Setting the Standard for Automation™

France

Processus et normes de cybersécurité dans l'industrie L'IEC 62443

Jean-Pierre HAUET
Président ISA-France

CAP'TRONIC
Strasbourg –5 octobre 2016

Sécurité fonctionnelle et cybersécurité

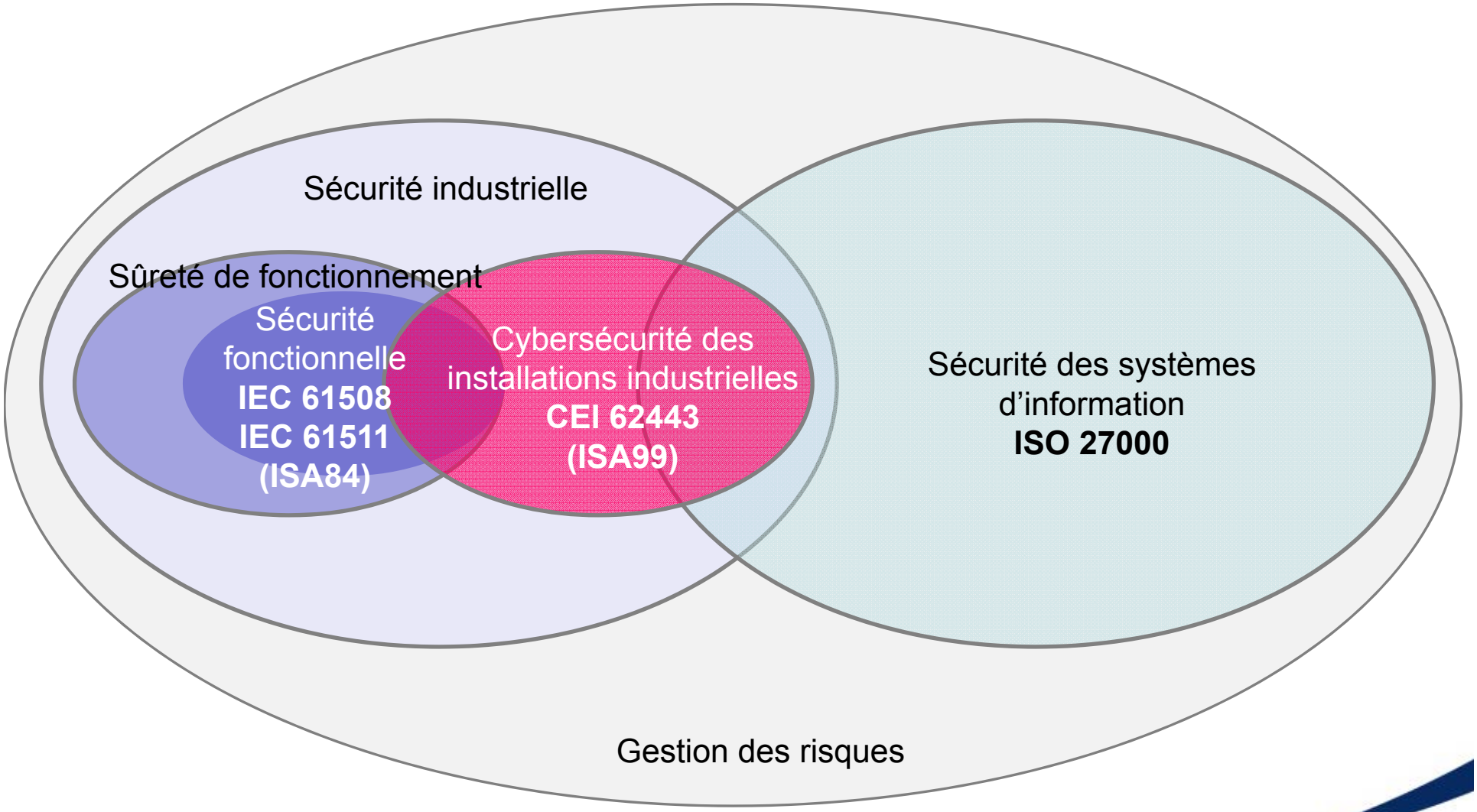
- **Sécurité fonctionnelle** (**functional safety) :** *Sous-ensemble de la sécurité globale, relatif aux équipements et aux systèmes de contrôle-commande associés, qui dépend du fonctionnement correct de systèmes électriques, électriques, programmables électroniques (E/E/PE) concernés par la sécurité*

  ➔ IEC 61508, ISA-84, IEC 61511 et normes sectorielles

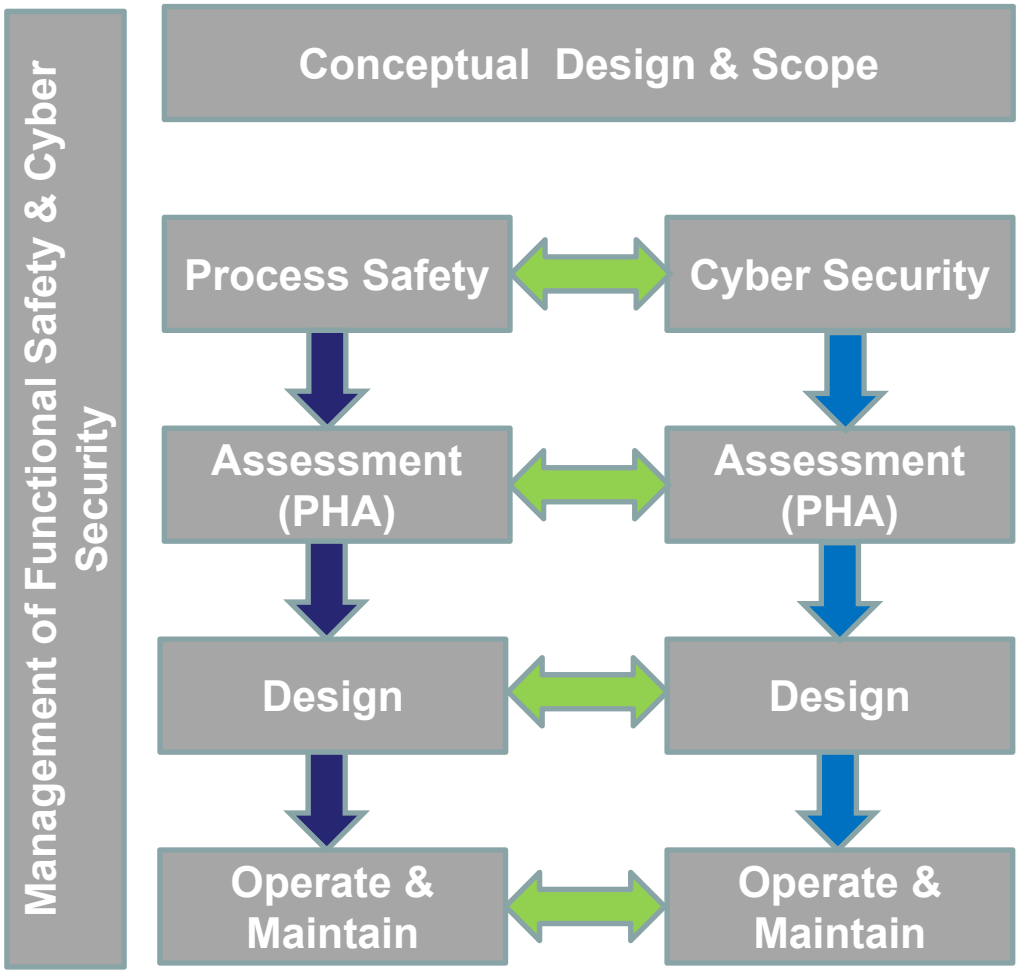
- **Cybersécurité des installations industrielles :** *Sous-ensemble de la sécurité globale ayant trait à la prévention des risques associés aux intrusions dans un système d'automatisme ou de contrôle (IACS : Industrial Automation and Control System), liés à de possibles actions malintentionnées sur des équipements informatiques, des réseaux de communication, des logiciels ou des données*

  ➔ IEC 62443, ISA-99, ISO 27000

La cybersécurité : une nouvelle branche de la sécurité industrielle



Sûreté de fonctionnement et cybersécurité doivent être analysées concurremment



Source : ISA-TR84.00.09

Nota : Le cycle de vie porte en sûreté de fonctionnement sur le SIS alors qu'il porte sur l'ensemble de l'installation (SUC) en cybersécurité

Etablir un système de gestion de la cybersécurité

Un système de gestion de la cybersécurité doit être :

