FROM RESEARCH TO INDUSTRY

cea tech

list

Des systèmes globaux, des systèmes cyberphysiques :

LA TRANSITION NUMÉRIQUE UN ENJEU MAJEUR DE L'USINE DU FUTUR

François TERRIER

Chef département d'ingénierie des logiciels et des systèmes
Pr. INSTN / Université Paris-Saclay

UN MOUVEMENT MONDIAL
UNE STRATÉGIE EUROPÉENNE

2011 : President Obama Launches Advanced Manufacturing Partnership ; The plan, leverages existing programs & proposals, will invest more than 500 M$

2011 : India launched a National Manufacturing Policy to increase activity from a 16% to 25% GDP by 2022

2014 - Advanced **Manufacturing** Technology in **China**: A Roadmap to **2050**

EFFRA
EUROPEAN FACTORIES OF THE FUTURE RESEARCH ASSOCIATION

MANUFUTURE-EU

Manufacturing: Key to Our Economy

- The important of manufacturing is now well recognised by EU and its member states and its competitors
- Significant transformation underway in advanced manufacturing
- Digitlaisation & ICT-enabled technologies are playing key roles in this transformation
- Europe must prepare, enable & respond to this
- 'Factories of the Future' partnership is a key EU programme to achieve this

Euro area industrial production +0.2% in Nov 14 over Oct 14, -0.4% over Nov 13

Factories of the Future
Digitalisation & Manufacturing

- 'Digitalisation' affects multiple aspects of manufacturing such as:
  - Process quality – monitoring and control
  - Interconnectivity of machines
  - Plant management
  - Data processing
  - Apps for workers
  - Training
- Advanced manufacturing cannot evolve without digitalisation – ICT fundamental for evolution of manufacturing
- Equally innovations in digitalisation will be driven by the demands of advanced manufacturing
- Manufacturing companies becoming much more involved in developing digital services & ICT-enabled tech. to meet their particular needs

FoF
EFFRA
ICMR
Irish Centre for Manufacturing Research

Industrie 4.0
CATAPULT
smart industry
DUTCH INDUSTRY FIT FOR THE FUTURE

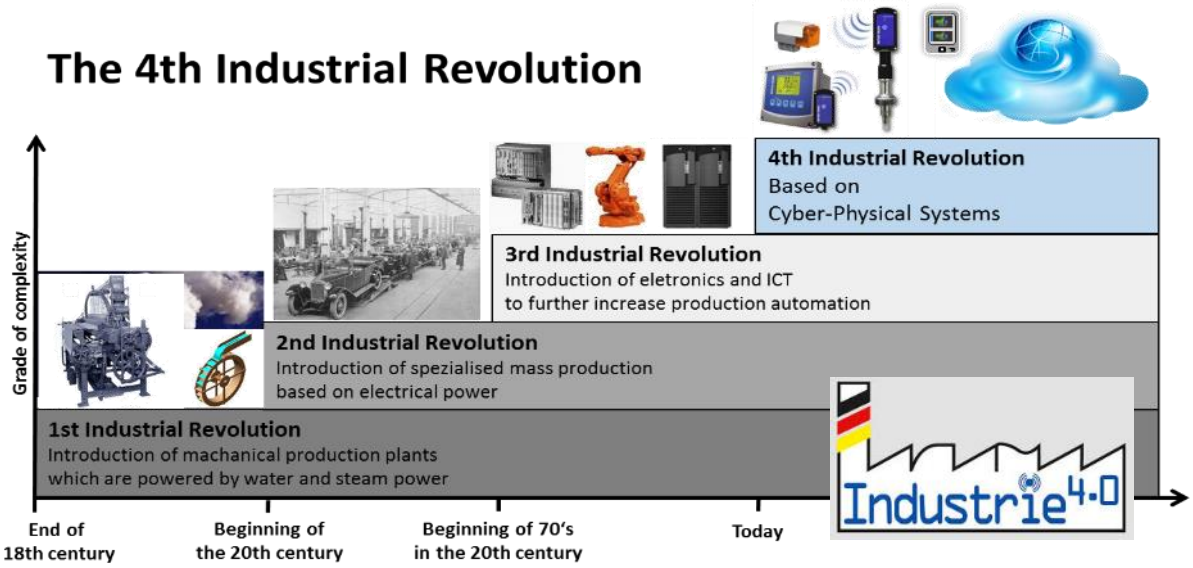
AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION
Report
AIOTI WG11 – Smart manufacturing
2015

