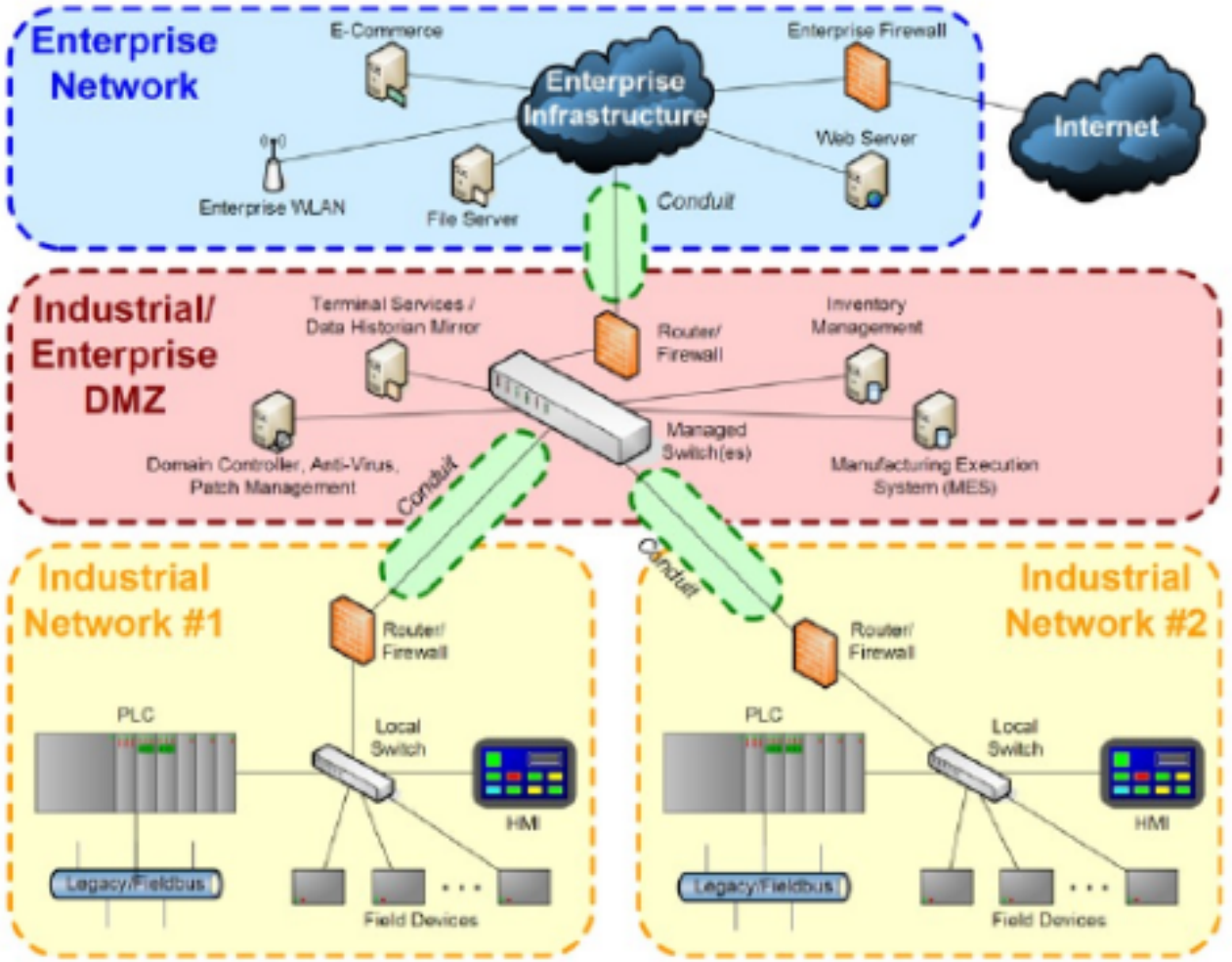
Modèle ISA/95

Une vue hiérarchisée du SI Industriel (SII)