- Global : personnel, organisation, technologie
- Cohérent avec les autres aspects de la sécurité :
  - Sécurité des systèmes d'information
  - Sécurité fonctionnelle (CEI 61508 et normes dérivées)
- Economiquement raisonnable : coût des contre-mesures proportionné aux risques encourus
- Soutenable dans le temps
- Adapté aux données particulières d'une entreprise ou d'une installation donnée

Un référentiel normatif permet de :

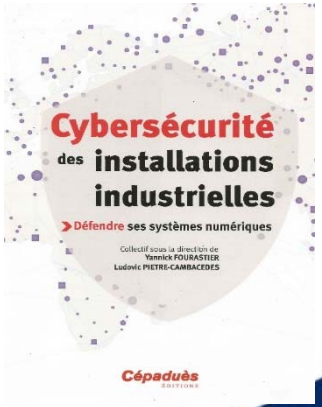
- Introduire de la « rationalité » dans un domaine très subjectif
- Etre davantage certain de ne rien oublier (éviter de se focaliser sur les points que l'on sait traiter)
- Etre homogène dans les évaluations

L'IEC 62443 (ex ISA99)

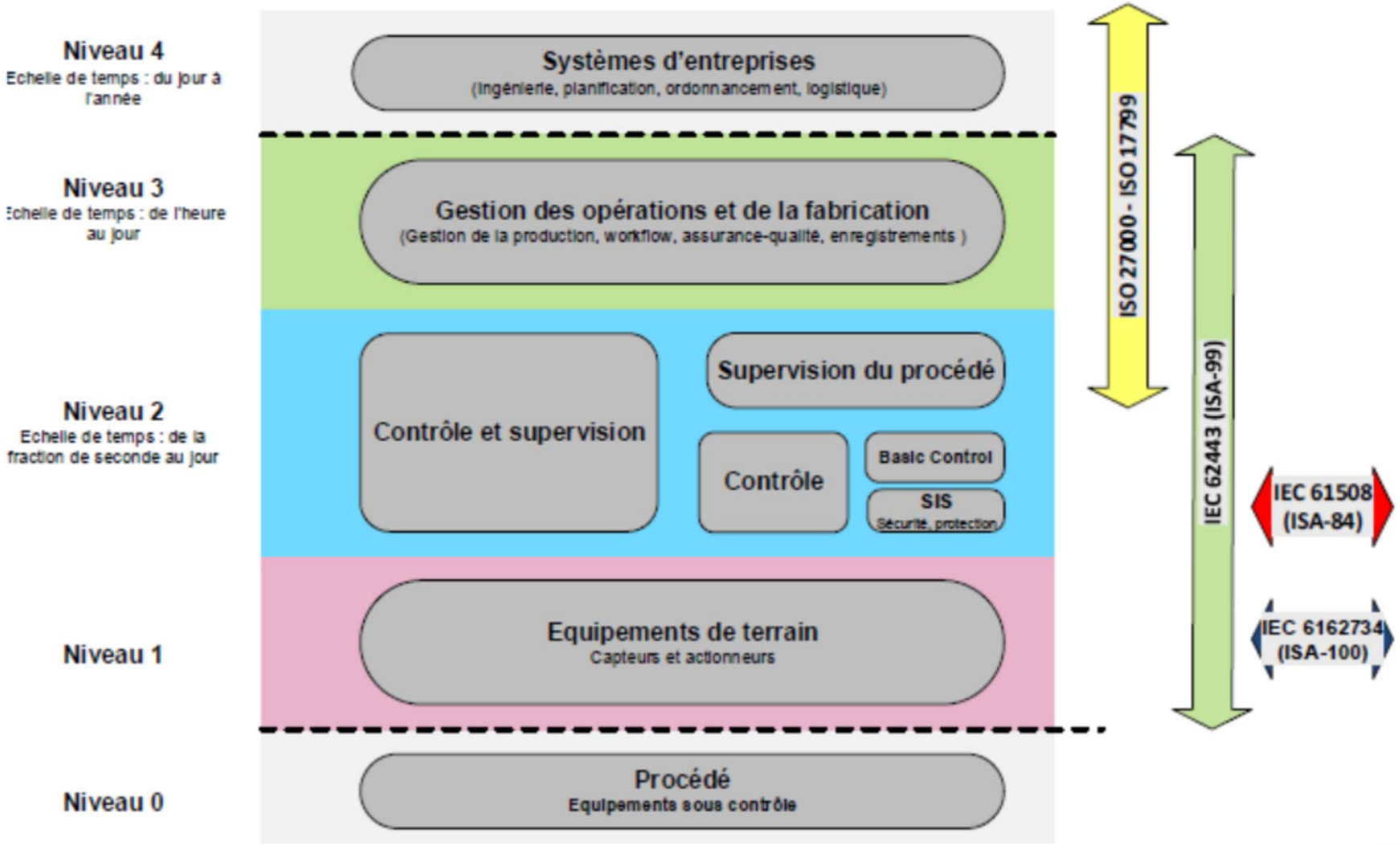
Projet né des travaux de l'ISA (International society of Automation – Comité ISA99) visant à :

- Définir un référentiel normatif applicable à tous les systèmes industriels d'automatisme et de contrôle (IACS)
- S'appuyant sur les normes reconnues en matière de cybersécurité des systèmes d'information mais prenant en compte les spécificités des systèmes industriels
- Prenant en compte les points de vue des diverses parties prenantes dans la conception, le développement, l'intégration, l'exploitation des IAC

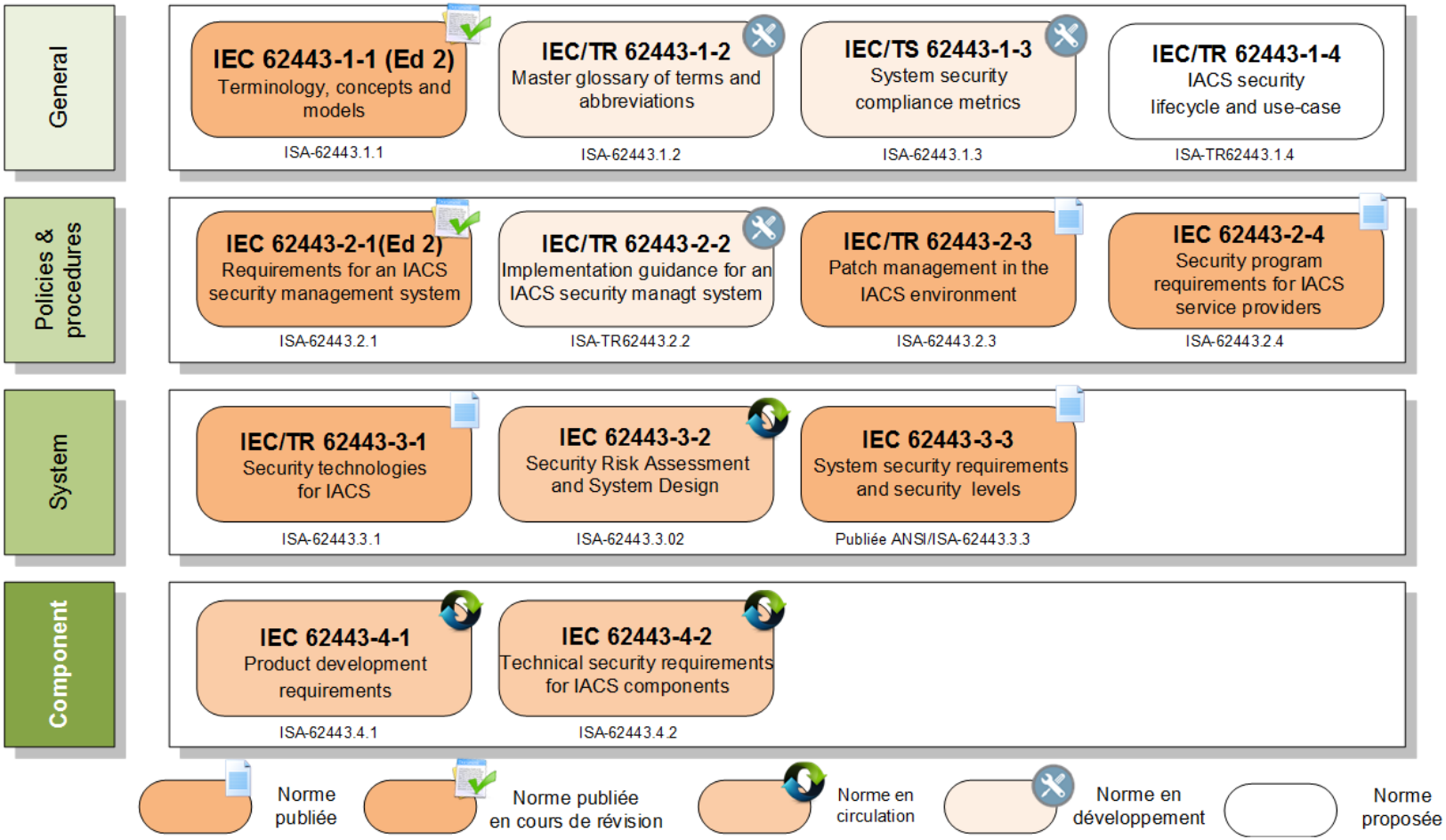
« L'IEC 62443 présente une position centrale dans les échanges entre acteurs des SNI (Systèmes numériques industriels). Elle est le seul référentiel à portée internationale avec l'ambition d'être multisectorielle… »



