Systèmes ferroviaires communiquant et hétérogènes : impact sur la sécurité et la certification

14:40-15:30 : Jean-Louis Boulanger

CERTIFER

Thème de la journée

- Les systèmes embarqués occupent une place importante dans les moyens de transport. Ceci s'explique par le fait qu'aujourd'hui, plus de 90% des innovations dans le secteur des transports, routiers comme l'automobile, aéronautiques ou ferroviaires, sont dues directement ou indirectement aux avancées technologiques dans les domaines de l'informatique et de l'électronique embarquées. Les systèmes embarqués, dans les moyens de transport modernes, deviennent de plus en plus complexes et ils contiennent, dans certaines plates-formes, plusieurs dizaines de processeurs.
- Cette complexité répond aux besoins des constructeurs, pour offrir des fonctionnalités de plus en plus avancées comme l'aide à la conduite, la communication véhicule-à-véhicule ou la conduite automatique.
  Grâce aux progrès technologiques, les performances (vitesse d'exécution) ne sont plus de nos jours la seule figure de mérite.
  Les outils de conception des systèmes embarqués doivent maintenant prendre en compte aussi la fiabilité, la dissipation thermique, la certification et la vérification du logiciel exécuté.

CERTIFER

- *Evaluation de la **sécurité** et de la **conformité** dans le domaine du ferroviaire*

- ***Accréditation** COFRAC INSPECTION « 17020 » et CERTIFICATION « 45011 »*
- *Nombreuses reconnaissances nationales et internationales*

- *Plus de 17 années d'expérience*
- *Plus de 350 experts sur l'ensemble des secteurs ferroviaires provenant de : SNCF, RFF, RATP, Apave et Industriels, etc.…*

cofrac MULTI ACTIVITES

VIS - ANSF Verificatore Indipendente Sicurezza

epsf sécurité ferroviaire

Service public fédéral Mobilité et Transports

MINISTÈRE DU DÉVELOPPEMENT DURABLE ET DES INFRASTRUCTURES
Département des transports

Administration des chemins de fer

RÉPUBLIQUE FRANÇAISE

NOTIFICATION 0942

banedanmark

RDSO रेल अग्रदूत Transforming Railways

MINISTÈRE DES TRANSPORTS

www.CERTIFER.eu

- Couvre tous les secteurs :
  - Grande vitesse,
  - Conventionnel,
  - Fret et
  - Urbain
- Couvre tous les domaines :
  - Infrastructure,
  - Energie,
  - Contrôle-commande et signalisation,
  - Matériel roulant,
  - Système, maintenance, exploitation

CERTIFER
AGENCE DE CERTIFICATION FERROVIAIRE

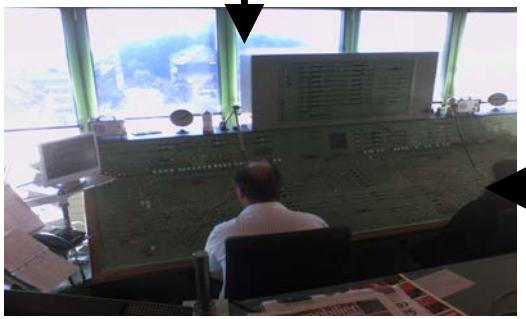
➢ *La référence pour vos missions* ***ISA/NOBO/DEBO/ CSM***

Sommaire

- Système ferroviaire
- Organisation des normes
- Cycle de Vie de la sécurité
- Logiciel
- CENELEC EN50128
- Conclusion
- Question