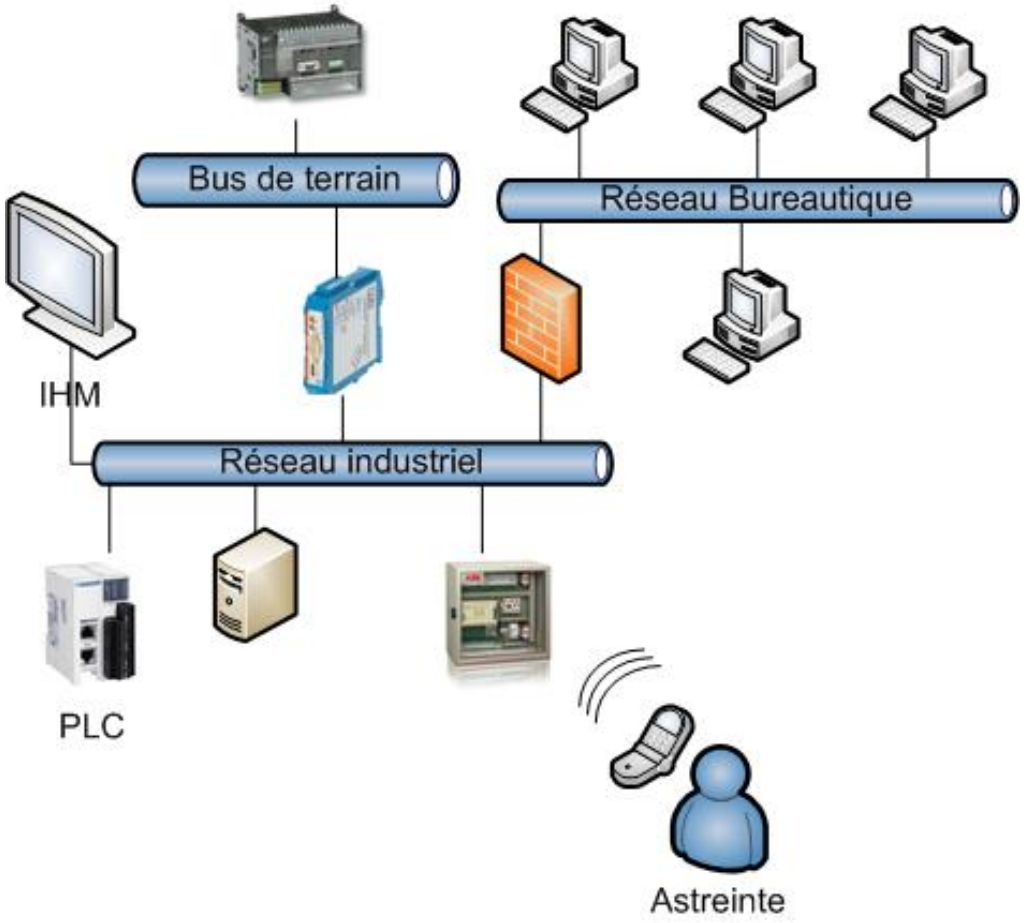
Modèle Zones et conduites

ISO/IEC 62443-2



Modèle réaliste

Un cloisonnement bien moindre



Une réalité très hétérogène 1/2

Size does matter

- La taille de l'organisation est déterminante
  - Permet de dédier des ressources à la sécurité
  - Des équipes plus nombreuses permettent de couvrir plus de compétences
  - Possibilité de dégager des budgets pour traiter la SSI
  - Certaines briques techniques ne se rentabilisent pas en deçà d'une certaine échelle
- Mais d'autres facteurs comptent
  - Ancienneté des installations
  - Secteur d'activité
  - Exigences de sécurité des clients
  - Étendue géographique de l'activité et des sites

Une réalité très hétérogène 2/2

L'état chez les petits industriels

- Résultat d'une évolution "organique"
  - Technologies de niveau bas hétéroclites
    - Des bus série
    - Technologies propriétaires
    - Variantes industrielles d'Ethernet
    - Cohabitation de plusieurs génération d'équipements
  - Informatique hétérogène peu ou pas mise à jour
    - Beaucoup de Windows XP : parfois imposé par des logiciels critiques
    - Rarement d'antivirus à jour
    - Politique de mise à jour souvent freinée par l'absence de procédure ou plateforme permettant de tester les non-régressions
  - Réseaux informatiques ad-hoc
    - Ethernet non managé
    - Wifi
    - Ou commutateurs manageables, mais non sécurisés
  - Connectivité externe souvent peu maitrisée
    - Via modem et GPRS ; sans mots de passe (ou faibles)
    - Accès aux sites distants via Internet
    - VPN non compartimentés: accès à la totalité du SII