La Fabbrica del Futuro

Alliance INDUSTRIE DU FUTUR

INSTITUT CARNOT CEA LIST
université PARIS-SACLAY

UNE STRATÉGIE NATIONALE : LA 4IÈME RÉVOLUTION INDUSTRIELLE

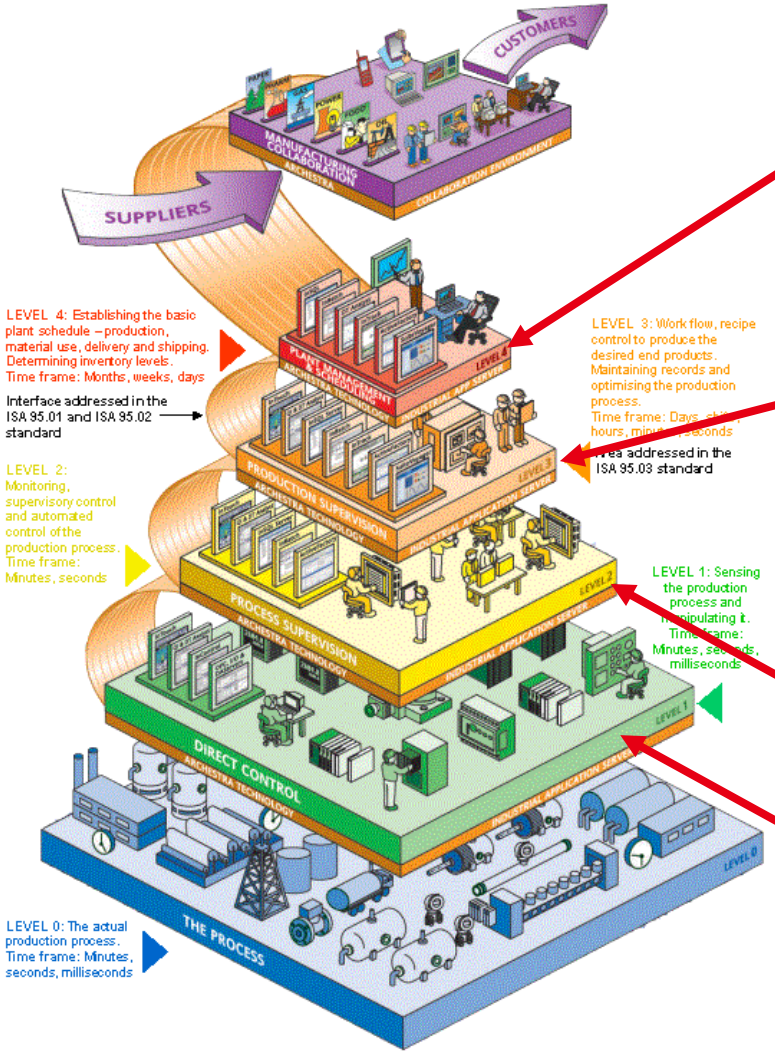


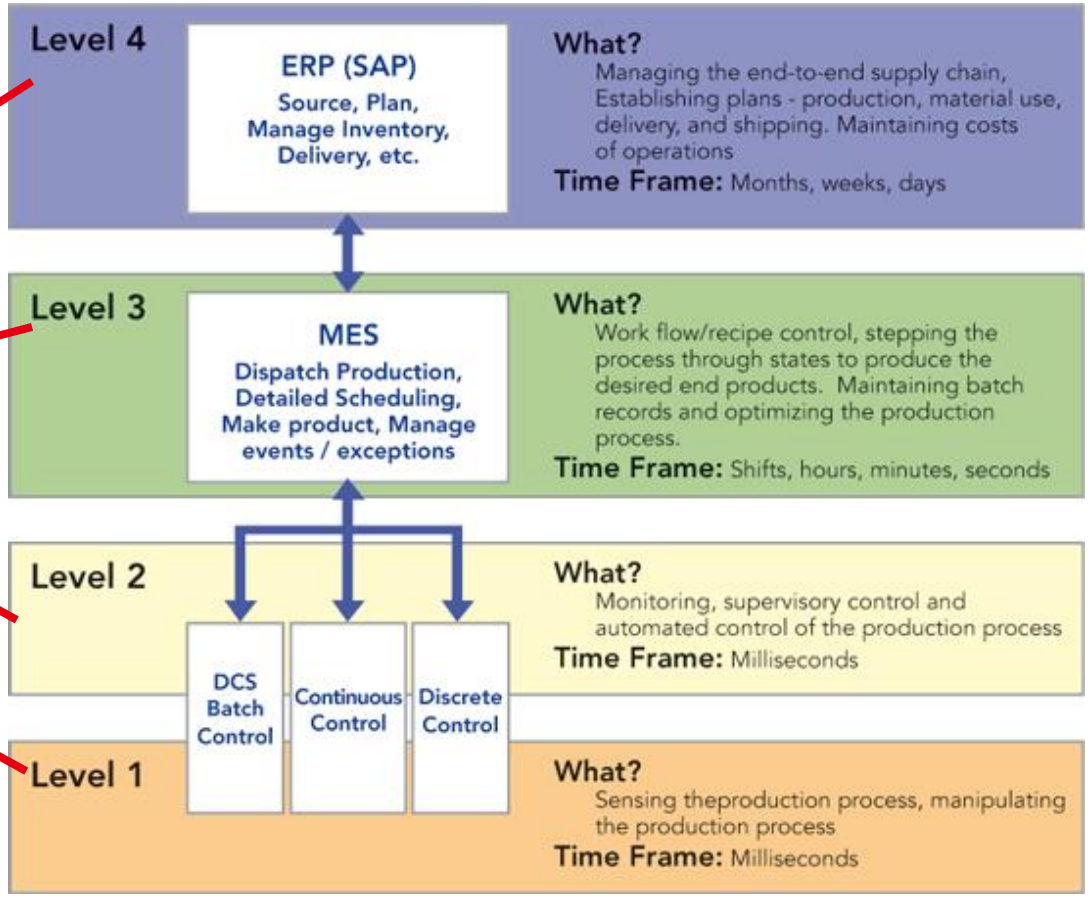
- Prise de conscience du rôle des TIC pour l'industrie manufacturière
- Vers une production de faible quantité, personnalisée, dans une organisation réactive, économe en moyens (finance et énergie)
- Convergence entre Internet des Objets, Systèmes Cyber-Physiques, Modélisation/Co-simulation, Cobotique
- Un besoin identifié :

➔ développer une vision intégratrice

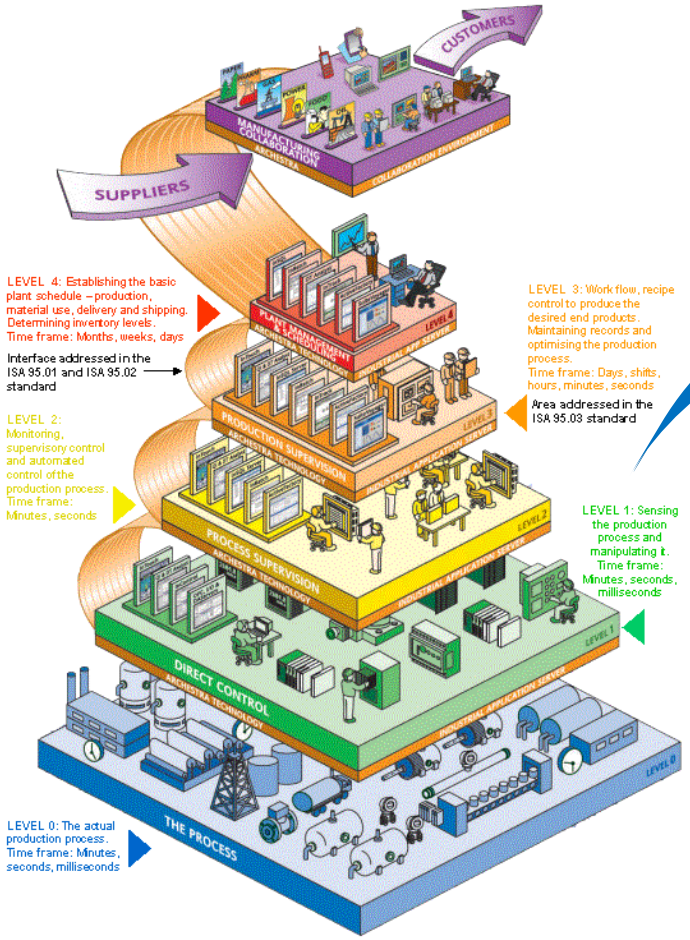
Un exemple (projet européen BEinCPPS)

Une architecture globale déjà standardisée (ISA 95)



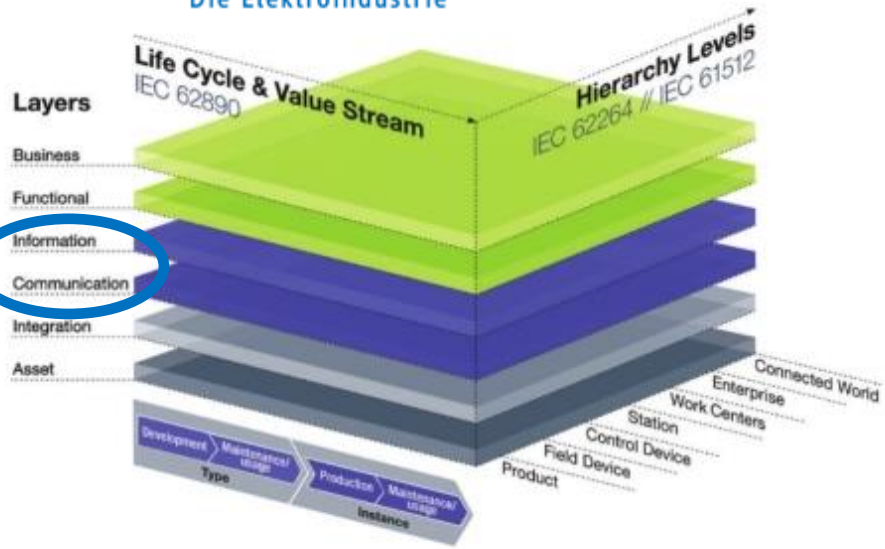


Un standard qui évolue ➔ « RAMI 4.0 »



