

- 
- Certification :
- Origines et importance pour les systèmes informatiques
 - Concepts de base et recherches induites

G. MOTET
LESIA / INSA Toulouse

gilles.motet@insa-tlse.fr www.lesia.insa-tlse.fr





Overview

- Embedded real-time software systems
 1. Statement: Increasing of their responsibilities
 2. Requirements: Assurance of absence of risks
 3. Solution: Certification
 4. Certification for new software technologies

Increasing of their responsibilities

- A. Responsibilities to improve product performance



- Not prone to ageing => implementation reliability



- Ignition of sparks => car reliability



- Flexibility => adaptable behaviours



- Ignition / valve opening control => lowest emission



- Easiness => complex behaviours



- Shock absorber laws => more comfortable

Increasing of their responsibilities

- B. Responsibilities to take charge of bad use of the product



Driving actions => Harms



Software actions -> Harm prevention



Too high speed => Accident

ESP & ABS -> Skid prevention

Increasing of their responsibilities

- C. Responsibilities to take charge of inadequacies of other technologies used in the product



Mechanical part = Ageing => deteriorated states



Software -> acceptable states / detection

Ageing of mechanical techno. => Excessive emission

Software control system -> detection and/or correction

Ex. Gaz recycling (EGR)



Increasing of their responsibilities

- D. Responsibilities to take charge of design faults of other components of the product

Car mechanically unstable at braking time



to prevent harms (skids)

Increasing of their responsibilities

- E. Responsibilities to act & decide

Decision



Action



Example

ABS



Overview

- Embedded real-time software systems

1. Statement: Increasing of their responsibilities

2. Requirements: Assurance of absence of risks

3. Solution: Certification

4. Certification for new software technologies

A contradiction

- Embedded software size & complexity increasing
 - => failure risk increasing
- Embedded software responsibility increasing
 - => failure risk acceptability decreasing
- More responsibilities => More guarantees



Requirements for more guarantees

- A justified suspicion
 - Citizens as product users (car failures & recalls)
 - Authorities as citizens require more assurance
 - Engineers as designers: long testing period
 - Firms as producers
 - Harms: trade and financial risks: penalties

Example of harms

- Toyota lawsuits
- September 1998: Court of California:
 - Recall requirement (software fault in an on-board system)
 - 330 000 cars x 250\$ > 82 million \$
- July 1999: US Department of Justice:
 - Recall of 2.2 million of cars = 250 million \$
 - + 58 BILLION \$ (civil fine)

Overview

- Embedded real-time software systems
 1. *Statement: Increasing of their responsibilities*
 2. *Requirements: Assurance of absence of risks*
 3. **Solution: Certification**
 4. *Certification for new software technologies*

Certification

- A third-party gives written assurance of the conformance
- Conformance to safety requirements: no harms

Certification

- Often considered
 - by engineers as
 - additional constraints
 - a way to judge their activities
 - by firms as
 - overcosts
 - additional issues

Certification

- Whereas it provides
 - for engineers
 - good practices to increase assurance
 - low responsibilities (using the best practices)
 - for firms
 - a trade advantage
 - a partial transfer of responsibilities to certification authorities

Toyota: end of story

- California court: 24 February 2000
 - No recall as Toyota software system complied ARB certification process
- California court settlement: March 2002
 - 7.9 million \$ for environmental projects
- Federal court settlement: March 2003
 - 20 million \$ for projects to reduce emission
 - 500 000 \$ for fine
- To be compared to 250 M\$ (recall)+58B\$ (fine)

Overview

- Embedded real-time software systems

1. *Statement: Increasing of their responsibilities*

2. *Requirements: Assurance of absence of risks*

3. *Solution: Certification*

- 4. Certification for new software technologies**

Certification issues

- Partial transfer of responsibilities to certification authorities
- Potential consequences: New requirements
 - Limitation of software system responsibilities (ex. SIS)
 - Limitation of software system complexity
 - Use only conventional software technologies
 - More assurance requirements: previous + + +
- Example: Object-Oriented design
- Coûts par secteurs : avionique, ferroviaire, ...