Mesures de sécurité

Un casse-tête pour une PME industrielle

- Intégration de la sécurité dans les SCADA/ICS
  - Suppose souvent des systèmes complets de générations homogènes
  - Ou repose sur la sécurisation de socles OS classiques
- Produits de filtrage de flux
  - Problèmes de positionnement : informatique classique ou protocoles industriels ?
  - Mesures statiques ou adaptables ?
  - Nécessite des compétences fortes d'intégration et une vue de haut niveau
- Outils pour l'authentification non adaptés
  - Monde industriel traditionnel
    - Pas d'authentification ou mot de passe partagé
    - La présence physique est preuve du droit d'accès
  - SI classique
    - Présume une authentification par mot de passe fort ou code personnel
    - Sessions fermées fréquemment
  - Que se passe-t-il quand l'industriel rencontre le *conventionnel* ?
- Mettre en œuvre correctement des mesures de sécurité industrielles :
  - Complexe : faute de compétences internes et disponibilités
  - Coûteux : intervenants externes ou dépendance aux fabriquants/intégrateurs

Cycles du monde industriel

La longue durée est la règle

- Un système mis en place pour 20 ans est la norme
  - Les automates, IHM, reporting doivent continuer à tourner
  - Plusieurs générations d'équipements se chevauchent souvent
  - Alignement fréquent sur le moins disant sécurité pour la rétro-compatibilité
- Gestion de version et configuration
  - Des programmes des automates
  - Des configurations physiques
  - Des configurations logicielles, systèmes et réseau
  - Nécessite une discipline forte pour permettre la gestion du changement
- Validation des changements
  - Les impacts peuvent être informatiques ou physiques.
  - Une plateforme de validation vraiment représentative est coûteuse, parfois impossible à monter
- *Reboot*
  - Redémarrer une installation industrielle n'est pas anodin
    - Perte d'activité
    - Redémarrages longs
    - Destruction dans certains cas
  - Les arrêts de maintenance doivent généralement être planifiés longtemps à l'avance

Les tiers

- Le monde industriel dépend fortement de tiers
  - Support et maintenance des équipements
  - Support des progiciels métier
  - Télé-opération de certains équipements (parfois loués)
- La tendance est à l'externalisation des fonctions hors cœur de métier
  - Donc la multiplication des tiers
  - Avec de plus en plus d'accès
- Une source de menace majeure
  - Quid de la PSSI, durcissement et conformité des postes tiers
  - Certains acteurs couvrent des pans entiers d'industrie
  - La compromission d'un mainteneur majeur d'installation industrielle est un scénario catastrophe

Points d'entrée des attaques 1/2

L'embarras du choix

- Réseaux interconnectés
  - Propagation virale sur des réseaux peu cloisonnés
  - Facteur d'amplification de tout risque :
  - Multi-dimensionnel
    - Verticalement: entre SII et SIE
    - Horizontalement: entre sites
- Médias
  - Clés USB multi-usages (bonus si personnelle)
  - Permet de contourner les *air-gaps*
  - Risque existant même si les numéros de série sont contrôlés
  - Combien d'organisation utilisent des stations de décontamination ?
- Gestion des mises à jour
  - Déploiement manuel
  - Complexité de validation des non-régressions
  - Mise à jour faites rarement (ou pas du tout)
  - Et pour les firmwares et programmes d'automates, le code n'est quasiment jamais signé
- Pratiques d'administration
  - Le poste d'un administrateur technique est rarement traité spécifiquement
  - Les bastions ou rebonds durcis sont rares