ZVEI: Die Elektroindustrie

Standard RAMI 4.0



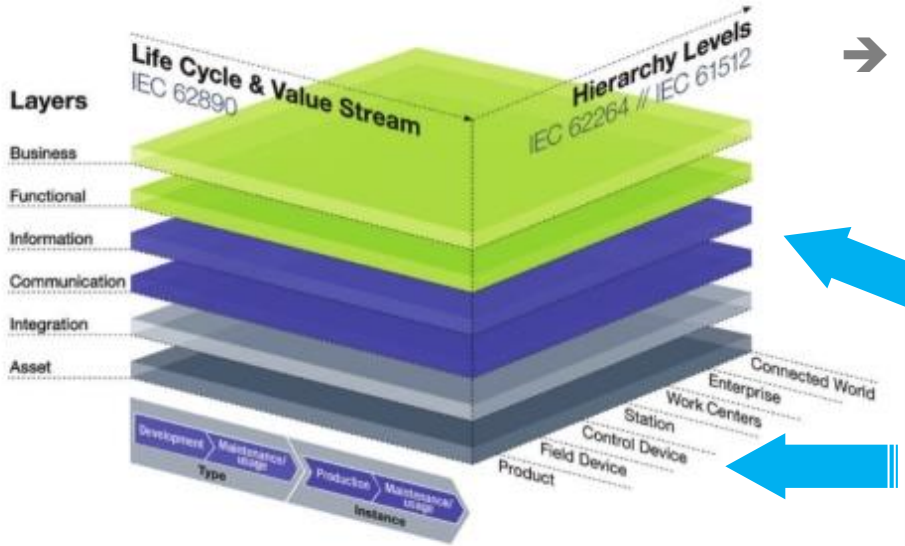
➔ **De plus en plus de produits intégrant logiciels avec des communications et la production de données**

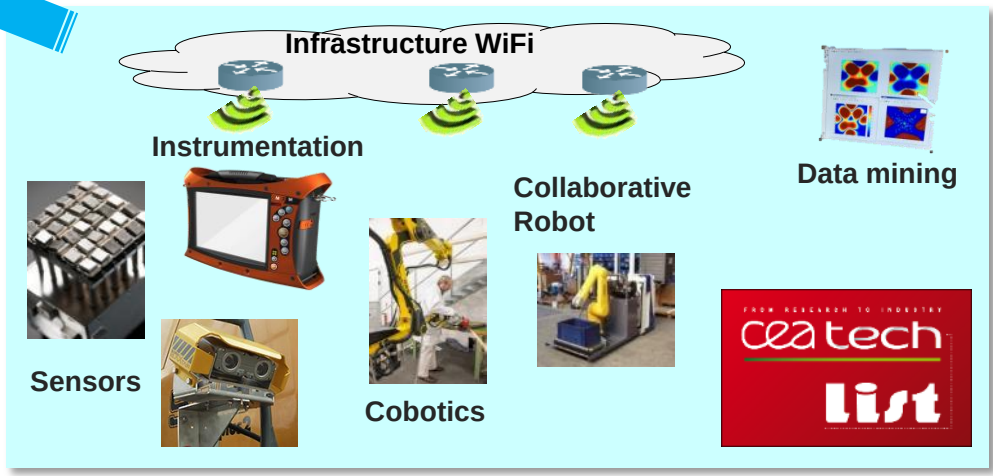
➔ **Déclinaison selon deux dimensions :**

- ❑ La structure de l'usine (composition)
- ❑ Le cycle de vie et la chaîne de valeur

INTRODUCTION DE NOUVELLES FONCTIONS

- ➔ Plus de capteurs (ex. caméra/vision)
- ➔ Du contrôle avancé (ex. CND en ligne)
- ➔ De l'assistance (ex. cobot)
- ➔ Des communication avancées (ex. wifi reconfigurable, optimisé)
- ➔ De l'analyse de données de masse (ex. pour la maintenance prédictive)



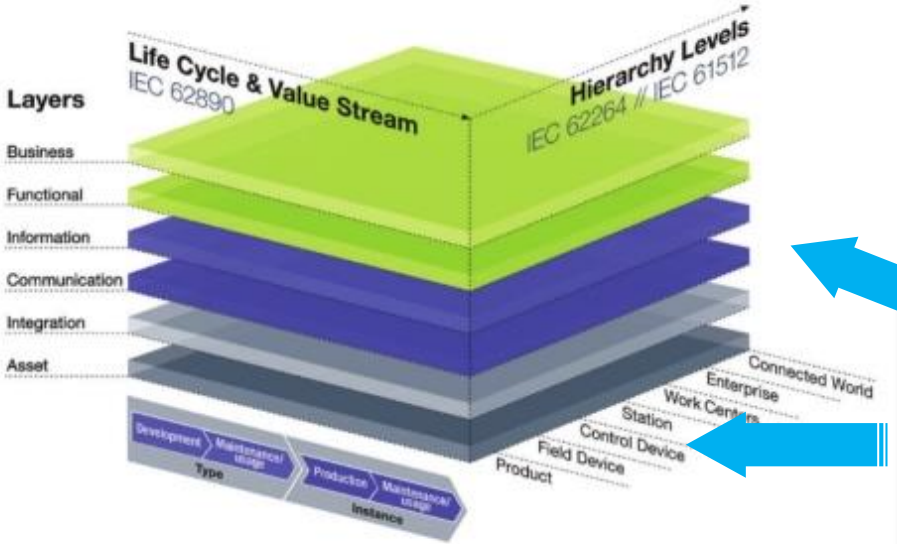


DE NOUVELLES FONCTIONS, PLUS DE COMMUNICATIONS

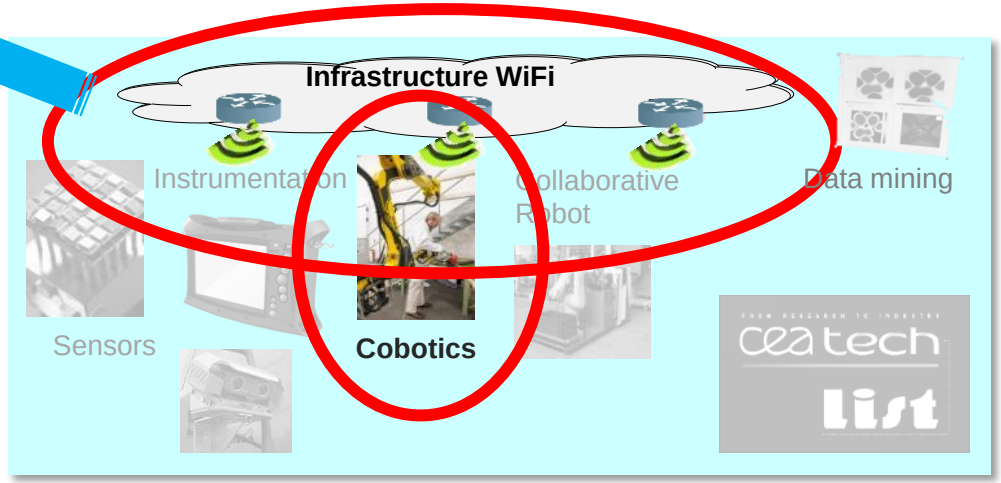
➔ **De nouvelles fonctions critiques : *Contrôle d'un cobot***

« le robot sort de la cage… »

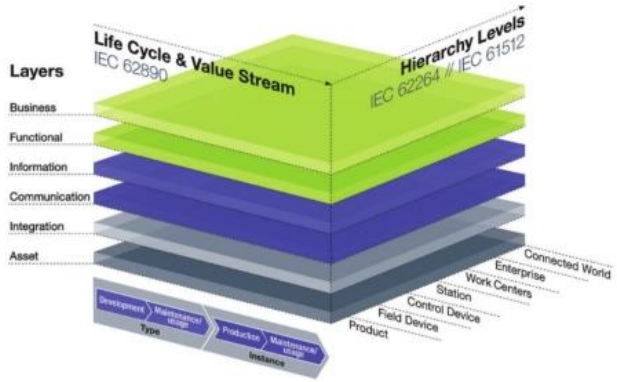
➔ ***Création de « cages logicielles »…***
Quid de la sûreté du logiciel ?
Quelle certification ?