Situation du standard IEC 62443 vis-àvis des principales normes de sécurité

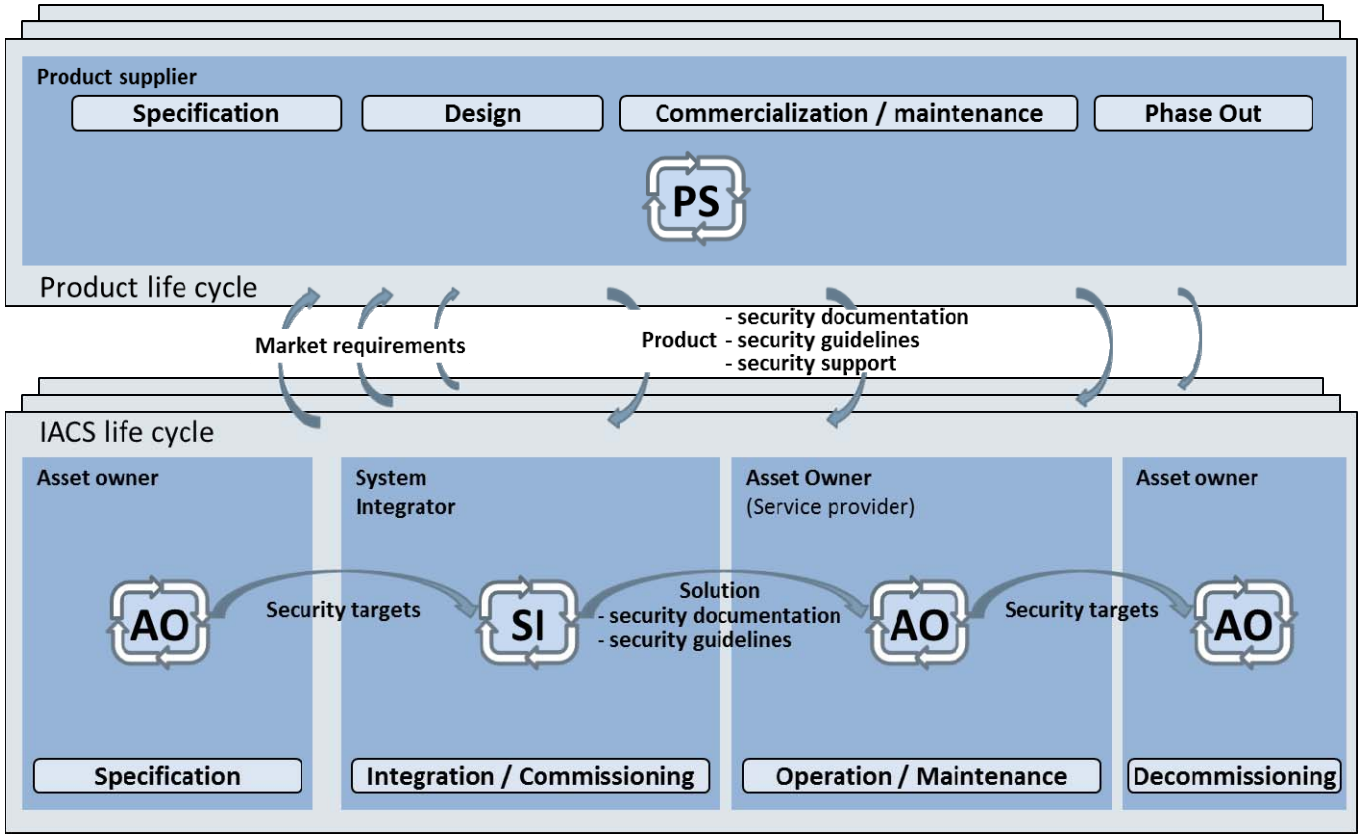


Structure documentaire de l'IEC 62443



Cybersécurité et cycles de vie : standards applicables

Cycle de vie produits (composants et systèmes)



Cycle de vie IACS (installations)

Background commun

IEC 62443-1-1
IEC TR62443-3-1

Produits

IEC 62443-2-3
IEC 62443-3-1
IEC 62443-3-3
IEC 62443-4-1
IEC 62443 4-2

IACS

Spécifications

IEC 62443-2-1
IEC 62443-2-3
IEC 62443-3-2

Integration & commissionin

IEC 62443-1-3
IEC 62443-2-4
IEC 62443-3-2
IEC 62443-3-2
IEC 62443-3-3

Operation & maintenance

IEC 62443-2-1
IEC 62443-2-3
IEC 62443-2-4
IEC 62443-3-2
IEC 62443-3-3

Les concepts essentiels de l'IEC 62443

- Processes (policies, procedures et guidelines)
- Technology
  - Foundational requirements (FR)
  - Zones & conduits
  - Security levels (SLs)
- Maturity

Policies, procedures & guidelines

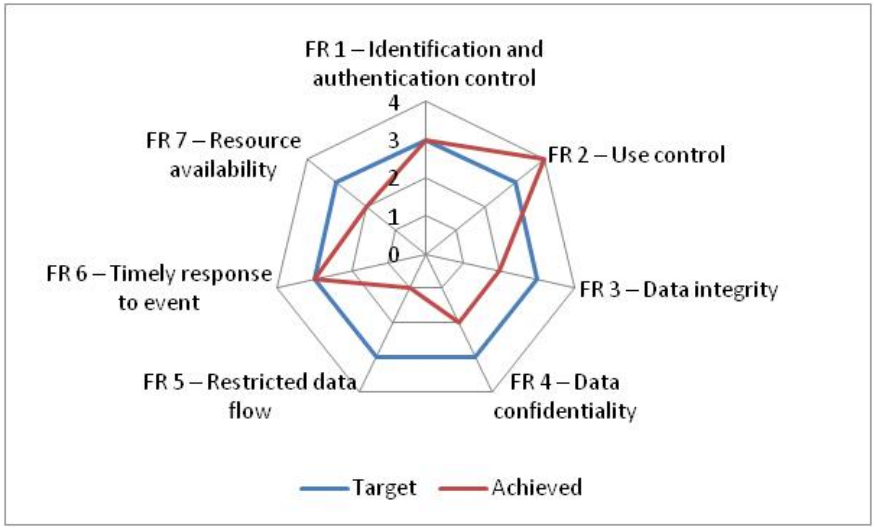
- L'IEC 62443-2-1 organise la démarche selon les 11 catégories issues de l'ISO 27002 et adaptées au cas des IACS

1	Security Policy	**7**	Access Control
2	Organization of Security	8	Systems acquisition, development and maintenance
3	Asset Management	9	Incident Management
4	Human Resources Security	10	Business Continuity Management
5	Physical and Environmental Security	11	Compliance
6	Communications and Operations Management		