Points d'entrée des attaques 2/2

- Fragilité des implémentations
  - Les piles réseau des automates sont traditionnellement fragiles
    - N'affecte souvent pas le fonctionnement
    - Mais opérez-vous votre usine si vous perdez la supervision ?
  - Les logiciels de contrôle, IHM et supervision ont une tradition d'identifiants statiques, impossibles à changer.
    - Qui va redémarrer une usine parce qu'un mot de passe est sur Internet ?
- Contrôle d'accès
  - Les logiques de contrôles d'accès du SIE sont rarement adaptées
  - Il n'existe que peu de systèmes de contrôle d'accès et d'authentification adaptés à des postes de contrôle
- Accès des tiers
  - Peu de contrôle sur ce que font vos fournisseurs

Évolution de l'exposition

Vers l'infini et au-delà

- Décloisonnement
  - L'usine numérique: intégration SII/SIE
  - Contrôle des systèmes industriels depuis appareils mobiles : déjà commercialisé
  - Équipements disposant de leur propre connexion 3G
- "Commoditisation"
  - Convergence vers des systèmes du monde bureautique
  - Disponibilité de l'information sur Internet
  - Fin de "l'exotisme" des systèmes industriels
- Le "tout intelligent"
  - Multiplication des appareils intelligents
  - Télémétrie généralisée
  - Interactions devenant de plus en plus complexes

Traitement technique des exigences LPM

Un équilibre complexe pour les petits OIV

- La situation
  - Une croissance ”organique” des réseaux
  - Des vues très différentes entre DSI et Automaticiens
  - Souvent tout repose sur quelques acteurs
  - Une vision globale complexe, souvent parcellaire, rarement à jour
- Travail demandé à ce stade
  - Inventaire SI
  - Architecture à jour
  - Élaborer une proposition de SIV
- Ces tâches sont déjà lourdes
  - Peut impliquer des réorganisations réseau significatives
  - Chantiers couteux et sans rentabilité à court terme

Méthode de classification du guide de cybersécurité des systèmes industriels

Sommaire

Guide de cybersécurité des systèmes industriels

- Micro-analyse de risques
- Classification de systèmes industriels en 3 niveaux
- Règles de sécurité ou recommandations selon les niveaux
- Censé être utilisé pour définir les modalités d'application des mesures de la LPM
- Peut être utilisé en attendant la parution des textes industriels
- Limitation : ne s'applique qu'aux SI industriels