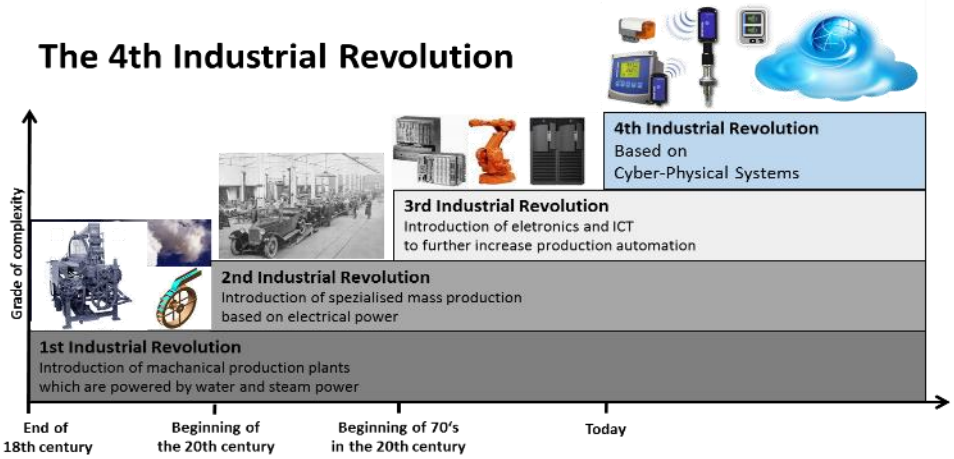


➔ **Décloisonnement, communication :**
Quid de la sécurité des données ?



DE NOUVELLES FONCTIONS, PLUS DE COMMUNICATIONS





Deux enjeux critiques :

✓ ***La constitution d'une vision système globale cohérente***

✓ ***La maîtrise du logiciel et de la sûreté / sécurité***

Retour sur les besoins de la transition numérique

1) La transition numérique est inévitable et touche tous les secteurs et tous les domaines de l'industrie, bien au-delà de l'industrie informatique

→ La question de l'intégration du numérique est alors non seulement une question **d'ingénierie logicielle**, mais bien **d'ingénierie système** devant intégrer de plus en plus de facettes et composants numériques

2) Pour être tenable elle doit s'attacher à la valorisation des métiers industriels afin de **préserver le patrimoine métier et humain**

→ L'informatique doit se rendre accessible aux métiers, domaines et savoir associer **standardisation** et **personnalisation**

3) Elle doit **bénéficier à tous : les grands groupes et les PMEs**

→ Le coût d'accès et d'exploitation doivent rester minimaux

4) Elle doit drainer **l'innovation et la recherche**

→ Fournir les supports de formation, capitalisation et fédération

Une transition numérique durable pour tous

Deux verrous essentiels

1. **Ingénierie système et déclinaisons métier ➔ Ingénierie des modèles**
   - Le modèle métier est « accessible », il évite de « parler informatique »

Optimisation de la production ➔ Virtualisation des produits
- modélisation et simulation pour raccourcir les temps de développement

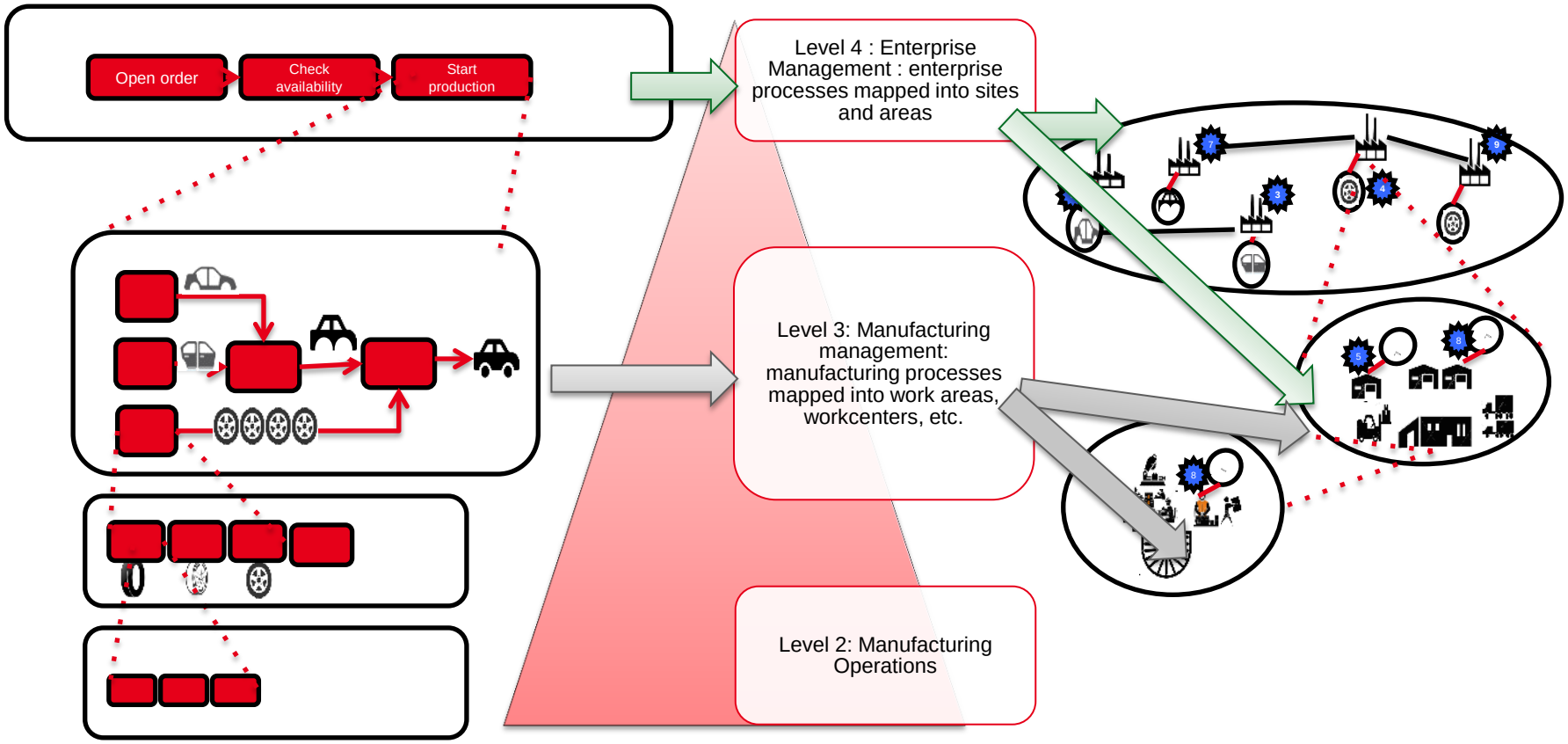
2. **Qualité, sûreté, sécurité, certification ➔ Méthodes formelles**
   - La formalisation permet l'automatisation de l'analyse des systèmes, logicielles et des processus