Attentes des organismes de certification

- Apporter la garantie de la sécurité/safety
- Sécurité = Absence de risques inacceptables (Guide 51 / ISO)
- Deux questions :
 - Quels risques ?
 - Comment en assurer l'absence ?
- Travaux LESIA :
 - Risques technologiques (UML, Java) + fonctionnels
 - Approche standard (Guide 73 / ISO)

Approche standard : Gestion du risque

- Risk identification (phenomenon, etc.)
 - associated with the technology & its use
 - Harms & Benefits
- Risk estimation
 - Seriousness & probability
- Risk evaluation -> Acceptability
- Risk treatment (reduction)
- Risk communication

Identification : source des dommages

- Quels dommages ? fautes dans modèles ou prog.
- Quels sources ?
- Individu + Phénomène danger. => évt domm. => Dommage
- Individu + Energie cinétique => choc => Blessure
- Ingénieur + Techno logicielle => erreur humaine => faute

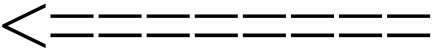
Identification : source des dommages

- Individu + Phénomène danger. => évt domm. => Dommage
- Ingénieur + construction lang => Erreur compréh. => faute
- Phénomène dangereux : Héritage
- Situation dangereuse : surcharge par une variable lors d'un héritage
- Evt domm. : Surcharge d'une variable ayant un sens différent
- Dommage : accès non autorisé à une variable par une méthode héritée

Identification des sources des dommages

- Java : par la littérature. ex. OOTiA
- UML : Modèle de faute / Norme 2.0
- Etude des bénéfices

Approche standard : Gestion du risque

- Risk identification (phenomenon, etc.)
- Risk estimation 
 - Seriousness & probability
- Risk evaluation -> Acceptability
- Risk treatment (reduction)
- Risk communication

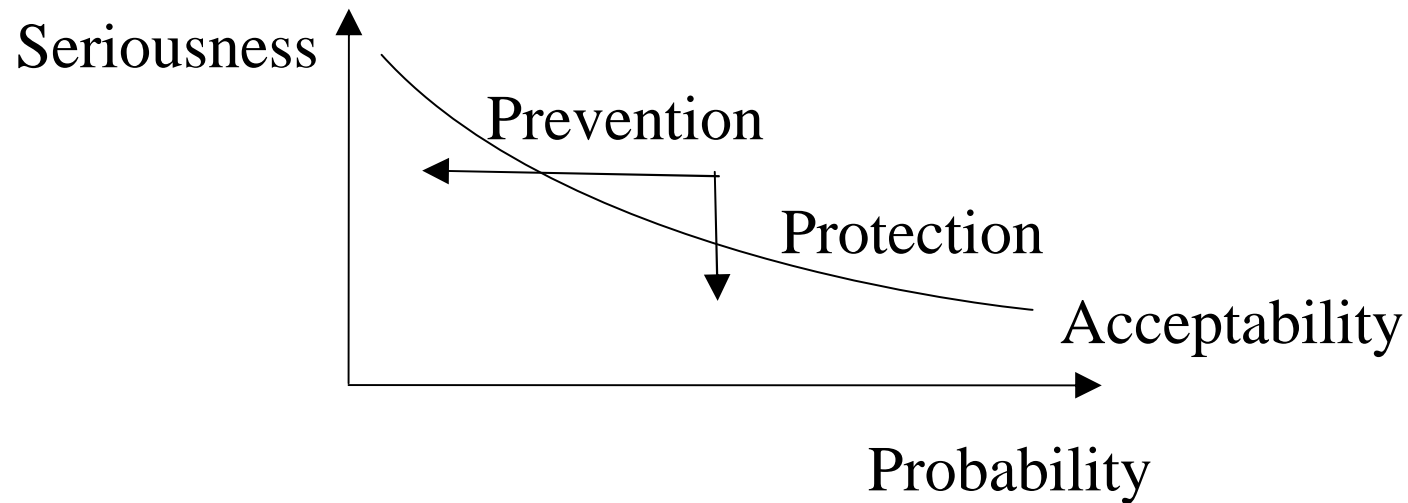


Estimation des risques

- Deux grandeurs :
 - Probabilité des fautes ? (systémique)
 - Gravité : difficulté à détecter
 - ISO 15942 (2000) / Ada