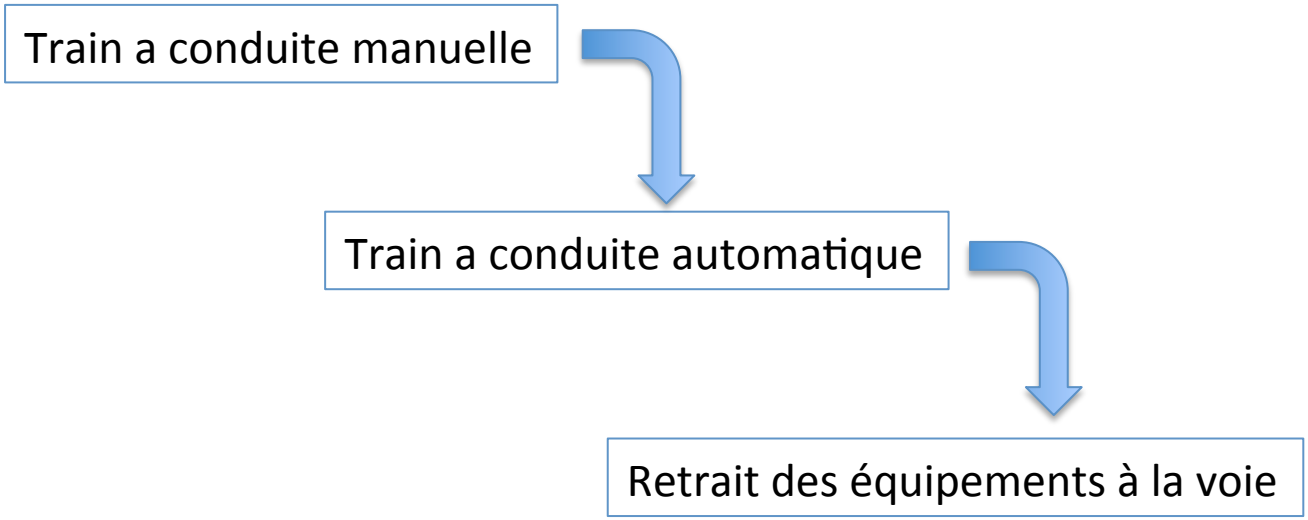
Système ferroviaire

Système ferroviaire



Changements

1er changement



2ème changement

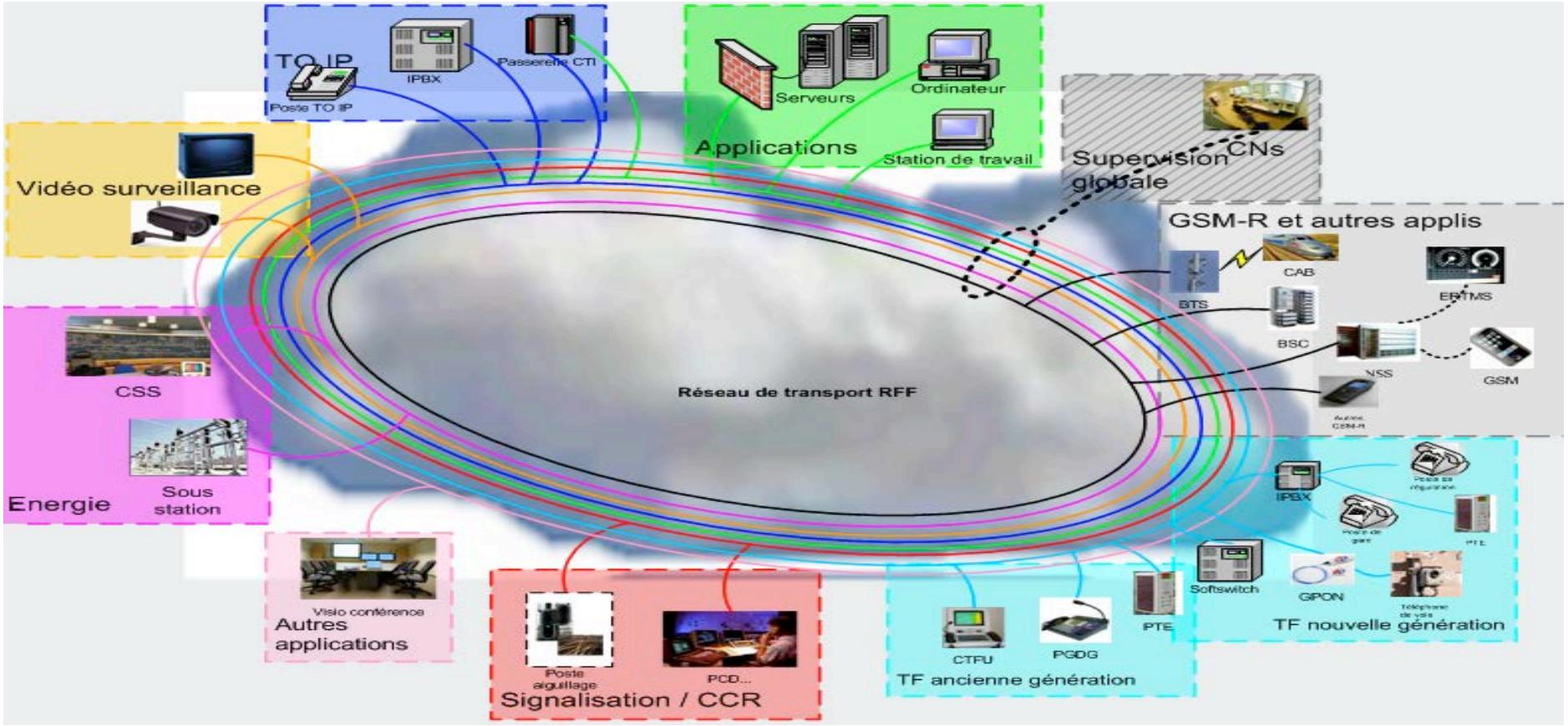
Monitoring
Récupération d'information
Maintenance distante
…

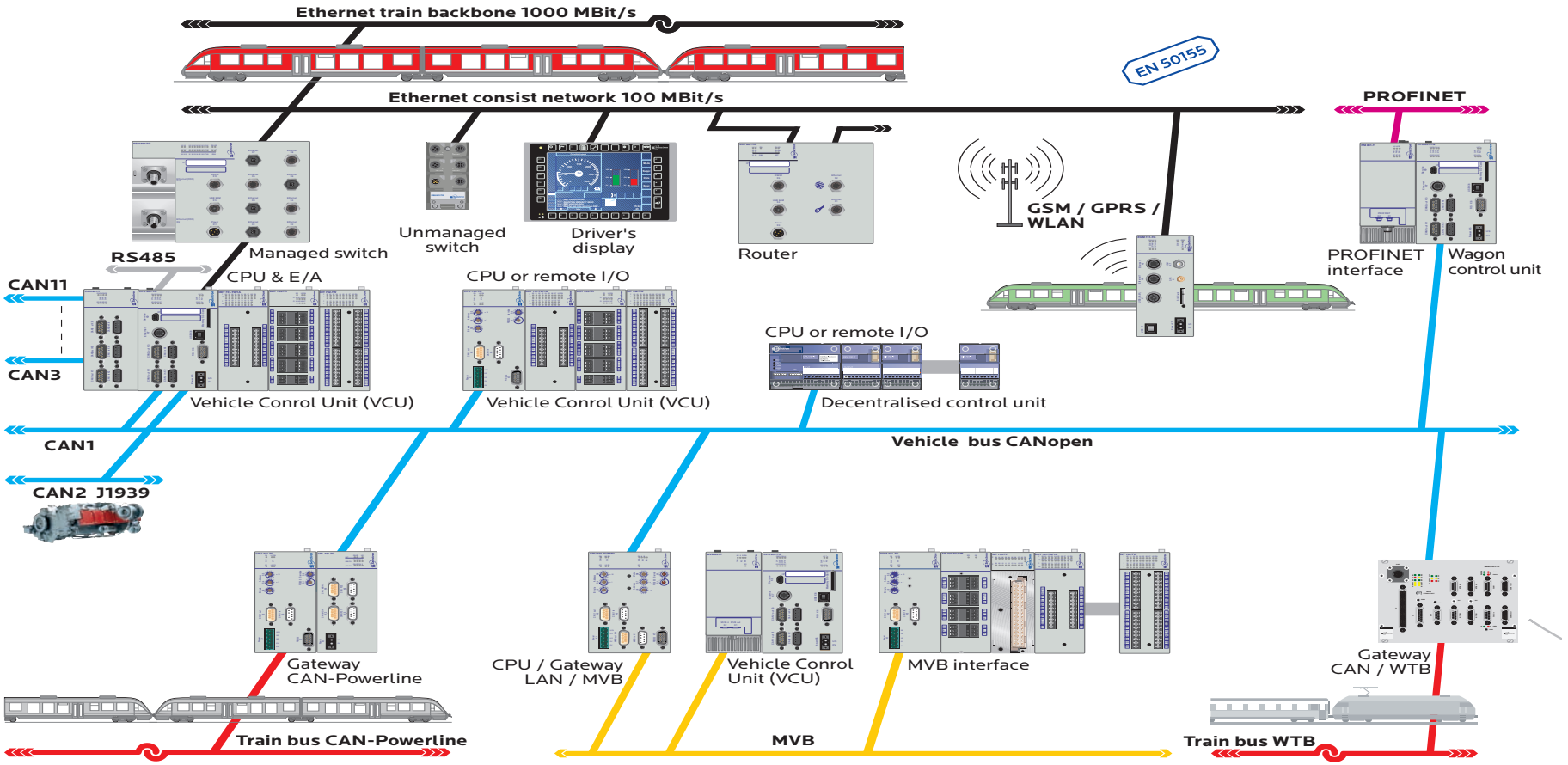
Communication entre système

Point sur les communications inter-système

- Communication au sein du train
  - Échange d'information au sein d'une voiture;
  - Échange d'information au sein d'une unité ;
  - Échange d'information au sein d'unité multiple:
    - Accouplement/désaccouplement
    - Phase d'inauguration
    - …
  - Mise en place de réseau passager (Wifi, GSM, ...).
- Communication sol – train
  - Mise en place de balise ;
  - Système de détection des trains ;
  - Système ERTMS
    - Utilisation de communication de type GSM-R
- Communication au sein du système ferroviaire
  - Information passager
  - Échange entre opérateur
  - …

Évolution du réseau global




Ethernet train backbone 1000 MBit/s
Ethernet consist network 100 MBit/s
EN 50155
PROFINET
Managed switch
Unmanaged switch
Driver's display
Router
GSM / GPRS / WLAN
PROFINET interface
Wagon control unit
RS485
CAN11
CAN3
CPU & E/A
CPU or remote I/O
CPU or remote I/O
Vehicle Conrol Unit (VCU)
Vehicle Conrol Unit (VCU)
Decentralised control unit
CAN1
Vehicle bus CANopen
CAN2 J1939
Gateway CAN-Powerline
CPU / Gateway LAN / MVB
Vehicle Conrol Unit (VCU)
MVB interface
Gateway CAN / WTB
Train bus CAN-Powerline
MVB
Train bus WTB