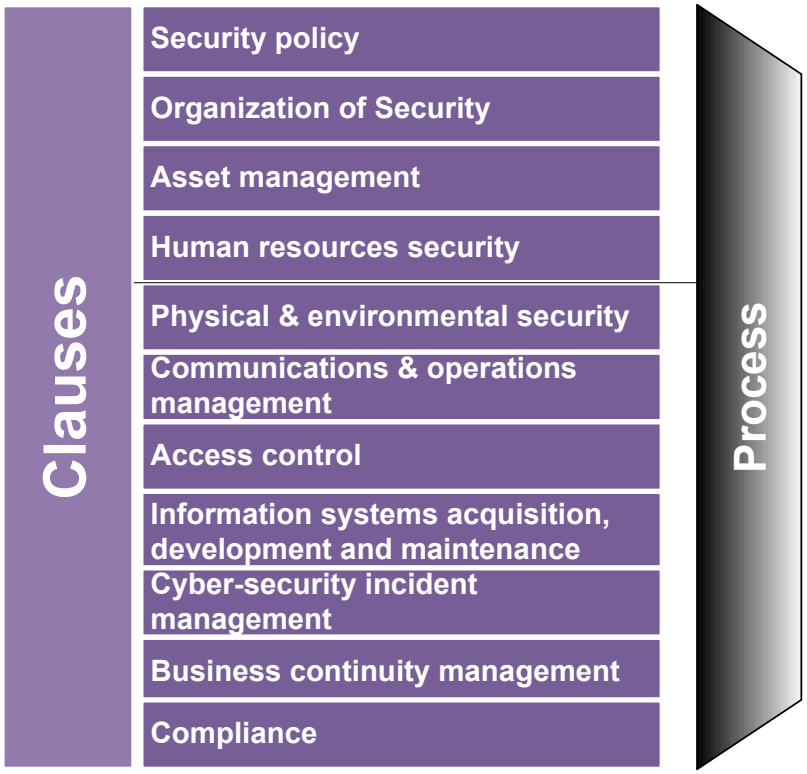
L'approche technique : les sept « Foundational Requirements »

FR1	Identification, authentication control and access control (AC)	FR5	Restrict data flow (RDF)
FR2	Use control (UC)	FR6	Timely response to events (TRE)
FR3	Data Integrity (DI)	FR7	Resource availability (RA)
FR4	Data confidentiality (DC)		

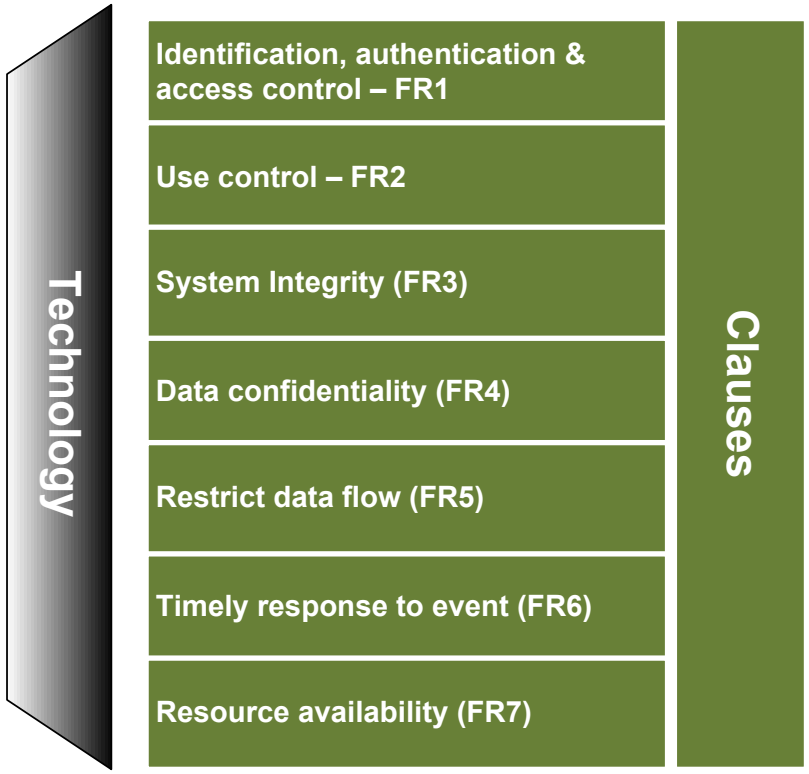
- IEC 62443-3-3 donne une liste de critères techniques permettant de situer le « Security level » d'un système dans une échelle de 0 à 4, au regard de chacun des FR, en «capability » ou en « achieved », (à comparer aux niveaux « target »)



Exigences organisation et exigences techniques



IEC 62443-2-1 (dérivée de ISO 27002) : process



IEC 62443-3-3 et IEC 62443-4-2: technology

Cinq niveaux de sécurité pour chaque zone

- **SL 0 :** Protection inférieure au niveau 1
- **SL 1** : Protection contre des violations usuelles ou de pure coïncidence
- **SL 2 :** Protection contre des violations intentionnelles utilisant des ressources simples
- **SL 3 :** Protection contre de violations intentionnelles utilisant des moyens sophistiqués
- **SL 4 :** Protection contre de violations intentionnelles utilisant des ressources très étendues

Format des vecteurs SLs

Achieved : $SL-A(BPCS\,Zone)=\{2,3,3,2,3,3,3\}$

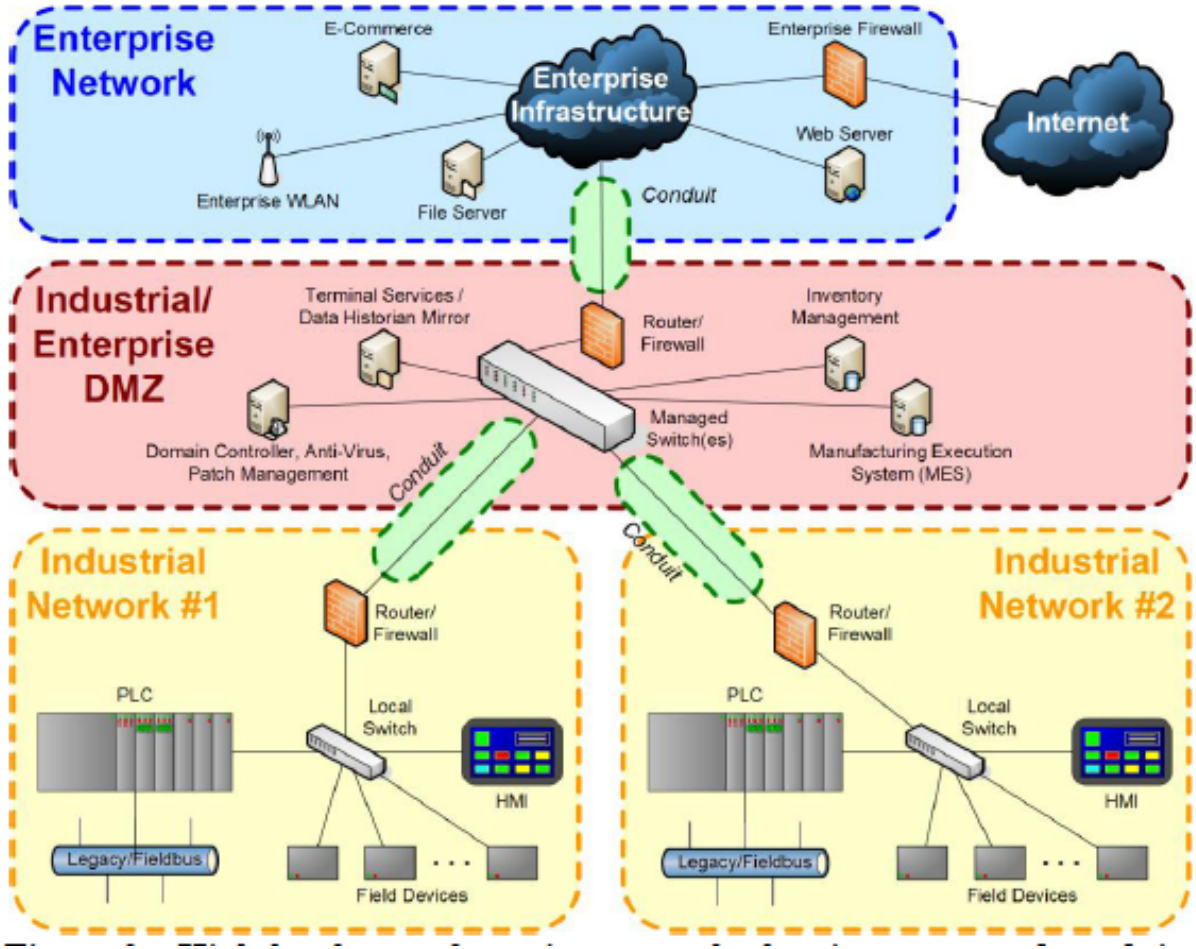
Capability : $SL-C(SIS\,Zone)=\{4,3,3,4,3,3,3\}$

Target : $SL-T(RA,FS-PLC)=4$

Dans ce dernier exemple, seule l'exigence RA fait l'objet d'un SL-T

Zones et conduits

Exemple d'une entreprise disposant de deux ateliers de fabrication indépendants



Source : NIST 2010

Déterminer les niveaux de sécurité objectifs

- Le rapport entre le niveau de risque non mitigé et le niveau de risque tolérable détermine le niveau de sécurité à assigner à chacune des zones
  Risques non mitigés/risque tolérable ➔ SL- T (targets).
- Les SL-T sont une expression du degré de sécurité à implémenter dans chaque zone pour ramener le risque initial au niveau considéré comme acceptable