Guide de cybersécurité des systèmes industriels

Menaces considérées

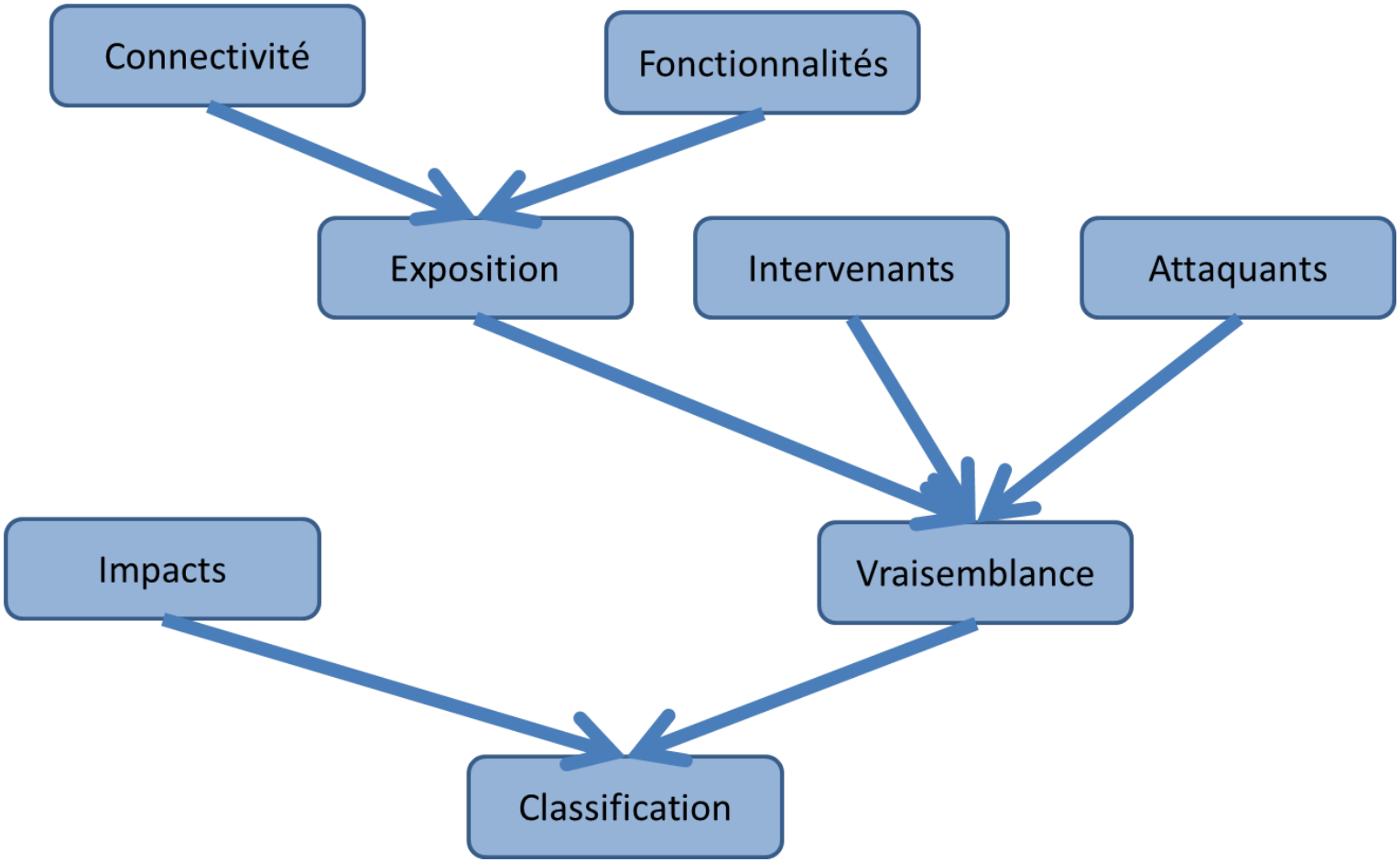
- Malveillance interne
- Attaques extérieures
- Pas les menaces accidentelles

Guide de cybersécurité des systèmes industriels

Utilisation dans le cadre de la LPM

- Utilisation de la méthode de classification pour déterminer quels sont les SIV
- Hypothèses possibles
  - Utilisation de l'échelle des impacts pour déterminer si un SI est d'importance vitale
  - Avoir une vision des mesures de sécurité potentiellement imposées par les arrêtés sectoriels
  - Sachant qu'il faut les adapter au secteur (analyse d'impact nécessaire)

Classification des systèmes industriels



Classification

Impacts

- Impacts humains
- Impacts environnementaux
- Impacts consécutifs à l'arrêt du service rendu

- Seuls critères pris en compte : disponibilité et intégrité
- Pas de prise en compte des conséquences pour l'organisme (réputation, chiffre d'affaires...)
- SIV : Impact minimum de 3 pour être conforme à la définition donnée par la LPM

Conclusion

Sommaire

Conclusion

Contexte

- Systèmes de moins en moins opérables à la main
- Modes dégradés manuels souvent uniquement théoriques
- Grands OIV favorisés
  - Structure sécurité existante : ne partent pas de zéro
  - Chaine d'interlocuteurs connue et rodée
  - Calendrier mouvant
- Volonté d'une démarche acceptée et soutenable par les différents acteurs
  - Règles adaptés aux différents secteurs
  - Groupes de travail

Conclusion

Perspectives

- Nécessité de passer par des étapes d'inventaire, d'évaluation de la connectivité et des intervenants
- Appréciation des risques SSI nécessaire
- Pour les petits OIV
  - Probablement nombreuses règles et nombreuses étapes préliminaires
  - Besoin de conseil pour ces étapes et pour la mise en oeuvre des règles
  - Coût important
  - Risque de retard important, mais sanctions pénales
- Pour les prestataires
  - Probable extension du référentiel PASSI aux systèmes industriels
  - Forte diversité des OIV
  - Difficultés à obtenir des informations concrètes
  - Coopération des prestataires (mise en oeuvre et audit) souhaitable

Conclusion

Questions ?