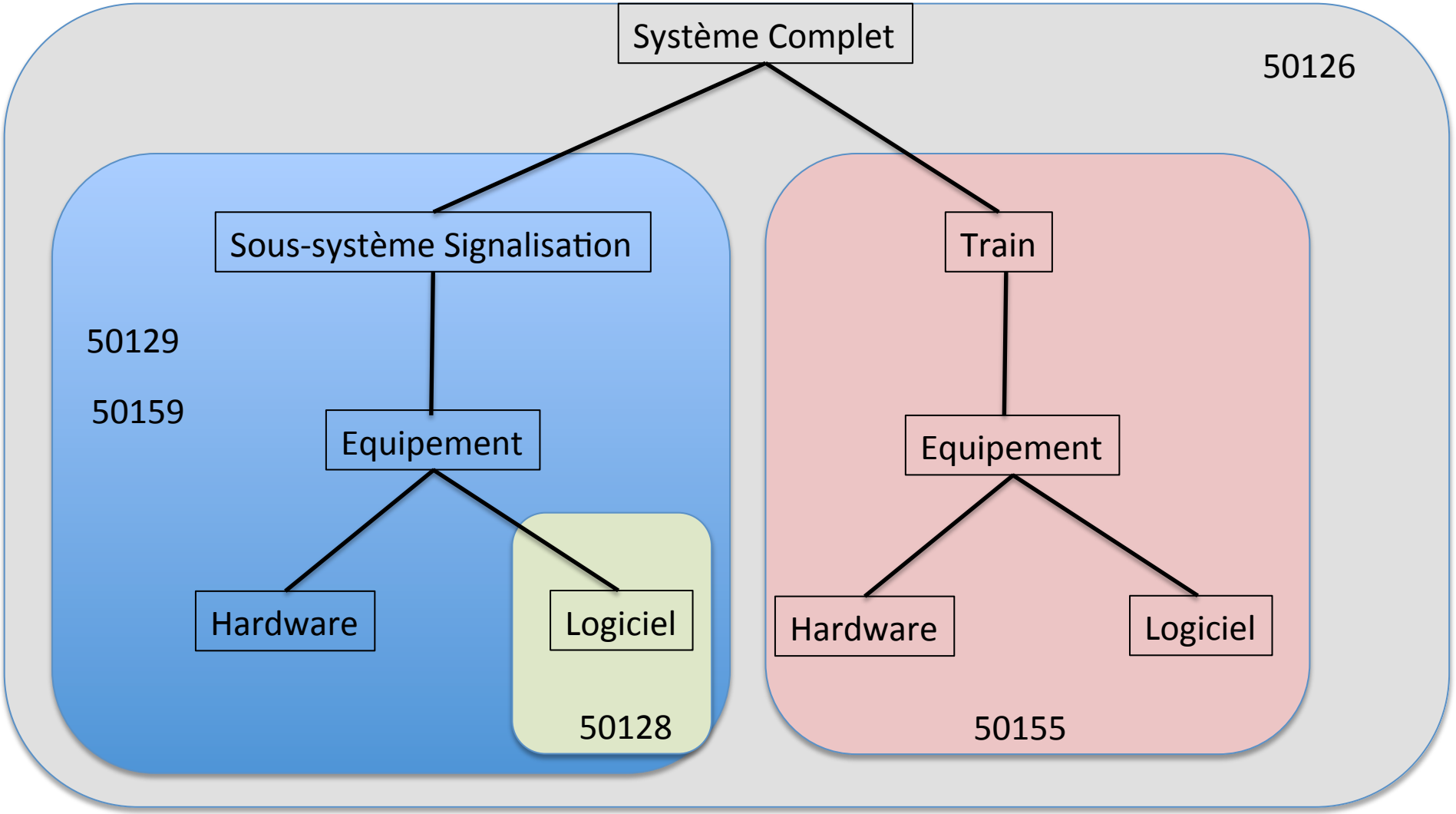
Que de logiciel

- Initialement : la sécurité reposait sur la signalisation

- Maintenant : le train dispose
  - de plusieurs réseaux et
  - de nombreux équipements qui comportent du logiciel

Contexte normatif

Organisation des normes



Cadre

- Les normes fournissent un cadre
- Ce cadre est un point de vue de l'état de l'art
- Une technique ou une approche non présente dans la norme ne signifie pas son rejet

- Mais la norme reste la référence, un objectif à atteindre, etc.

Innovation et normes

- Au sein des normes, il n'y a aucun élément explicite lié à l'innovation.

Pourquoi l’innovation ?

Principe de sécurité

- Un système/sous-système/équipement/ hardware/logiciel doit être capable de réaliser les fonctions en sécurité.
- Pour ce faire, des principes de sécurité doivent être
  - Identifiés;
  - Mis en œuvre;
  - Et démontrer leurs efficacités.

Innovation

- L'innovation doit répondre à un besoin et pour les aspects sécuritaires, doit être associée à un ou plusieurs principes de sécurité.