Zoom sur l'ingénierie des modèles

EXEMPLE : GESTION DE PRODUCTION

Vue processus :
l'enchaînement des tâches

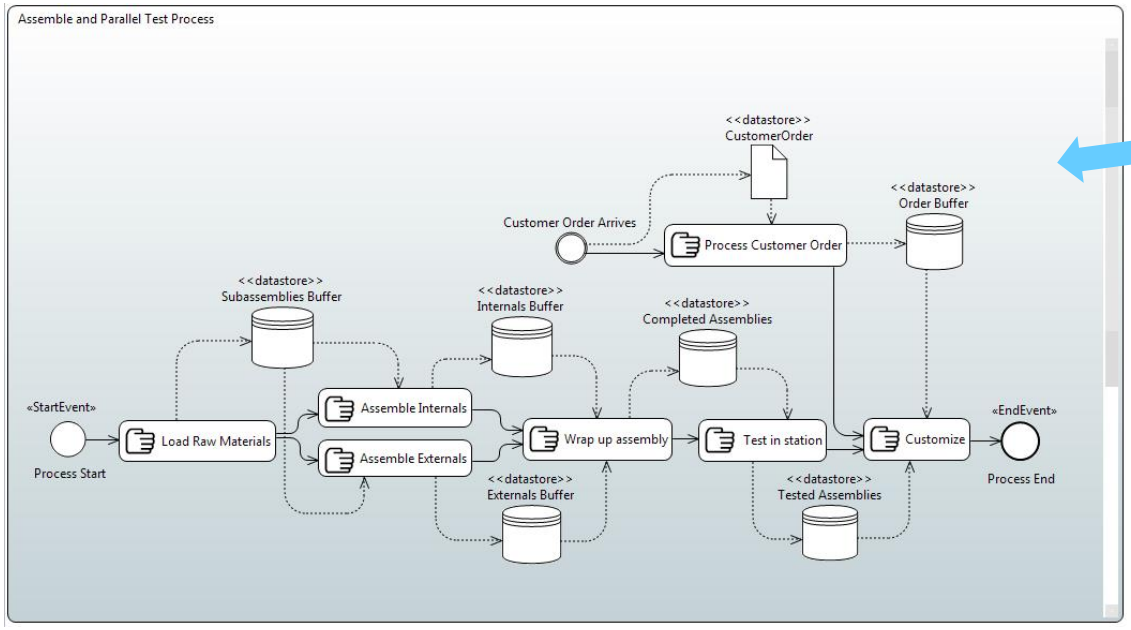
Vue ressource:
capacités, organisation

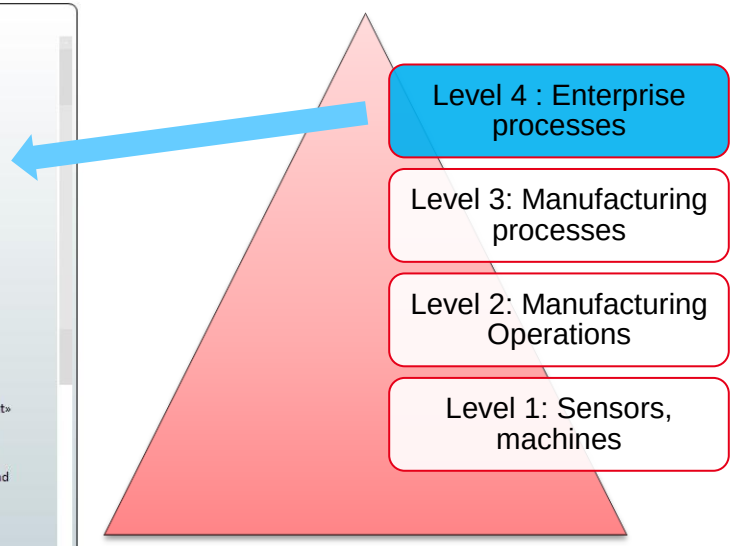


Modéliser pour comprendre, formaliser et optimiser

MODÉLISATION DU PROCESSUS

Processus usine global / Responsable de production





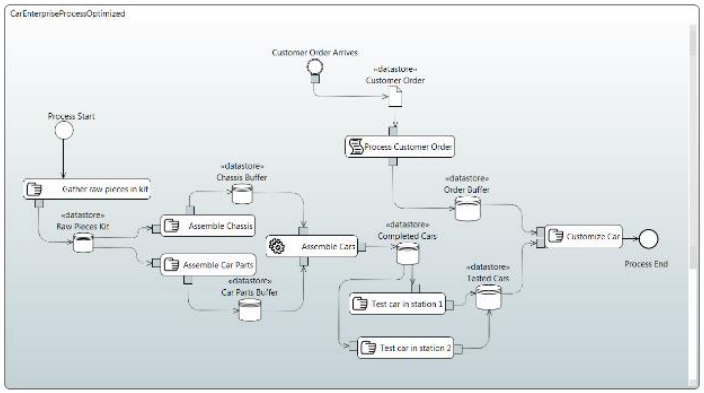
➔ configuration usine

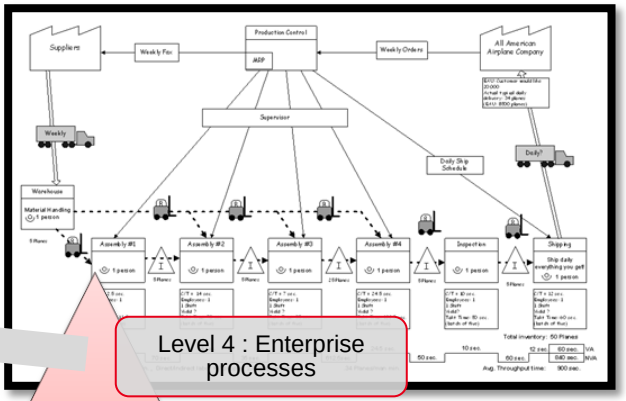
➔ Des standards ouverts d'ingénierie système

➔ Un langage (normalisé) pour décrire (formaliser)

MODÉLISATION DU PROCESSUS

Processus usine global





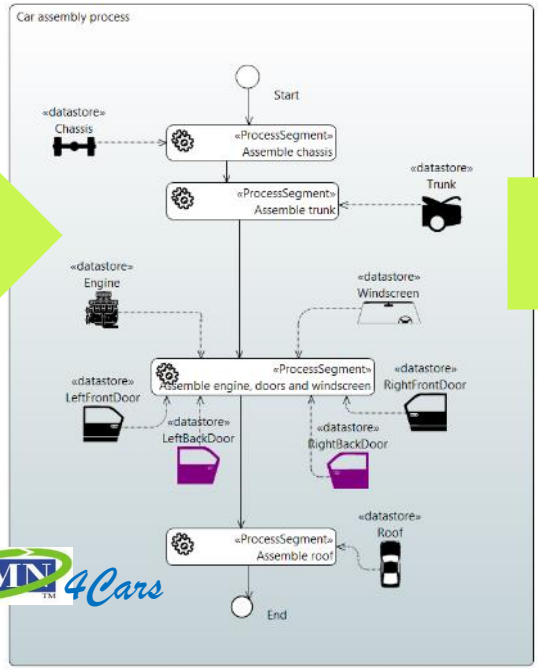
Level 4 : Enterprise processes

Level 3: Manufacturing processes

Level 2: Manufacturing Operations

Level 1: Sensors, machines

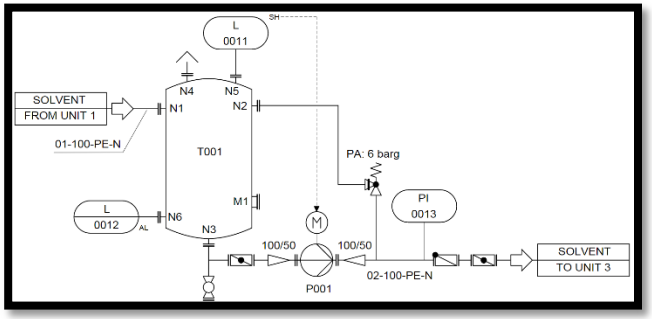
Processus fabrication véhicule



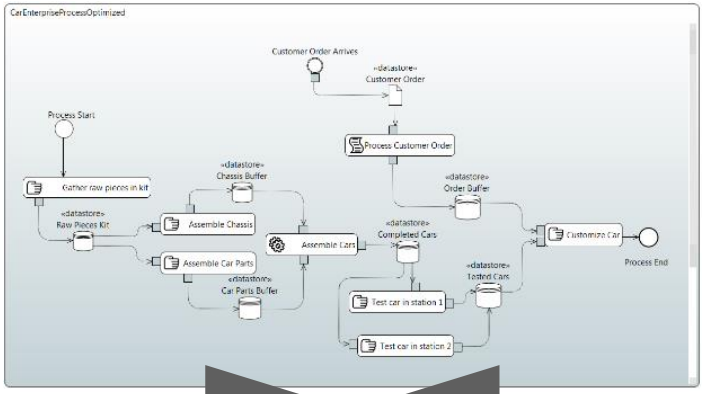
BPMN 4Cars

➔ Le même langage pour le niveau fabrication

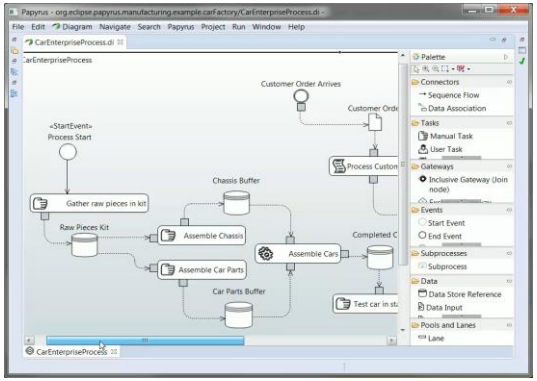
➔ Spécialisation métier pour l'accessibilité