Merci de votre attention.

HSC by Deloitte

Conseil en sécurité des systèmes d'information depuis 1989

- PME française avec 26 ans d'expérience
- Exclusivement des interventions d'expertise SSI
  - Pas de distribution, ni intégration, ni infogérance, ni délégation de personnel
  - Prestations : conseil, études, audits, tests d'intrusion, formations
  - Garantie d'indépendance
- Domaines d'expertise
  - Sécurité Windows / Unix et linux / embarqué / informatique industrielle / applications
  - Enquêtes inforensiques / Expertise judiciaire
  - Sécurité des réseaux : TCP/IP, téléphonie, réseaux opérateurs, réseaux industriels...
  - Organisation de la sécurité, droit des systèmes d'information

HSC by Deloitte

Certifications

- Des consultants (certifications individuelles)
  - CISSP (ISC)2
  - CISA
  - PCI DSS QSA
  - ISO 27001 LI / LA et ISO 27005 Risk Manager par LSTI
  - EBIOS Risk Manager par LSTI
  - ISO 22301 LI / LA par LSTI
  - OCSP
  - GIAC: GCFA, GPEN, GWAPT, GCFE GREM, GWEB, GXPN, GCUX, GSEC
- De la société
  - PASSI
  - Organisme certificateur ARJEL
  - OPQF, OPQCM (habilité au conseil juridique)
  - SMQ ISO 9001 sur les formations
  - Expert judiciaire
  - PCI DSS

Intervenants

- Béatrice Joucreau
  - Diplômée ENSIIE, et de l'Université de Manchester, en Sécurité des Systèmes d'Information et en Management et Administration des Entreprises à l'Ecole de Management de Strasbourg
  - Intègre HSC en 2012
  - Intervient depuis sur des missions de sécurité organisationnelle de conseil et d'audit: l'analyse de risques, accompagnement à la mise en place de SMSI, audits de SMSI
  - Certifiée ISO 27001 Lead Auditor, ISO 27001 Lead Implementer et ISO 27005 Risk Manager par LSTI, et GIAC Security Essentials (GSEC)
- Christophe Renard
  - Exerce dans le domaine des réseaux et systèmes depuis 1997 dans les domaines des télécommunications, des FAI, de la veille technologique et de défense. Précédemment architecte et expert en France et au Moyen-Orient sur systèmes critiques
  - Rejoint HSC en 2011
  - Travaille sur la mise en oeuvre de la sécurité informatique : architecture, dans le développement, dans le domaine industriel
  - Certifié ISO 27005 Risk Manager, ISO 27001 Lead Auditor et ISO 27001 Lead Implementer par LSTI, et GIAC Security Essentials (GSEC) et GIAC Web Applications Defender (GWEB)

La LPM pour un petit OIV

Bibliographie 1/5

- Références légales et règlementaires
  - Définition OIV
    - Legifrance Code de la Défense Article R1332-1
      http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006574323
  - Définition SAIV
    - Legifrance Code de la Défense Article R1332-2
      http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006574324
  - Définition PIV et ZIV
    - Legifrance Décret 2006-212 du 23 février 2006
      http://www.legifrance.gouv.fr/eli/decret/2006/2/23/2006-212/jo/texte
  - Composition et rôle du comité national des SAIV
    - Legifrance Code de la Défense Articles R1332-7 et suivants, abrogé le 19 février 2014
      http://legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FFCF574DB1409D59119974560FB7452.tpdila18v_1?idArticle=LEGIARTI000021544838&cidTexte=LEGITEXT000006071307&dateTexte=20140218
  - Composition et rôle de la commission interministérielle de défense et de sécurité des SAIV
    - Legifrance Code de la Défense Articles R1332-10 et suivants
      http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000021544835
  - Composition et rôle de la commission zonale de défense et de sécurité des SAIV
    - Legifrance Code de la Défense Articles R1332-13 et suivants
      http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006574336