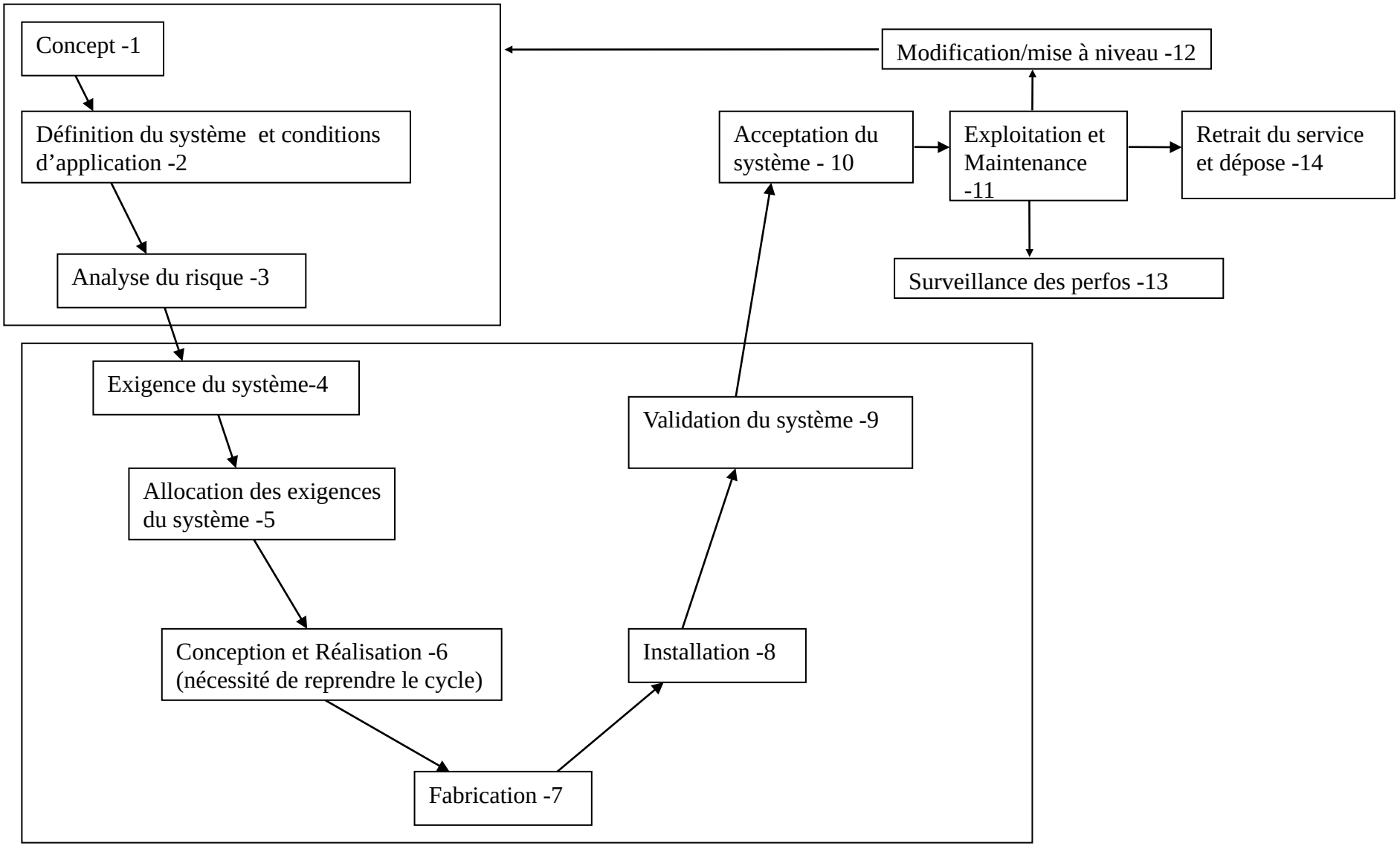
- Concernant le besoin :
  - Aspect financier (solution moins onéreuse, etc.)
  - Aspect délais (gain sur les délais de dev/..)
  - Aspect charge (gain sur les activités, …)
  - Aspect efficacité
  - …
  - Aspect démonstration sécurité

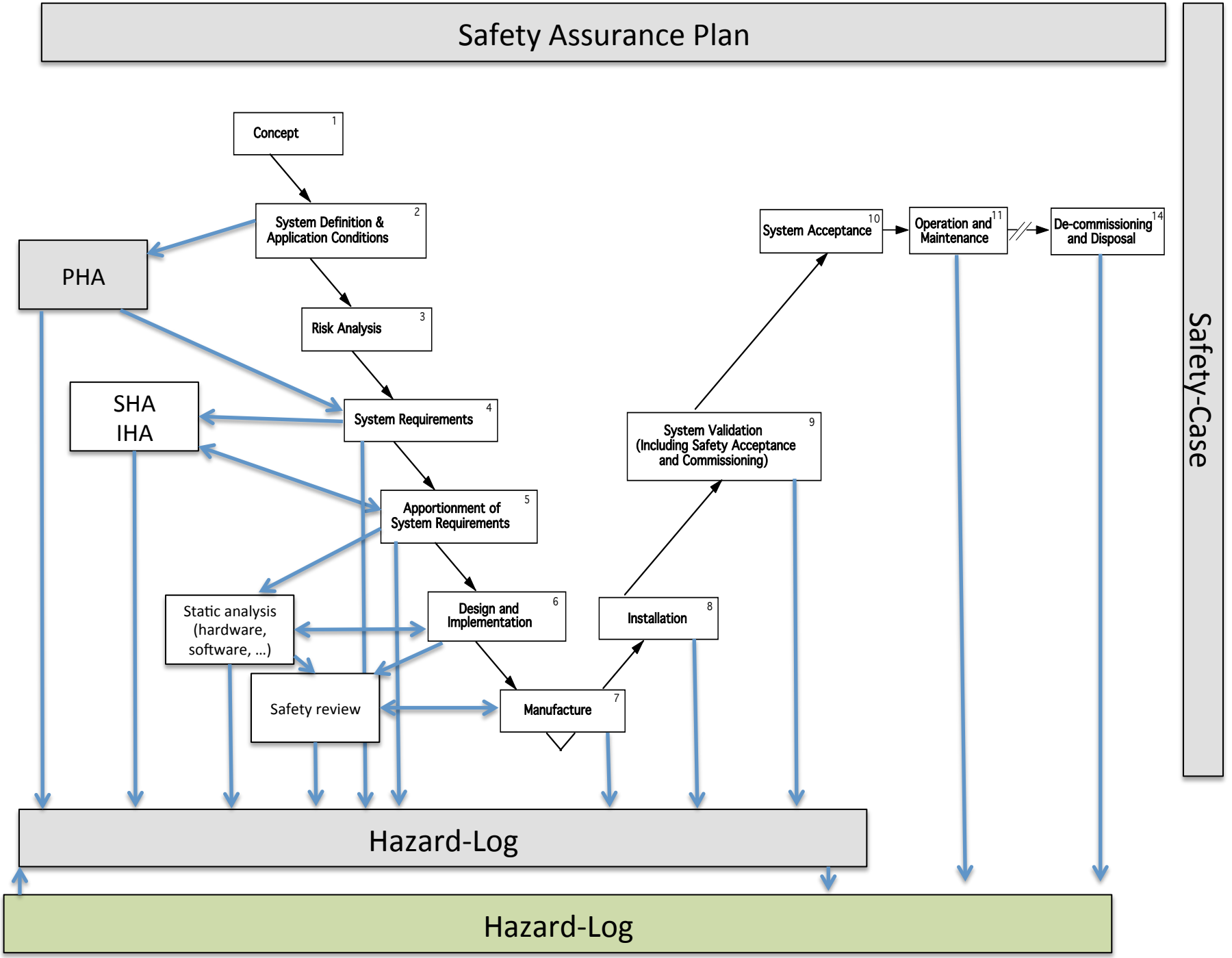
Exemple

- Soit un système ferroviaire X, la taille du logiciel est en général de 400 000 lignes
  - Il a été choisi de le développer en C++
  - Impact
    - Environ 1 000 000 de lignes de code C++
      - 60% du code concernent des classes abstraites ou d'interfaces
      - 40% représentent le code exécutable
    - Difficulté à tester le C++
    - Difficulté à relire l'ensemble du code

Cycle de vie de la sécurité

Cycle de vie


Concept -1
Définition du système et conditions d'application -2
Analyse du risque -3
Exigence du système-4
Allocation des exigences du système -5
Conception et Réalisation -6 (nécessité de reprendre le cycle)
Fabrication -7
Installation -8
Validation du système -9
Acceptation du système - 10
Exploitation et Maintenance -11
Modification/mise à niveau -12
Surveillance des perfos -13
Retrait du service et dépose -14


Safety Assurance Plan
Concept
1
System Definition & Application Conditions
2
PHA
Risk Analysis
3
SHA
IHA
System Requirements
4
Apportionment of System Requirements
5
Static analysis (hardware, software, ...)
Design and Implementation
6
Safety review
Manufacture
7
Installation
8
System Validation (Including Safety Acceptance and Commissioning)
9
System Acceptance
10
Operation and Maintenance
11
De-commissioning and Disposal
14
Safety-Case
Hazard-Log
Hazard-Log