		Criticité des conséquences			
		Pas d'impact	Mineure	Majeure	Très sévère
Probabilité	Haute	Risque moyen	Risque élevé	Risque très élevé	Risque très élevé
	Moyenne	Risque moyen	Risque élevé	Risque très élevé	Risque très élevé
	Faible	Risque faible	Risque moyen	Risque moyen	Risque élevé
	Très faible	Risque faible	Risque faible	Risque moyen	Risque élevé

Attention : Dans le choix des SL-T, tenir compte du coût des contre-mesures (itération nécessaire)

Niveau de risque et SL correspondant		Criticité des conséquences			
		Pas d'impact	Mineure	Majeure	Très sévère
Probabilité	Haute	SL-T 2	SL-T 3	SL -T 4	SL -T 4
	Moyenne	SL-T 2	SL-T 3	SL -T 4	SL -T 4
	Faible	SL-T 1	SL-T 2	SL-T 2	SL-T 3
	Très faible	SL-T 1	SL-T 1	SL-T 2	SL-T 3

L’évaluation des niveaux de sécurité atteints

Le document IEC-62443.03.03 définit les exigences système (SE : System requirement) à remplir, pour atteindre un niveau donné (de 1 à 4) du vecteur SL-C, au regard de chacun des sept Foundational Requirements

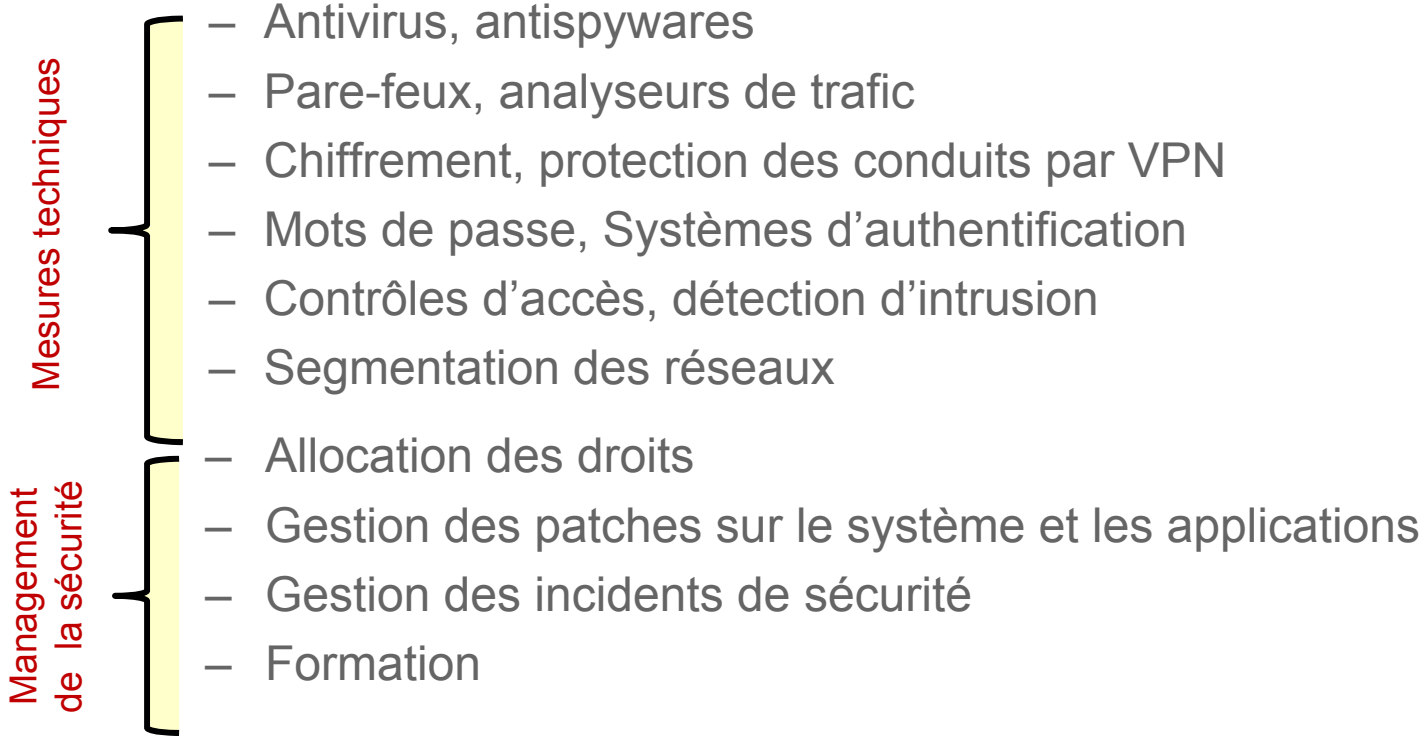
- Chaque « System requirement » (SR) comporte une « baseline » commune à tous les niveaux de SL et des Requirement Enhancements (RE) qui doivent être satisfaits pour passer aux niveaux supérieurs de SL.
- Le tableau qui suit donne à titre d’exemple, la correspondance entre les SR (baseline et RE) et les niveaux SL correspondant à la première exigence fondamentale (Contrôle de l’identification et authentification)

Mapping entre les SR et les RE dans le cas de l'exigence FR1 (extrait)

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
RE (2) Multifactor authentication for untrusted networks			✓	✓
RE (3) Multifactor authentication for all				✓
SR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓
SR 1.3 – Account management	✓	✓	✓	✓
RE (1) Unified account management			✓	✓
SR 1.4 – Identifier management	✓	✓	✓	✓

Stratégie de protection
Les contre-mesures

- En cas de non-concordance entre les SL-A et les SL-T des contre-mesures sont nécessaires (ISA TR62433-3-1)



➔Eventuellement, reconsidération de l'architecture système

Setting the Standard for Automation™

France

Application au cas de l'attaque contre les réseaux électriques ukrainiens 23 décembre 2015

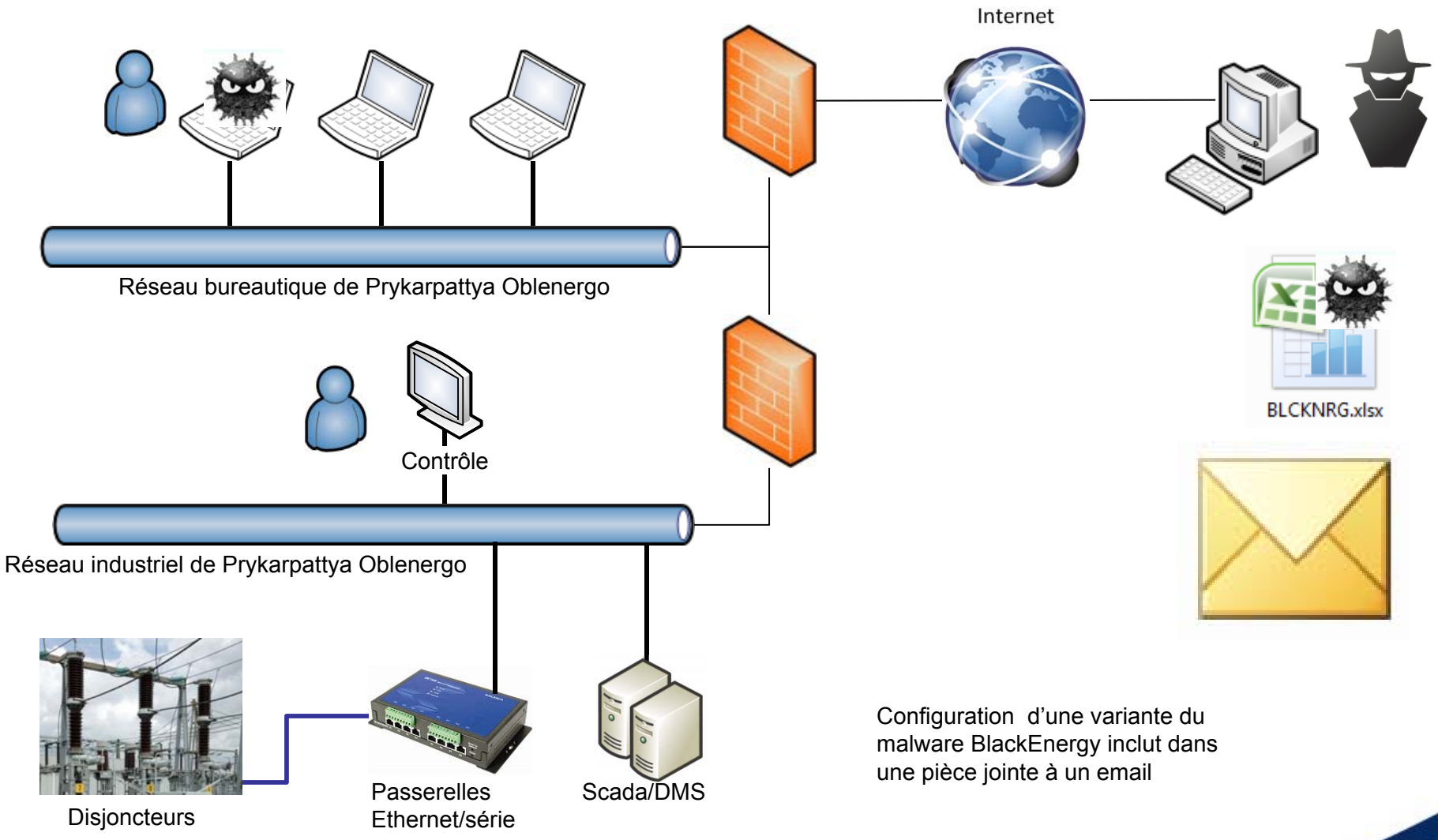
Analyse effectuée par Patrice Bock – ISA-France