La LPM pour un petit OIV

Bibliographie 2/5

- Références réglementaires et référentiels ANSSI
  - Instruction Interministérielle 6600
    - Legifrance 07/01/2014
      `http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf`
  - Loi de Programmation Militaire 2014-2019 - Loi Numéro 0294 du 19 Décembre 2013
    - Legifrance
      `http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id`
  - Instruction Interministérielle 901 du 28/01/2015
    - Legifrance
      `http://circulaires.legifrance.gouv.fr/index.php?action=afficherCirculaire&hit=1&retourAccueil=1&r=39217`

La LPM pour un petit OIV

Bibliographie 3/5

- Communications ANSSI
  - 29/04/2013 - Livre blanc sur la défense et la sécurité nationale
    - http://www.livreblancdefenseetsecurite.gouv.fr/
  - 16/04/2013 - Publication de la stratégie de la France en matière de cyberdéfense (datant de 2011)
    - http://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite/
  - 20/02/2014 - Publication de la politique de la France en matière de cybersécurité
    - http://www.ssi.gouv.fr/uploads/IMG/pdf/dossier_de_presse_web_20140220.pdf
  - 09/04/2014 - Début officiel des travaux sur les décrets d'application de la LPM
    - http://www.ssi.gouv.fr/actualite/lanssi-sattele-aux-decrets-dapplication-de-la-lpm-portant-sur-la-protection-des-ope
  - 28/07/2014 - Appel à commentaires sur le référentiel PRIS
    - http://www.ssi.gouv.fr/actualite/appel-public-a-commentaires-sur-le-referentiel-dexigences-applicables-aux-prestatai
  - 28/10/2014 - Annonce des premiers groupes de travail
    - http://www.ssi.gouv.fr/actualite/cybersecurite-et-loi-de-programmation-militaire-preparation-des-regles-de-securite/
  - 16/01/2015 - Appel à commentaires sur le référentiel PDIS
    - http://www.ssi.gouv.fr/actualite/appel-public-a-commentaires-sur-le-referentiel-dexigences-applicables-aux-prestatai

La LPM pour un petit OIV

Bibliographie 4/5

- Guides et recommandations ANSSI
  - La cybersécurité des systèmes industriels
    - http://www.ssi.gouv.fr/guide/la-cybersecurite-des-systemes-industriels/
  - Recommandations de bonnes pratiques
    - http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/
  - Profils de protection pour les systèmes industriels
    - http://www.ssi.gouv.fr/guide/profils-de-protection-pour-les-systemes-industriels/
- Référentiels ANSSI
  - Prestataire Audit de Sécurité des Systèmes d'Information
    - Référentiel PASSI
      http://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_C.pdf
  - Prestataires de Réponses aux Incidents de Sécurité
    - Présentation du référentiel PRIS
      http://www.ossir.org/paris/supports/2014/2014-10-14/Presentation_OSSIR_-_Referentiel_Reponse_Incidents_de_Securite_-_14_octobre_2014.pdf
    - Projet de référentiel PRIS
      http://www.ssi.gouv.fr/actualite/appel-public-a-commentaires-sur-le-referentiel-dexigences-applicables-aux-prestatai
  - Prestataires de Détection des Incidents de Sécurité
    - Projet de référentiel PDIS
      http://www.ssi.gouv.fr/actualite/appel-public-a-commentaires-sur-le-referentiel-dexigences-applicables-aux-prestatai

La LPM pour un petit OIV

Bibliographie 5/5

- Normes et standards
  - ISA-95
    - http://isa-95.com/
  - ISO/ISA 62443 (ex ISA-99)
    - http://isa99.isa.org/ISA99%20Wiki/Home.aspx
  - Clusif - Cybersécurité des systèmes industriels: Par ou commencer ? Panorama des référentiels
    - http://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-2014-SCADA-Panorama-des-referentiels.pdf
- Presse
  - Attaque sur le pipeline BTC, Bloomberg 10/12/2014
    - http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar
  - Attaque sur une fonderie Allemande, Bundesamt fur Sicherheit in der Informationstechnik 21/01/2015
    - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf
  - Attentat contre le réseau électrique pakistanais 26/01/2015
    - http://www.bbc.com/news/world-asia-30981338