Besoins

- Démonstration de la sécurité du produit
  - Certificat des composants
- Fiabilité et Disponibilité
- Maitrise de la sécurité jusqu'au retrait
  - Capacité à maitriser les évolutions après la mise en service et jusqu'au retrait
  - Capacité à déployer de nouvelles versions
- Maitrise de l'obsolescence
  - Au moins 40 années d'exploitation

Démonstration de la sécurité du produit (1/3)

- Pour un produit nouveau :
  - Certificat de produit
  - Retour d'expérience documenté
  - Validation du produit

- Le guide CENELEC 50129 – partie 1 fixe le cadre de la « cross-acceptance »

- Difficulté :
  - DAL est différent de SIL et SSIL
  - ASIL est différent de SIL et SSIL
  - SIL (61508) est différent de SIL(CENELEC)

Démonstration de la sécurité du produit (2/3)

- Pour la démonstration de sécurité, il est nécessaire de démontrer la compétence des personnes :
  - Besoin de définir une méthodologie;
    - Guide
    - Instruction
    - Etc.
  - Besoin de formation;
  - Etc.

Démonstration de la sécurité du produit (3/3)

- Pour la démonstration de sécurité, il est nécessaire de démontrer que les exigences sont prises en comptes:
  - Besoin de testabilité ;
  - Besoin de rejeu des activités;
  - Besoin de définir une méthodologie;
  - Etc.

- Il est nécessaire d'avoir une évaluation indépendante
  Besoin de disposer d'éléments auditables;
  - Nécessité de former les évaluateurs et de donner accès à la technologie.

Fiabilité et Disponibilité

- Pour un produit nouveau :
  - Des éléments liés à la fiabilité
    - MTBF, MTTR, …
  - Des éléments liés à la disponibilité

- Problématique du retour d'expérience
  - Disposer d'informations (nom projet, taille, niveau de sécurité, etc.);
  - Disposer de chiffres (temps d'utilisation, …);
  - Disposer d'une liste des défauts connus;
  - Etc.

Maitrise de la sécurité jusqu'au retrait

- Capacité à maitriser les évolutions après la mise en service et ceci jusqu'au retrait
  - Remise en œuvre du processus de réalisation;
  - Maitrise des évolutions;
  - Maitrise des moyens d'exécution (mémoire, cycle, etc.);
  - Etc.
- Capacité à déployer de nouvelles versions
  - Nouvelle version de l'équipement
  - Nouvelle version des OS/firmware
  - Nouvelle version des logiciels
  - Etc.

Maitrise de l'obsolescence

- Gestion de l'obsolescence
  - Hardware;
  - Logiciels;
  - Outils et OS;
  - Etc.

Acceptation du risque

- Le référentiel CENELEC introduit 3 approches d'acceptation du risque : ALARP, GAME et MEM
- En France, il est recommandé d'utiliser le GAME

  => Le GAME peut sembler un frein à l'innovation

… logiciel

Que du logiciel

- Une des difficultés : les innovations impliquent, en général, la mise en œuvre de logiciel:
  - Environnement de développement
  - Système d'exploitation
  - Bibliothèques
  - Compilateur
  - Générateur de code
  - Logiciels spécifiques
  - Etc.

CENELEC 50128

50128:2001

- Dans le cadre de la CENELEC 50128:2001, les tableaux A.x contenaient des éléments nommés comme par exemple

TECHNIQUE/MESURE	Réf	NISL 0	NISL 1	NISL 2	NISL 3	NISL 4
1. Méthodes formelles comprenant par exemple CCS, CSP, HOL, LOTOS, OBJ, logique temporelle, VDM, Z et B	B.30	-	R	R	HR	HR
2. Méthodes semi-formelles	D.7	R	R	R	HR	HR
3. Méthode structurée comprenant par exemple JSD, MASCOT, SADT, SDL, SSADM et Yourdon.	B.60	R	HR	HR	HR	HR

Exigences

1. La Spécification des Exigences du Logiciel exige toujours une description du problème en langage naturel et toutes les notations mathématiques nécessaires pour refléter l'application.
2. Le tableau reproduit des exigences supplémentaires permettant d'obtenir une spécification claire et précise. Une ou plusieurs de ces techniques doivent être choisies en vue de satisfaire au niveau d'intégrité de la sécurité logicielle utilisé.

50128:2011

- Retrait du nom des méthodes
- Ajout de la capacité d'utiliser d'autres langages

Table A.15 – Textual Programming Languages

TECHNIQUE/MEASURE	Ref	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
1. ADA	D.54	R	HR	HR	HR	HR
2. MODULA-2	D.54	R	HR	HR	HR	HR
3. PASCAL	D.54	R	HR	HR	HR	HR
4. C or C++	D.54 D.35	R	R	R	R	R
5. PL/M	D.54	R	R	R	NR	NR
6. BASIC	D.54	R	NR	NR	NR	NR
7. Assembler	D.54	R	R	R	R	R
8. C#	D.54 D.35	R	R	R	R	R
9. JAVA	D.54 D.35	R	R	R	R	R
10. Statement List	D.54	R	R	R	R	R

Requirements:

1) The selection of the languages shall be based on the requirements given in 6.7 and 7.3.

2) There is no requirement to justify decisions taken to exclude specific programming languages.