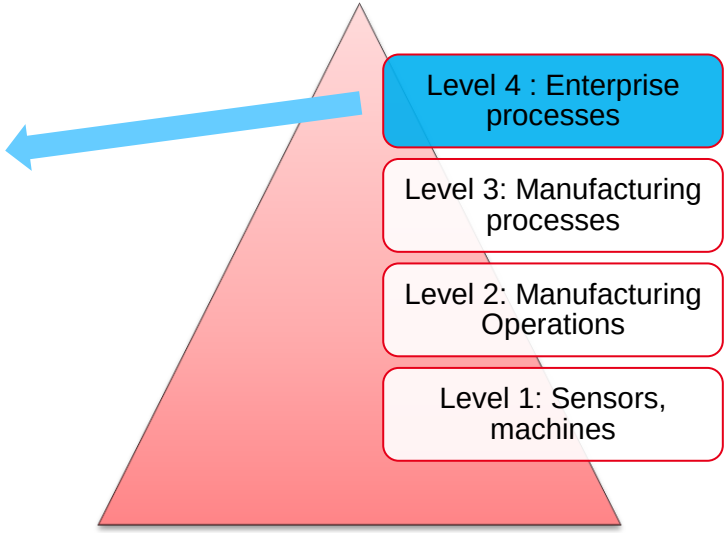


Processus usine global / Responsable production

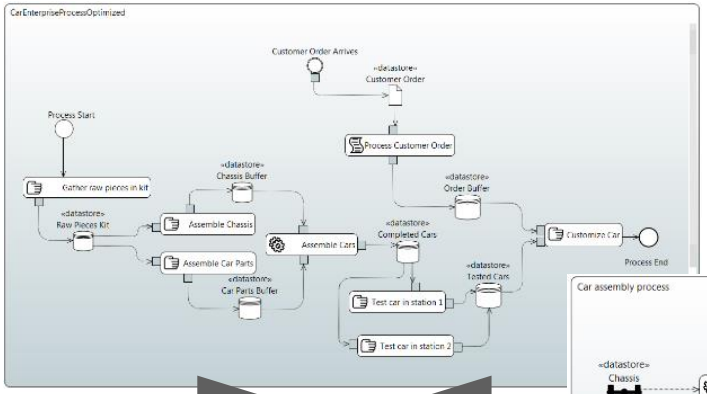


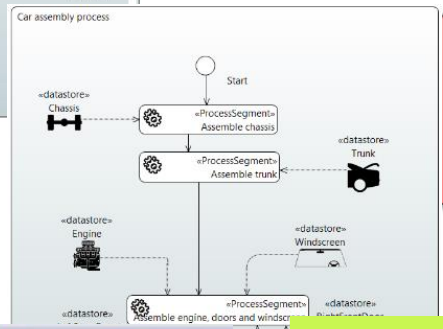
Simulation & Optimisation



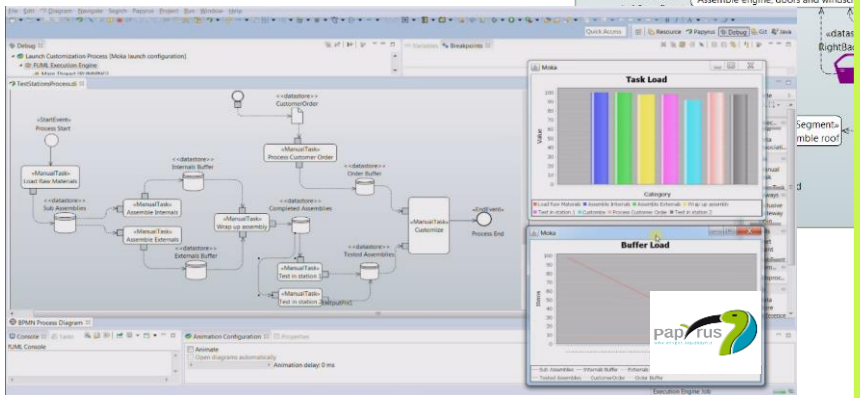


Processus usine global / Responsable production





Simulation & Optimisation



- Level 4 : Enterprise processes
- Level 3: Manufacturing processes
- Level 2: Manufacturing Operations
- Level 1: Sensors, machines

Un atelier couvrant modélisation, spécialisation, simulation…

Le modèle devient le référentiel commun
L'utilisateur le perçoit en vues métier

Zoom sur la sécurité logicielle

LA SÉCURITÉ LOGICIELLE : UN VRAI ENJEU

- 2007: A generator self-destruct after an experimental cyberattack in a powerplant
- 2008: A polish teenager takes control (via internet) of a tram and makes it derailing.
- 2010: STUXNET worm was targeting the Iranian nuclear program
- 2010: Wireless sensors used for carjacking

Sources: Staged cyber attack reveals vulnerability in power grid

September 26, 2007 | From CNN's Jeanne Meserve

Share Twitter Email

Recommend 23 recommendations. S what your friends reco

Researchers who launched an experimental cyber attack caused a generator to self-dest alarming the federal government and electrical industry about what might happen if such were carried out on a larger scale, CNN has learned.

Print Tweet J'aime 8

Polish teen derails tram after hacking train network

Turns city network into Hornby set

By **John Leyden** • **Get more from this author**

Posted in Enterprise Security, 11th January 2008 11:56 GMT

Free whitepaper – King's College LondonUses IBM BNTRackSwitch for HPC

Le programme nucléaire iranien, cible de Stuxnet ?

Edition du 22/09/2010 Réagissez Partager

Plusieurs experts qui travaillent sur ce ver pensent que le réacteur Iranien de Bushehr était la cible.

Le ver informatique très sophistiqué qui s'est propagé en Iran, Indonésie et Inde a été élaboré pour détruire un seul objectif: le réacteur nucléaire de Bushehr en Iran. C'est le consensus qui se dégage des experts en sécurité qui ont examiné Stuxnet. Ces dernières semaines, ils ont cassé le code de chiffrement du programme et ont observé la façon dont le ver fonctionne dans des environnements de test. Les chercheurs s'accordent sur le fait que Stuxnet a été conçu par un attaquant très sophistiqué - peut-être un État - et il a été imaginé pour détruire quelque chose de grand.

Wireless Car Sensors Vulnerable to Hackers

Researchers figure out how to hijack sensor communications.

By Robert Lemos TUESDAY, AUGUST 10, 2010

Hackers could 'hijack' the wireless pressure sensors built into many cars' tires, researchers have found. Criminals might then track a vehicle or force its electronic control system to malfunction, the University of South Carolina and Rutgers University researchers say.

Wireless kit: The equipment used to hijack a car's tire sensors included a laptop, a programmable radio

The team, which successfully hijacked two popular tire-pressure-monitoring systems (TPMS), will describe the work at the USENIX Security conference in Washington, DC, this week.

The tire-sensor attack poses little immediate risk to drivers. However, in recent months, research groups have identified other security weaknesses in vehicle electronics systems. As automakers add more powerful computers to cars, and connect those computers to critical components, in-car systems will need to be secured against hackers, experts warn.