CAP'TRONIC
Strasbourg –5 octobre 2016

Déroulement de l'attaque sur le réseau électrique ukrainien, le 23 décembre 2015

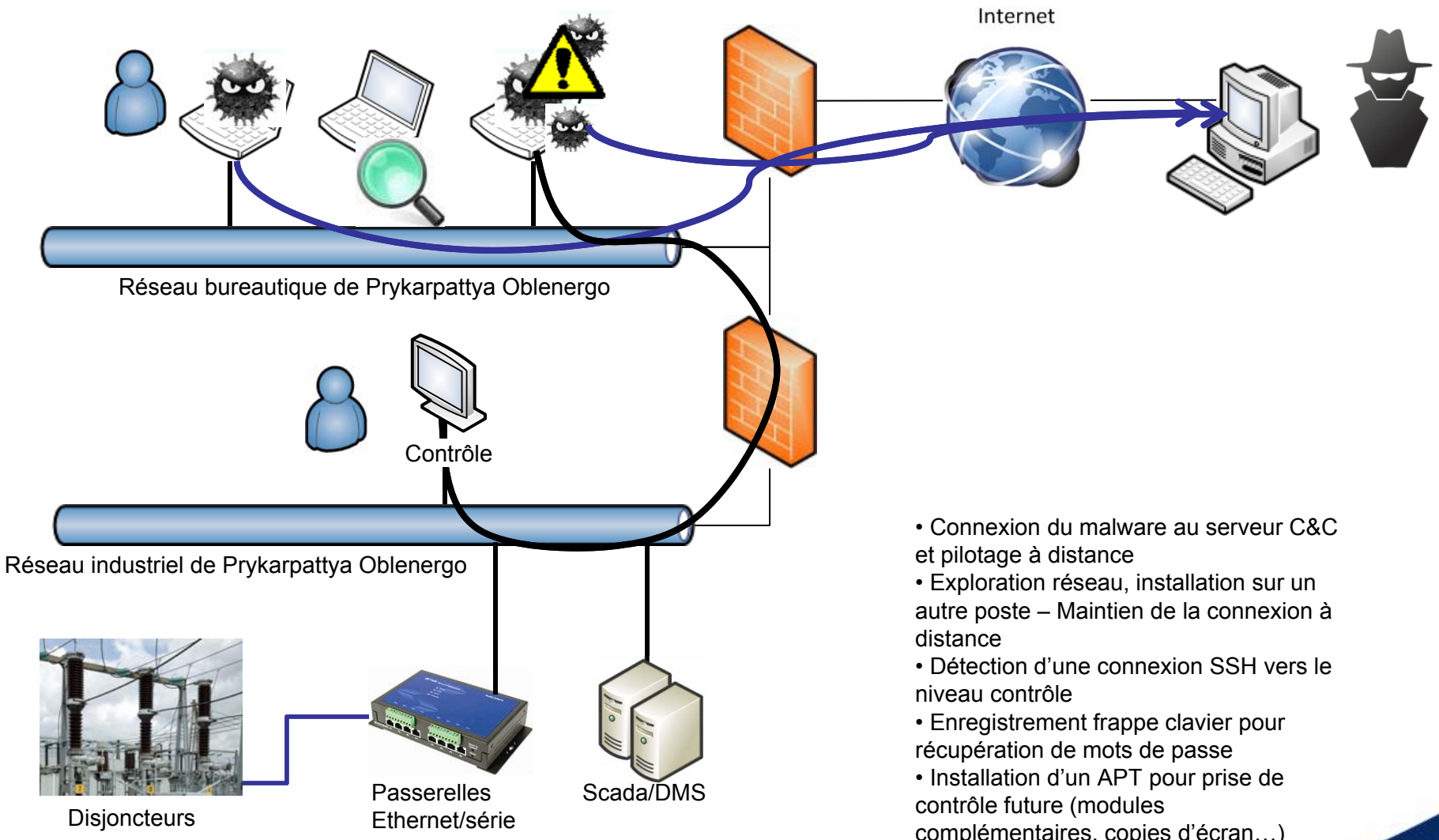
- Un PC de bureautique disposant d'un accès VPN (SSH) vers un poste de conduite du réseau industriel est compromis :
  - Infection préparée avant l'été 2015, fondée sur une variante de BlackEnergy insérée dans une pièce jointe Microsoft Office envoyée par email (spear phishing)
  - Installation du malware qui se connecte, se repère et prend ses ordres à distance auprès des hackers qui l'ont introduit
- Le jour J :
  - Accès à distance, via le PC compromis, aux postes de contrôle du réseau
  - Activation des disjoncteurs via ces postes (d'abord sous les yeux des opérateurs, puis déconnection opérateur local et changement mot de passe)
  - Effacement des firmwares des passerelles séries faisant la liaison avec les disjoncteurs
  - Effacement plus ou moins complet des disques durs des postes de conduite
  - Désactivation des UPS – Control room dans le noir
  - Saturation de la plate-forme téléphonique du service clients
  - Rétablissement manuel du service par des équipes envoyées sur place

Déroulement de l'attaque
1) compromission d'un poste bureautique



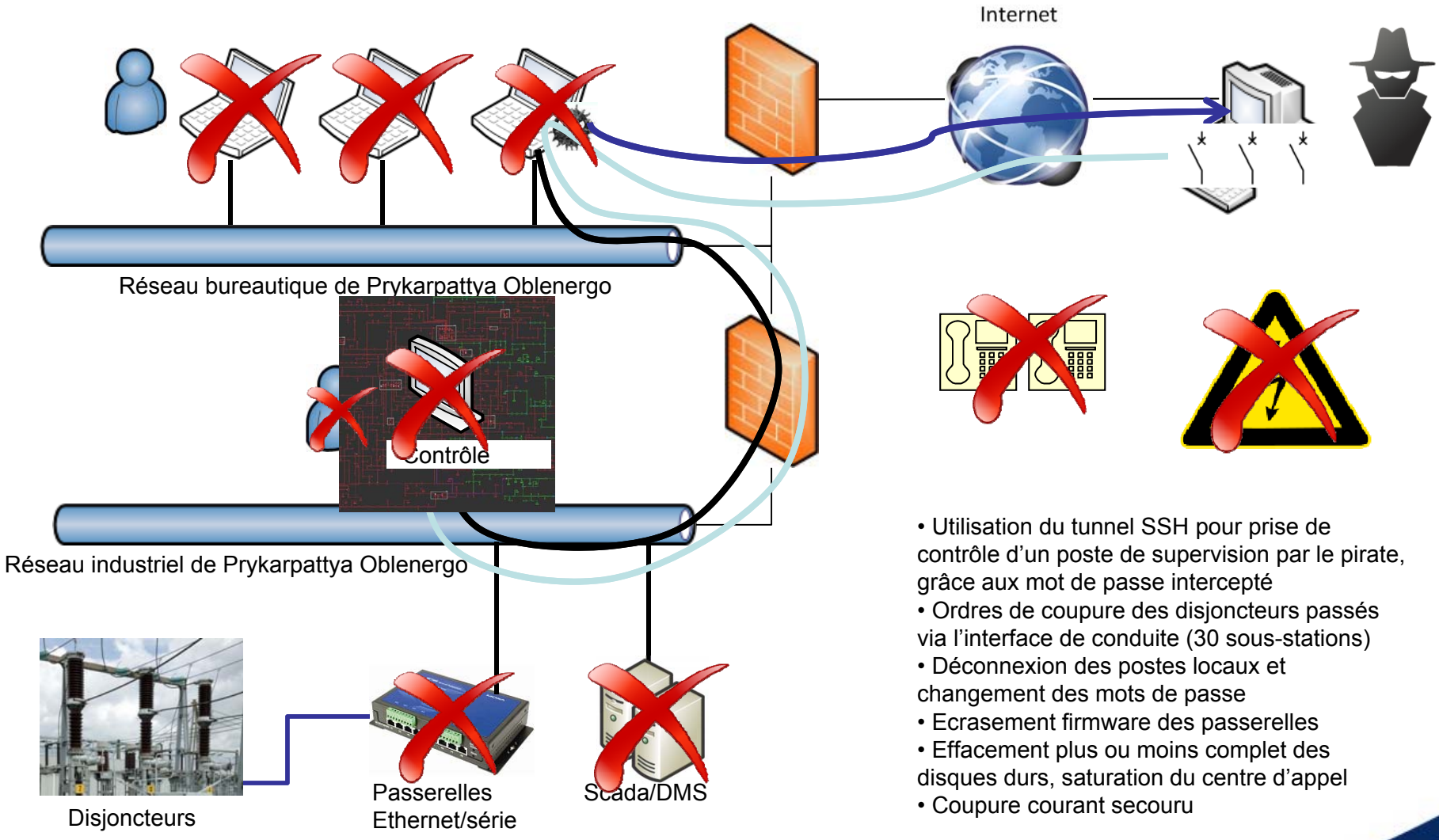
Configuration d'une variante du malware BlackEnergy inclut dans une pièce jointe à un email