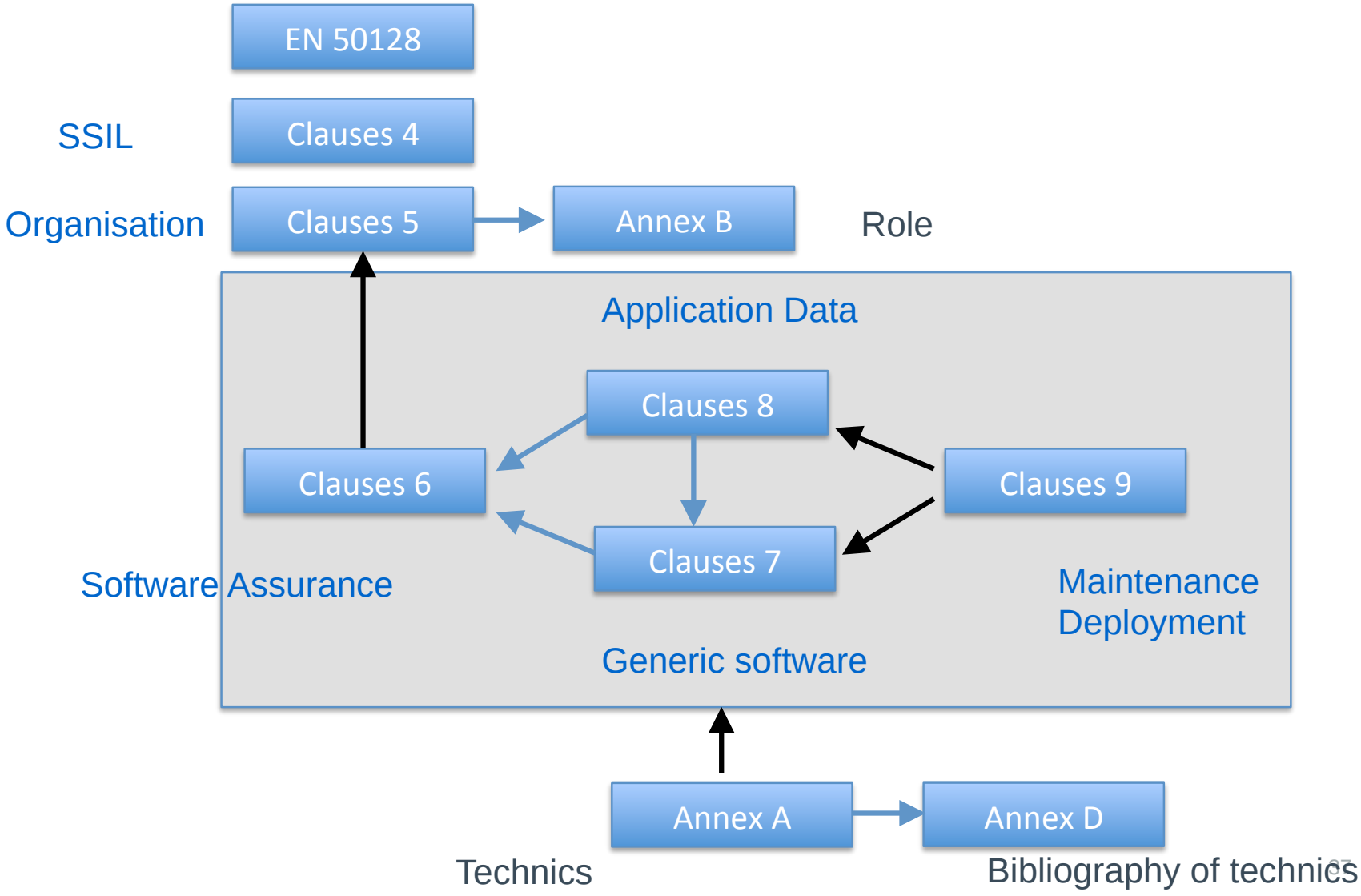
NOTE 1 For information on assessing the suitability of a programming language see entry in Clause D.54 'Suitable Programming Languages',

NOTE 2 If a specific language is not in the table, it is not automatically excluded. It should, however, conform to Clause D.54.

NOTE 3 Run-time systems associated with selected languages which are necessary to run application programs still have to be justified for usage according to the Software Safety Integrity Level.

CERTIFER
RAILWAY CERTIFICATION AGENCY

50128:2011



Innovations possibles

- Évolution méthodologique
  - Modélisation
  - Vérification statique
  - Etc.
- Utilisation d'outils
- Environnement d'exécution
  - Machine virtuelle
  - Couche logicielle
    - Partitionnement
    - Virtualisation
    - Etc.

Évolutions méthodologiques

- Démontrer la prise en compte de la CENELEC 50128
- Ou une efficacité similaire
  - Justification
  - Demande d'acceptation de la justification par l'évaluateur

Utilisations d'outils

- Justification de l'utilisation par rapport au processus de la 50128
- Qualification des outils
  - 3 classes T1,T2,T3

1) tools and Tx selection

[6.7.4.1 **AND** 6.7.4.2 **AND** 6.7.4.3]

AND

2) Tools specification and validation

[(6.7.4.4 **AND** 6.7.4.5) **OR** 6.7.4.6]

AND

3) Design methodology justification

[6.7.4.7 **OR** 6.7.4.8]

AND

4) Code generation

(6.7.4.9)

AND

5) configuration management and new version

[6.7.4.10 **AND** 6.7.4.11]

AND

6) effort for Tx

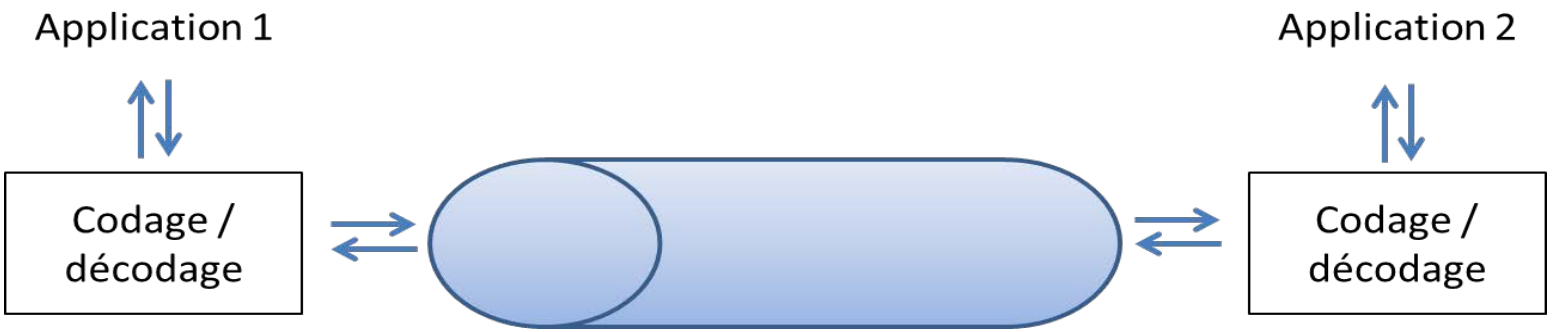
(6.7.4.12)

Environnement d'exécution

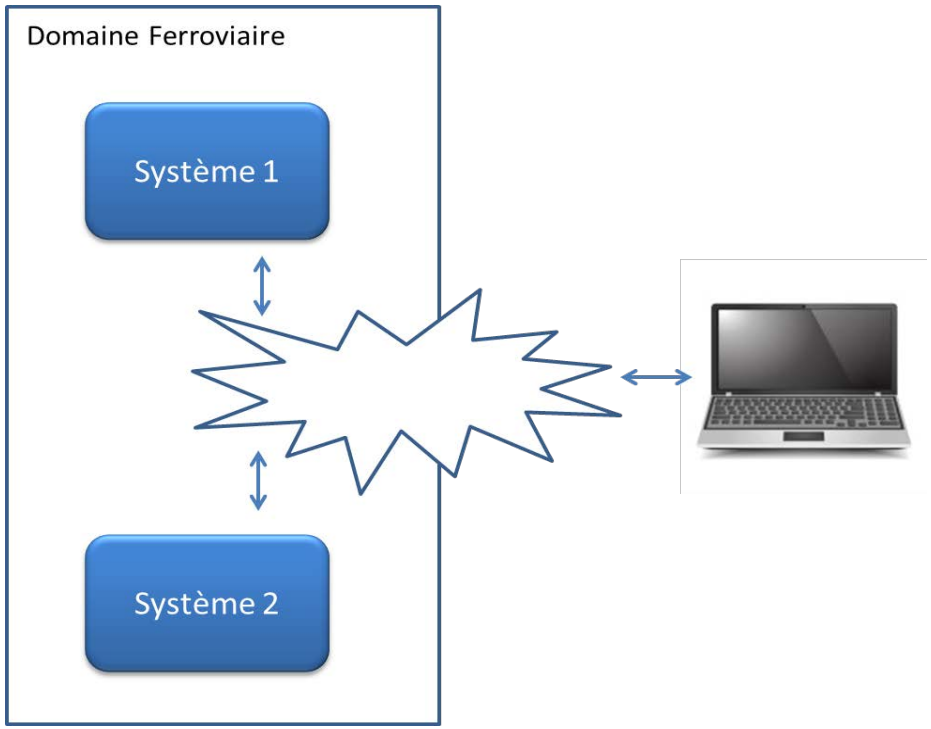
- Concernant les machines virtuelles, les systèmes d'exploitation, la virtualisation, etc.
  - Il convient de faire très attention car il est difficile de démontrer que la norme a été appliquée pour les développer
- Concernant les couches logicielles ou bibliothèques,
  - La nouvelle 50128 introduit la notion de composants réutilisés en place des COTS