NDIA
National Defense Industrial Association
Promoting National Security Since 1919

CYBERSECURITY FOR ADVANCED MANUFACTURING

a
White Paper
prepared by
National Defense Industrial Association's
Manufacturing Division
and
Cyber Division

May 5, 2014

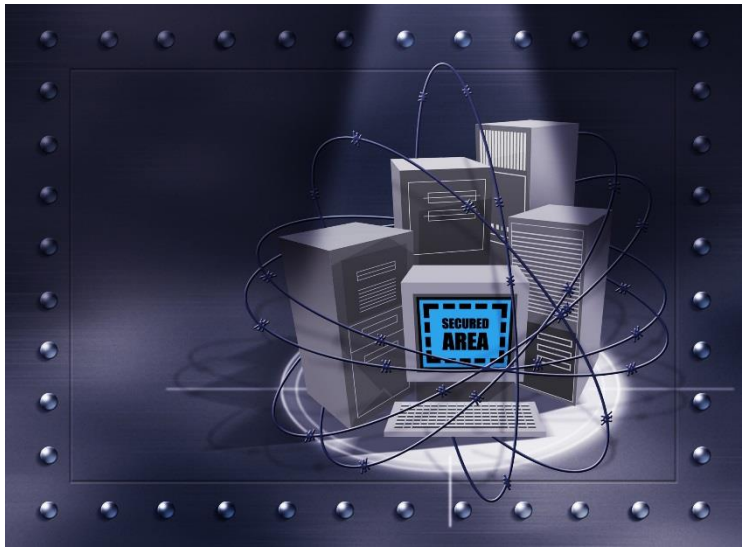
What's Different about ICS

Industrial Control Systems compared to IT

- ICS are long-lived capital investments (15-30 year life)
  - *Old processors, operating systems, network protocols, and configuration management.*
  - *Little processing power. Incompatible with IT cybersecurity products.*
  - *New systems architected for security, but hard to interoperate with old*
- "Production mindset" with little tolerance for OT down time
  - *Operate in real time with critical safety implications – cannot install patches without scheduled downtime and testing*
  - *System availability valued over integrity or confidentiality. Weak privilege management among operators and maintainers who troubleshoot the systems. Growing use of wireless devices.*
  - *Nascent cybersecurity awareness. Poor password management, etc.*
- Manufacturing differs from other ICS applications (Power Grid et al.)
  - *Every manufacturing job brings new executable code into system*
  - *Tech data flowing through the system is a target*

SÉCURITÉ LOGICIELLE DANS L'USINE

- L'usine n'est pas un coffre fort !



Système physiquement étendu

Des réseaux de communications étendus

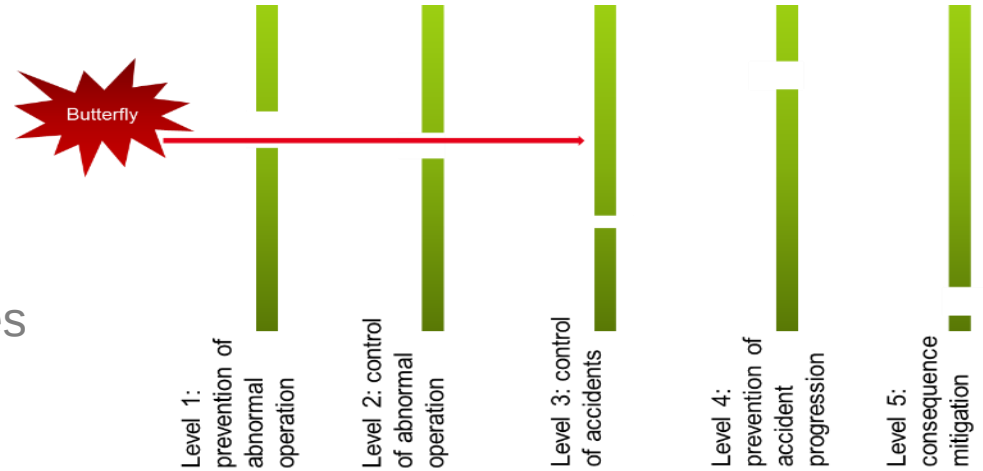
Beaucoup d'équipements hétérogènes à tous les niveaux

Des systèmes/équipements/logiciels achetés sur étagère

Pas de référenciel « sécurité » dur

LE ROBOT SORT DE LA CAGE
ETABLIR LA SÛRETÉ DES LOGICIELS

- Analyse de qualité logicielle
- Constitution de barrières
- Analyse et pondération des risques



- Test : basé sur l'expert ou le hasard
  - Technologies simples
  - Ne conclut pas avec certitude
  - Temps selon l'inquiétude…
    → peut être très long (70% du coût)
- Techniques formelles : démontrer mathématiquement des propriétés
  - Ex. débordement de buffer
  - Relation entrée / sortie

~~?? « *Difficile d'accès, passage à l'échelle* » ??~~

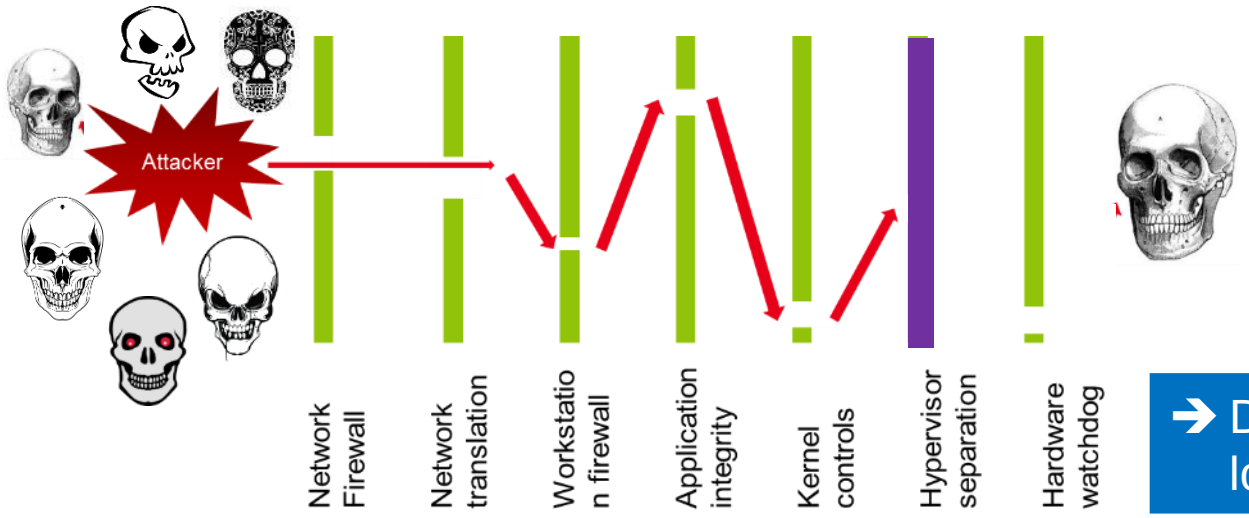
Dans le critique : usage historique et ciblé des techniques formelles

Généralisées, intégrées aux compilateurs + avancées techniques et méthodologiques : tests et preuves se combinent/complètent et passent à l'échelle des logiciels grand public

SÛRETÉ VERSUS SÉCURITÉ

➔ **Securité :** Modification nature des risques

- Attaques « intelligentes »
- Probabilités élevées/non mesurables : « cibles »