Traitement du risque

- Acceptability (SIL)
- Risk reduction



Traitement des risques

- Individu + Phénom. danger. => évt domm. => Dommage
- Individu + Energie cinétique => choc => Blessure

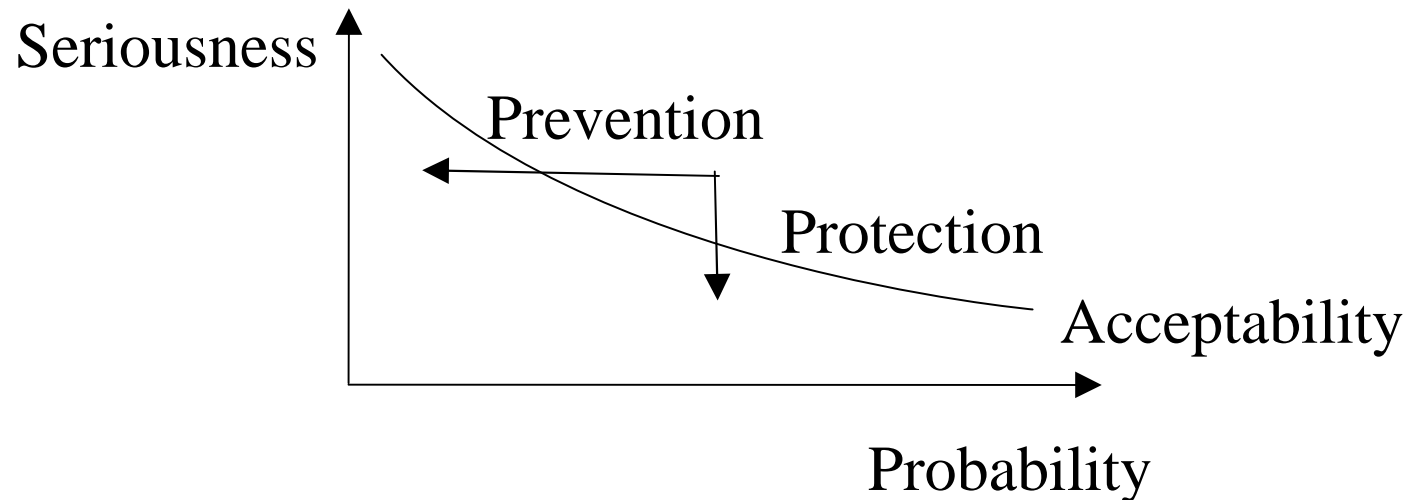
- Réduire la probabilité (prévention) :
 - Barrières
- Réduire la gravité :
 - Phénomène : vitesse réduite
 - Dommage : muscles compliants

Réduction des risques

- Individu + Phénom. danger. => évt domm. => Dommage
- Ingénieur + Techno logicielle => erreur humaine => faute
- Phénomène : restriction des constructions ou de leur usage
 - Pour prévenir les fautes
 - Pour faciliter leurs détections
- Evénement dommageable : Guide de style
 - Pour prévenir les fautes
 - Pour faciliter leurs détections

Acceptabilité

- Mettre en avant les bénéfices
- Evaluer le rapport Dommages / Bénéfices



Current studies

- Java technology (language and virtual machine)
 - Thales Avionics
- UML technology
 - Avionics: Airbus, Aonix, Thales + CEAT & CNRT AE
 - Military systems: DGA & ONERA
- Based on a risk management approach (ISO Guide 73) showing
 - Harms & Benefits to safety

Personnes

- Louise TYSK (CIFRE Thales)
- Hugues MALGOUYRES (DGA)
- Jean-Pierre SEUMA VIDAL (MNRT)
- Stéphane LERICHE (Thales Avionics)
- Gilles MOTET (LESIA – INSA)
- + collaborations

- 
- ## Certification :
- Origines et importance pour les systèmes informatiques
 - Concepts de base et recherches induites

G. MOTET
LESIA / INSA Toulouse

gilles.motet@insa-tlse.fr www.lesia.insa-tlse.fr