Communication

Gray channel



Réseau ouvert



- Au final, les erreurs de base concernant les messages se limitent à :
  - la répétition : un message existant est resoumis à un moment inapproprié.
  - la suppression : un message est détruit (par exemple une demande de freinage d'urgence)
  - l'insertion : un message est inséré dans le flux existant
  - le séquencement : la séquence des messages est modifiée (retard sur un message par exemple)
  - la corruption : un message est modifié en un autre message correct
  - le retard : le système de transmission est surchargé
  - la mascarade : un intrus se fait passer pour un des interlocuteurs.
-
- Sur cette base, la norme CENELEC 50159 propose une approche pour traiter et démontrer la sécurité des communications. Une des caractéristiques au final des applications ferroviaires est que la sécurité est réalisée par les applications (et non par le réseau) et qu'en cas de défaillances le système va atteindre un état de sécurité prédéfini (en général de manière passive).
-
- Les réseaux (fermés ou ouverts) sont construits sur des médias de communication qui sont maitrisés et dont les accès sont limités.

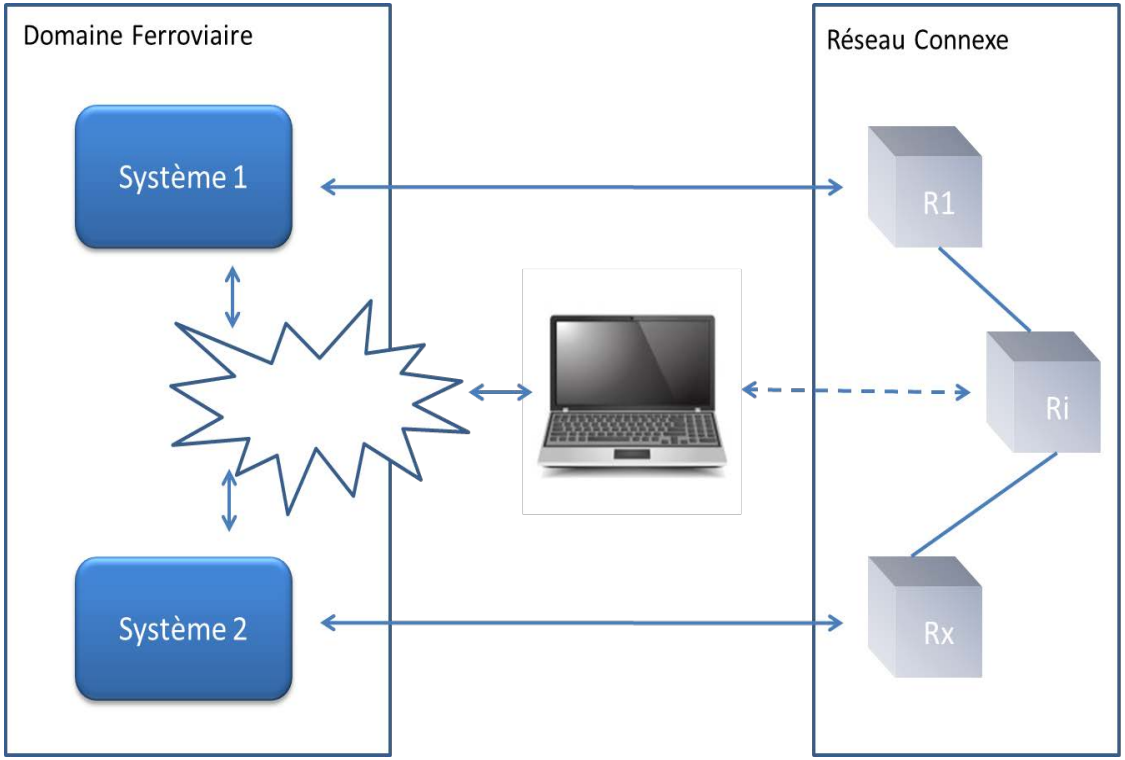
Politique

- La mise en place d’un réseau distant doit se faire en définissant une politique qui doit prendre en compte différents sujets :
  - La définition des missions du réseau distant (type d’accès, etc.) ;
  - La définition des objectifs (accès à tout moment à chaque équipement, etc.) ;
  - La définition du réseau (choix des éléments, etc.) ;
  - Le processus d’installation (procédure, etc.) ;
  - Le processus de gestion ;
  - La gestion des modes dégradés (perte d’une partie du réseau, etc.) ;
  - La gestion des rôles ;
  - La politique de sécurité au sens « *security* » ;
  - etc.