Déroulement de l'attaque
2) préparation de l'attaque été 2015



- Connexion du malware au serveur C&C et pilotage à distance
- Exploration réseau, installation sur un autre poste – Maintien de la connexion à distance
- Détection d'une connexion SSH vers le niveau contrôle
- Enregistrement frappe clavier pour récupération de mots de passe
- Installation d'un APT pour prise de contrôle future (modules complémentaires, copies d'écran…)

Déroulement de l'attaque
3) déclenchement le 23 décembre 2015



- Utilisation du tunnel SSH pour prise de contrôle d'un poste de supervision par le pirate, grâce aux mot de passe intercepté
- Ordres de coupure des disjoncteurs passés via l'interface de conduite (30 sous-stations)
- Déconnexion des postes locaux et changement des mots de passe
- Ecrasement firmware des passerelles
- Effacement plus ou moins complet des disques durs, saturation du centre d'appel
- Coupure courant secouru

Tentative d’évaluation du système ukrainien au regard de la norme IEC 62443-3-3

Functional Requirement (FR) et Security Requirements associés (SRs) – Cas du FR5

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 5 – Restricted data flow (RDF)				
SR 5.1 – Network segmentation	✓	✓	✓	✓
RE (1) Physical network segmentation		✓	✓	✓
RE (2) Independence from non-control system networks			✓	✓
RE (3) Logical and physical isolation of critical networks				✓
SR 5.2 – Zone boundary protection	✓	✓	✓	✓
RE (1) Deny by default, allow by exception		✓	✓	✓
RE (2) Island mode			✓	✓
RE (3) Fail close			✓	✓
SR 5.3 – General purpose person-to-person communication restrictions	✓	✓	✓	✓
RE (1) Prohibit all general purpose person-to-person communications			✓	✓
SR 5.4 – Application partitioning	✓	✓	✓	✓

RE : Requirement Enhancement

Evaluation

SRs and REs	SL 1	SL 2	SL 3	SL 4	Audit
FR 5 – Restricted data flow (RDF)					
SR 5.1 – Network segmentation	✓	✓	✓	✓	✓
RE (1) Physical network segmentation		✓	✓	✓	✓
RE (2) Independence from non-control system networks			✓	✓	✓
RE (3) Logical and physical isolation of critical networks				✓	✗
SR 5.2 – Zone boundary protection	✓	✓	✓	✓	✓
RE (1) Deny by default, allow by exception		✓	✓	✓	✓
RE (2) Island mode			✓	✓	✓
RE (3) Fail close			✓	✓	n/a
SR 5.3 – General purpose person-to-person communication restrictions	✓	✓	✓	✓	✓
RE (1) Prohibit all general purpose person-to-person communications			✓	✓	✗
SR 5.4 – Application partitioning	✓	✓	✓	✓	?
	SL1 ok (sous réserve)	SL2 ok (sous réserve)	SL3 nok	SL-A(FR5) = 2+	

Synthèse évaluation du FR5

SR	Audited?	SL1 required	SL2 required	SL3 required	SL4 required
5.1	Y	SR	SR + RE(1)	SR + RE(1) + RE(2)	SR + RE(1) + RE(2) RE(3)
5.2	Y	SR	SR + RE(1)	SR+RE(2)+RE(3)	SR+RE(2)+RE(3)
5.3	Y	SR	SR	SR + RE(1)	SR + RE(1)
5.4	N	SR	SR	SR	SR

SL-A(FR5) = 2+

Résultat de l'évaluation

FR	FR title	SR	SR title	Audited ?	SL1	SL2	SL3	SL4	Eval FR
1 - IAC	Identification and authentication control	1.1	Human user identification and authentication	Y					FR1
		1.10	Authenticator feedback	Y					0
		1.13	Access via untrusted networks	Y					
2 - UC	Use control	2.1	Authorization enforcement	Y					
		2.4	Mobile code	Y					FR2
		2.6	Remote session termination	Y					0
		2.8	Auditable events	Y					
		2.9	Audit storage capacity	Y					
		2.11	Timestamps	Y					
3 - SI	System integrity	3.2	Malicious code protection	Y					FR3
		3.9	Protection of audit information	Y					0
4 - DC	Data confidentiality	4.1	Information confidentiality	Y					FR4 : 0
5 - RDF	Restricted data flow	5.1	Network segmentation	Y					
		5.2	Zone boundary protection	Y					FR5
		5.3	person-to-person communication restrictions	Y					2
		5.4	Application partitioning	Y					
6 - TRE	Timely response to events	6.1	Audit log accessibility	Y					FR6
		6.2	Continuous monitoring	Y					1
7 - RA	Resource availability	7.3	Control system backup	Y					
		7.4	Control system recovery and reconstitution	Y					FR7
		7.5	Emergency power	Y					0
		7.7	Least functionality	Y					

Vulnérabilités mises en évidence

FR	FR title	SR	SR title	Audited ?	SL1	Eval FR
1 - IAC	Identification and authentication control	1.1	Human user identification and authentication	Y		FR1
		1.10	Authenticator feedback	Y		0
		1.13	Access via untrusted networks	Y		
2 - UC	Use control	2.1	Authorization enforcement	Y		
		2.4	Mobile code	Y		
		2.6	Remote session termination	Y		
		2.8	Auditable events	Y		
		2.9	Audit storage capacity	Y		
		2.11	Timestamps	Y		
3 - SI	System integrity	3.2	Malicious code protection	Y		FR3
		3.9	Protection of audit information	Y		0
4 - DC	Data confidentiality	4.1	Information confidentiality	Y		FR4 : 0
5 - RDF	Restricted data flow	5.1	Network segmentation	Y		
		5.2	Zone boundary protection	Y		FR5
		5.3	person-to-person communication restrictions	Y		2
		5.4	Application partitioning	Y		
6 - TRE	Timely response to events	6.1	Audit log accessibility	Y		FR6
		6.2	Continuous monitoring	Y		1
7 - RA	Resource availability	7.3	Control system backup	Y		
		7.4	Control system recovery and reconstitution	Y		FR7
		7.5	Emergency power	Y		0
		7.7	Least functionality	Y		