➔ Les attaquants sont nombreux et ont des moyens importants

➔ Il faut remonter très haut la difficulté des attaques

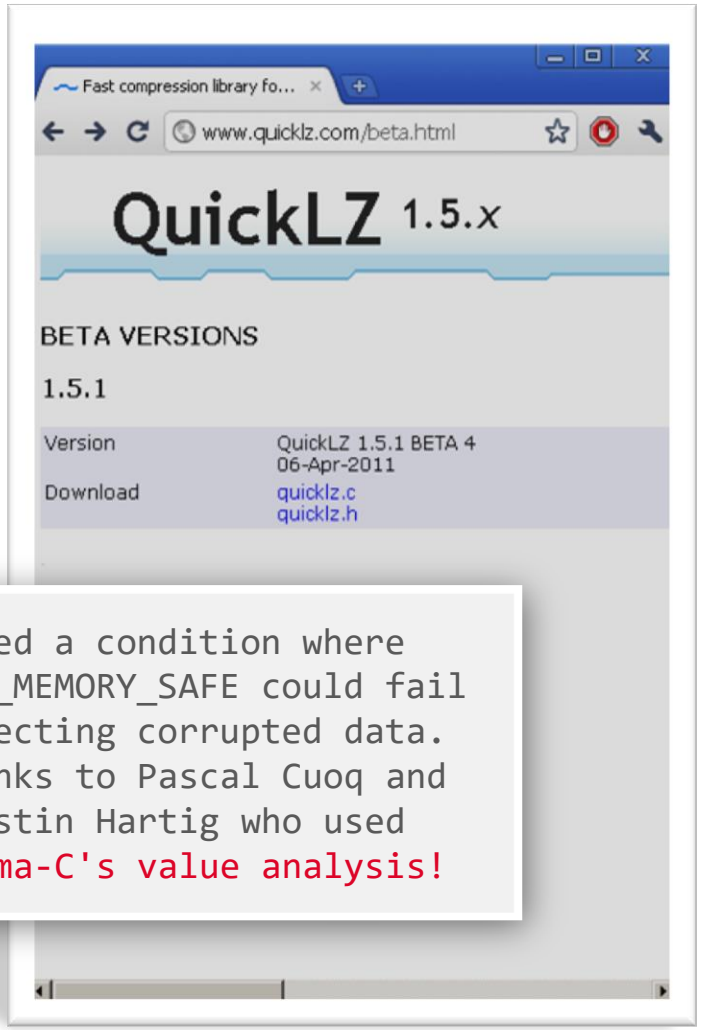
➔ Des outils pour des logiciels sans défaut

Adapter et cibler les preuves aux propriétés liées à la sécurité

Les failles peuvent être partout, exemple : une bibliothèque de compression d'image

How do we reach the sophisticated "last vulnerabilities" in core IT components?

- *Detect all occurrences of a given category of vulnerabilities.*
- *Using automated code analyses*
- *Analysis of the normative context*

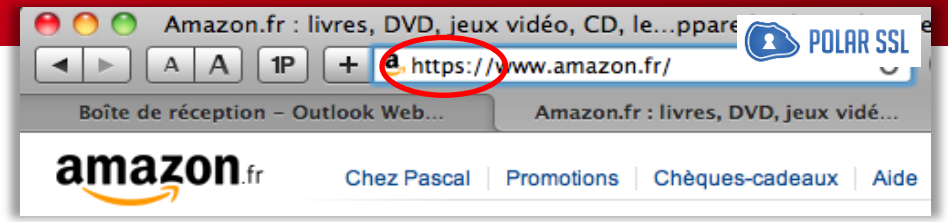


Utilisation d'outils d'analyse formelle

frama C

EMC² where information lives · facebook · AGFA

PRINCIPE DE FONCTIONNEMENT



- **Recherche des zones à risque** *(expertise, bibliothèque de risques)*
- **Analyse des domaines de valeurs possibles :**
  modèles formels du programme, calcul et preuve des domaines d'exécution

➔ **Verdict sur le risque et correction si besoin**

Before

trunk/library/ssl_tls.c — Tabular | Unified

```
r1194
881        * Always compute the MAC (RFC4346, CBCTIME).
882        */
883       ssl->in_msglen -= ssl->maclen + padlen );
884
```

No test for writing outside of the authorized zone

trunk/library/ssl_tls.c

Authorized zone verification

```
r1194 r1221
881   881    * Always compute the MAC (RFC4346, CBCTIME).
882   882    */
      883    if( ssl->in_msglen <= ssl->maclen + padlen )
      884    {
      885        SSL_DEBUG_MSG( 1, ( "msglen (%d) < maclen (%d) + padlen (%d)",
      886                            ssl->in_msglen, ssl->maclen, padlen ) );
      887        return( POLARSSL_ERR_SSL_INVALID_MAC );
      888    }
      889
883   890    ssl->in_msglen -= ( ssl->maclen + padlen );
884   891
```

After

Construction de logiciels intrinsèquement sécurisé (absence de familles entières de failles)
Très supérieur aux tests statistiques ou empilements de barrières

Vers une démarche plate-forme

LES GRANDS FOURNISSEURS D'OUTILS SE RECONFIGURENT

- Développement d'offres d'ingénierie système, PLM, ERP, ALM…
- Conception mécanique/physique, simulation, suites logicielles
- Offres verticalisées et guides méthodologiques de grands fournisseurs

- **Mais est-ce suffisant ?** **… ce n'est pas sûr !**

Coût d'accès ?

Spécialisation métier ?

Langage commun ?

Intégration vs juxtaposition ?

Innovation continue ?

Capitalisation ?

Stabilité vs évolutivité ?

La 4ième révolution industrielle nécessite une nouvelle approche des outils

Plate-forme ouverte pour l'ingénierie logicielle et systèmes

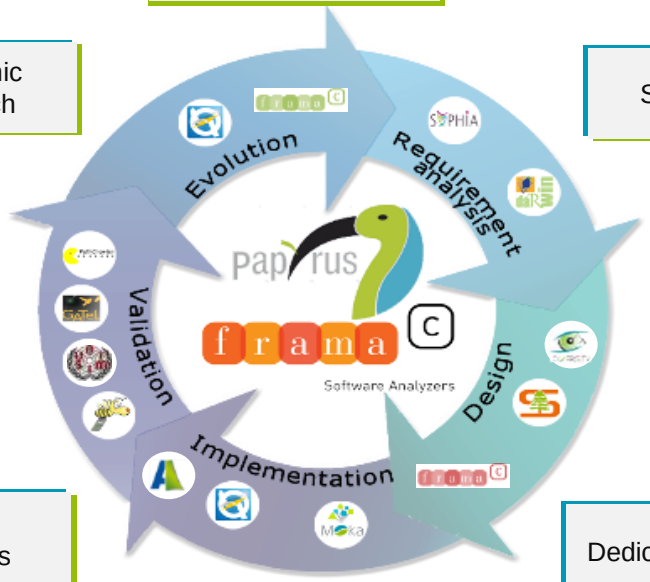
- **La démarche plate-forme : capitaliser, factoriser, intégrer, inter-opérer**
  - **Eviter** les démarches sectorielles de **solutions indépendantes**
  - **Mutualiser** les expressions de besoins, abstraire, généraliser
  - **Coordonner** les projets, développements inter domaines, inter exploitants
  - **Centraliser** les démarches de formations, maintenance, support
  - **Partager** les coûts pour réduire les barrières à l'appropriation

- **L'open source pour réduire et partager l'investissement initial : un moteur de fédération, déclencheur de transitions numériques**
  - Coût initial centré sur le **minimum** nécessaire à l'**intégration métier**
  - Impose une démarche **qualité rigoureuse** pour l'intégration de l'innovation
  - **Evite** la dispersion et le **blocage commercial** sur des offres figées
  - Pousse au développement de solutions/services commerciaux **centrés besoins**
  - **Attracteur** international des **innovations** académiques

Open source

Modélisation système

Academic research



Standards

Techniques formelles

Bibliothèques métiers

Global solutions

Dedicated tools

Bibliothèques métier

Une plate-forme open source d'ingénierie système et logiciel offrant les outils/solutions les plus avancés du moment

Les outils : c'est critique !

Exigez plus !

MERCI !