Réseau ouvert

+

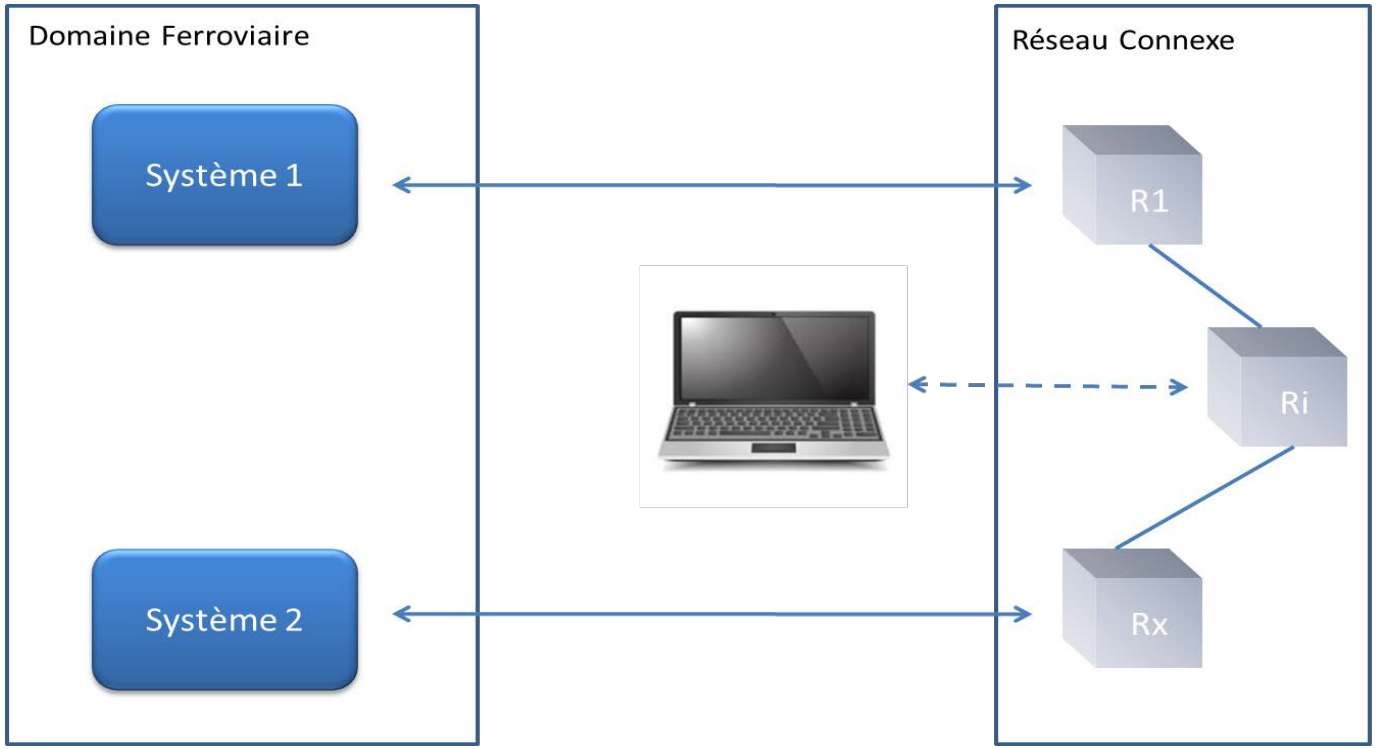
accès distant



Point faible 50159

- Il apparaît au travers de ces nouveaux usages (utilisation de réseau WiFi par exemple) que la norme CENELEC 50159 n’est pas suffisante car elle ne traite
  - ni de la gestion des COTS ;
  - ni des protections contre les attaques externes ;
  - ni des protections physiques contre l’intrusion dans les locaux ;
  - etc.

Accès distant



- Du point de vue de la « security », il va falloir être capable
  - d'identifier et de contrôler l'ensemble des accès ;
  - d'identifier et de contrôler les flots de données sécuritaires et/ou prioritaires ;
  - de garantir les objectifs de qualité de service (QoS), de disponibilité et de fiabilité ;
  - …

- Du point de vue de la FDMS classique, il va falloir (liste partielle)
  - analyser les impacts sur la « safety » des nouvelles menaces comme
    - les virus : que se passe-t-il si un virus se charge sur un calculateur de sécurité ? même s'il ne peut avoir d'impact, il peut entrainer une consommation de temps, de place, …
    - les surcharges du réseau : le retard et/ou la perte de message pourrait entrainer des indisponibilités ;
    - …
  - analyser les impacts des problèmes réseaux sur la disponibilité du(des) système(s) ;
  - …

- Les équipements liés au réseau distant doivent être hébergés dans des locaux spécifiques qui sont à la limite du système ferroviaire (voire à l’extérieur) et qui peuvent être sujets à des intrusions physiques (la personne mal intentionnée cherchant un moyen de se connecter physiquement).

- Concernant la politique de sécurité, il faut maintenant prendre en compte tous les types d’intrusions (physiques ou pas). Mais il est aussi nécessaire de bien analyser les usages qui sont prévus et d’identifier les nouvelles menaces qui pourraient apparaître. Si un PC de supervision est installé sur le réseau et qu’il dispose d’un accès au net permettant de surfer sur le web, il y a de fortes chances qu’un malware soit chargé et qu’il passe d’un réseau à l’autre.

Conclusion

Innovation

- Elle est nécessaire pour offrir un meilleur service, des nouvelles fonctionnalités ou pour gagner en compétitivité
- Elle doit rendre un service (ne peut pas être qu'un moyen de se démarquer)
- Elle doit être maitrisée (connaissance des impacts et des gains)
- Elle doit s'inscrire dans un produit et dans une approche de sécurité

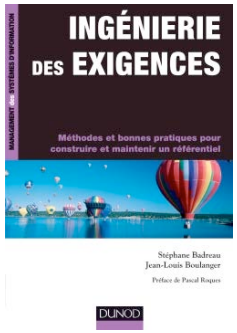
Pour conclure

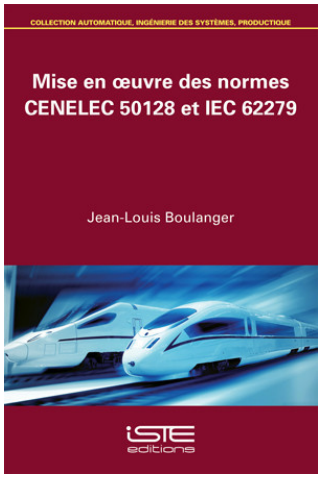
- Une politique « security » nécessite de définir un cycle de vie et un objectif à atteindre (du type du SIL).
- On parle de SL
- La norme 27005 présente une politique de « security » très générale qui reste a préciser.
- La norme IEC 62443 concernant la « security » dans le monde des automates est un bon point de commencement

Pour finir

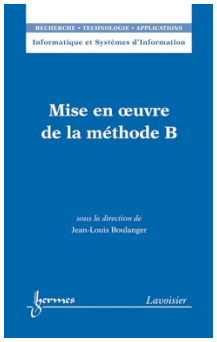
- L’innovation ne doit pas chercher à simplifier l’application des normes mais elle doit simplifier la conformité aux normes.

Question ?

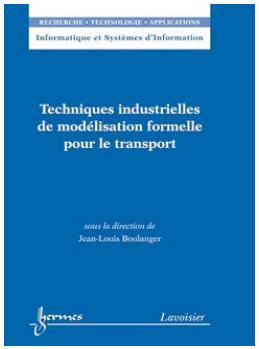

INGÉNIERIE
DES EXIGENCES
Méthodes et bonnes pratiques pour construire et maintenir un référentiel
Stéphane Badreau
Jean-Louis Boulanger
Préface de Pascal Roques
DUNOD


COLLECTION AUTOMATIQUE, INGÉNIERIE DES SYSTÈMES, PRODUCTIQUE
Mise en œuvre des normes
CENELEC 50128 et IC 62279
Jean-Louis Boulanger
iSTE
editions


Maîtriser la sécurité des
systèmes programmables


RECHERCHE • TECHNOLOGIE • APPLICATIONS
Informatique et Systèmes d'Information
Mise en œuvre
de la méthode B
sous la direction de
Jean-Louis Boulanger
Hermes
Lavoisier


RECHERCHE • TECHNOLOGIE • APPLICATIONS
Informatique et Systèmes d'Information
Outils de mise en œuvre
industrielle des techniques
formelles
sous la direction de
Jean-Louis Boulanger
Hermes
Lavoisier


RECHERCHE • TECHNOLOGIE • APPLICATIONS
Informatique et Systèmes d'Information
Techniques industrielles
de modélisation formelle
pour le transport
sous la direction de
Jean-Louis Boulanger
Hermes
Lavoisier


Hermes
Lavoisier


IC2
Traité Informatique et Systèmes d'Information
Sécurisation
des architectures
industrielles
sous la direction de
Jean-Louis Boulanger
Hermes
Lavoisier


IC2
Traité Informatique et Systèmes d'Information
Sécurisation
des architectures
informatiques
exemples concrets
sous la direction de
Jean-Louis Boulanger
Hermes
Lavoisier