Accès possible depuis SI gestion sans contrôle ni validation local

Transfert de code sur des systèmes sans contrôle

Pas de moyen simple de couper connexion distante

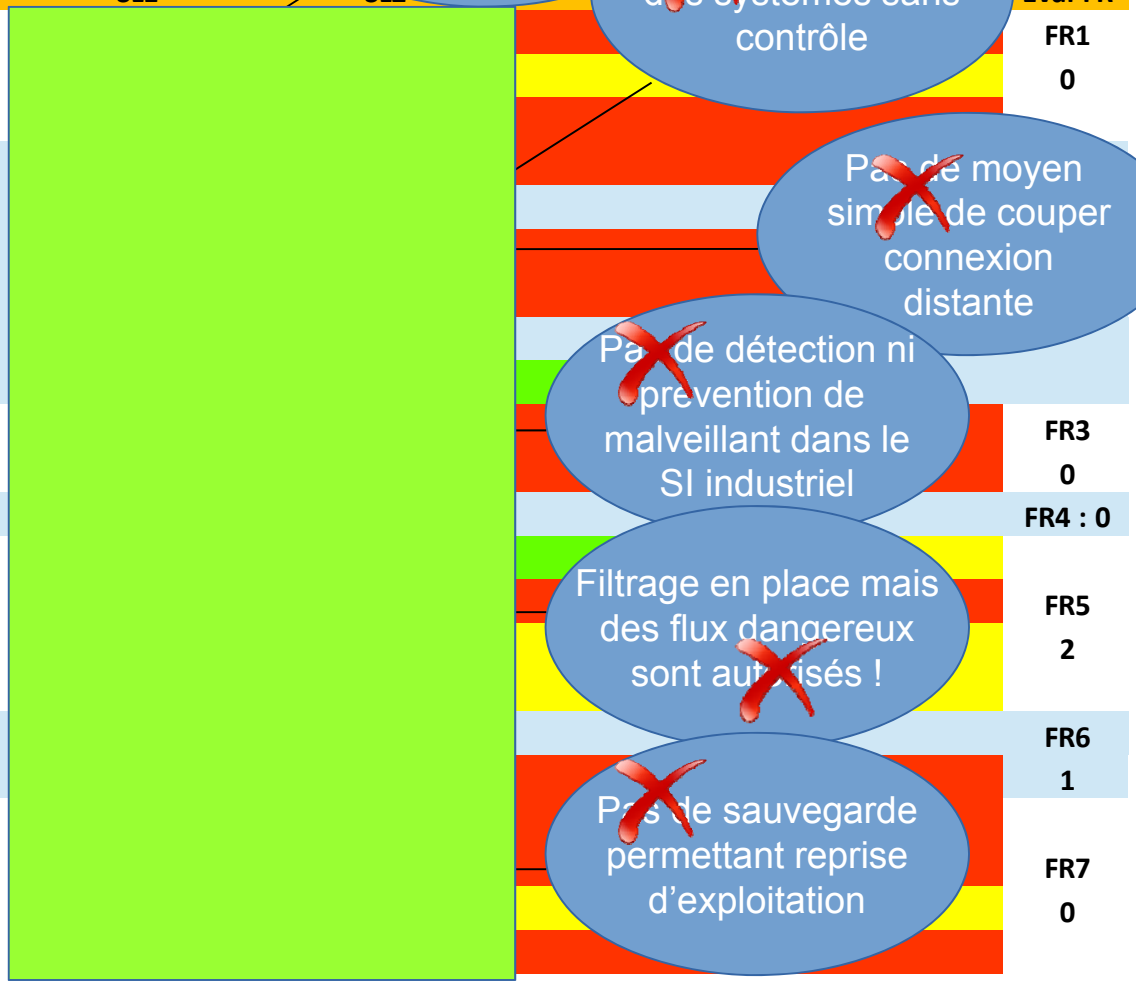
Pas de détection ni prévention de malveillant dans le SI industriel

Filtrage en place mais des flux dangereux sont autorisés !

Pas de sauvegarde permettant reprise d'exploitation

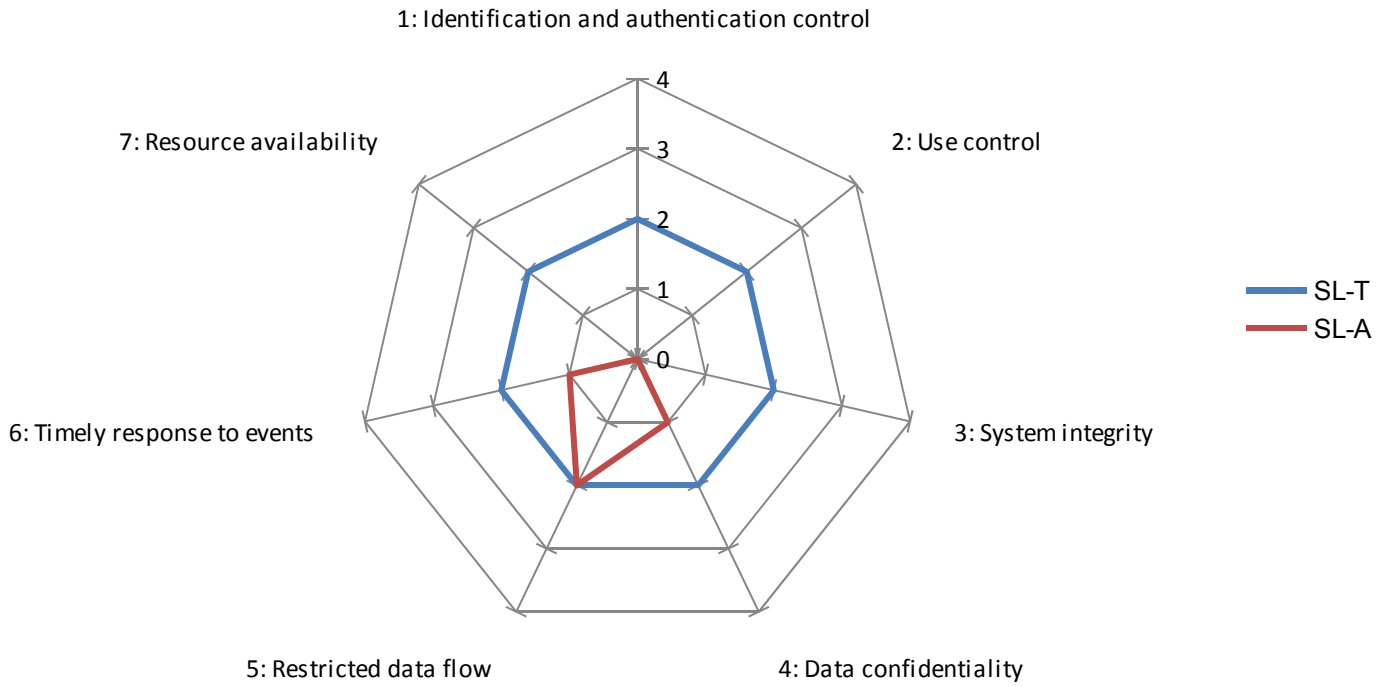
Quel niveau de sécurité aurait dû [illegible] Prykarpattya Oblenergo ?

FR	FR title	SR	SR title	Audited ?	Eval FR
1 - IAC	Identification and authentication control	1.1	Human user identification and authentication	Y	FR1
		1.10	Authenticator feedback	Y	0
		1.13	Access via untrusted networks	Y	
2 - UC	Use control	2.1	Authorization enforcement	Y	
		2.4	Mobile code	Y	
		2.6	Remote session termination	Y	
		2.8	Auditable events	Y	
		2.9	Audit storage capacity	Y	
		2.11	Timestamps	Y	
3 - SI	System integrity	3.2	Malicious code protection	Y	FR3
		3.9	Protection of audit information	Y	0
4 - DC	Data confidentiality	4.1	Information confidentiality	Y	FR4 : 0
5 - RDF	Restricted data flow	5.1	Network segmentation	Y	
		5.2	Zone boundary protection	Y	FR5
		5.3	person-to-person communication restrictions	Y	2
		5.4	Application partitioning	Y	
6 - TRE	Timely response to events	6.1	Audit log accessibility	Y	FR6
		6.2	Continuous monitoring	Y	1
7 - RA	Resource availability	7.3	Control system backup	Y	
		7.4	Control system recovery and reconstitution	Y	FR7
		7.5	Emergency power	Y	0
		7.7	Least functionality	Y	



Conclusion

SL-T = 2 aurait suffi à contrer l'attaque telle qu'elle a été menée



SL-T = 2 correspond à des attaquants moyennement équipés/motivés – Le niveau aurait été suffisant face à l'attaque telle qu'elle a été menée

Nota : si l'attaque a effectivement bénéficié d'un sponsoring étatique, des moyens plus puissants auraient pu être employés. Mais l'effort à accomplir pour SL-T = 3 (proche LPM en France) est très important

Setting the Standard for Automation™

France

Merci de votre attention

CAP'TRONIC
Strasbourg –5 octobre 2016