FAULT TOLERANCE IN CONTROL ARCHITECTURES FOR MOBILE ROBOTS : FANTASY OR REALITY ?

CRESTANI D. – GODARY-DEJEAN K.

CAR'2012 – Nancy – 10-11 mai 2012

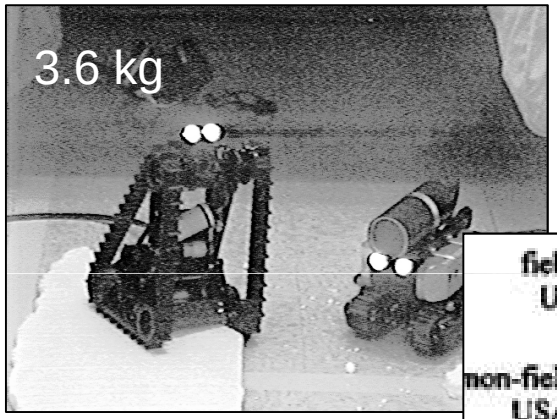
PRÉAMBULE

- FIABILITÉ DES ROBOTS MOBILES : Carlson et Murphy (2005)
- CONCEPTS DE SÛRETE DE FONCTIONNEMENT : Avizienis et al. (2004)
- SYSTÈMES TOLERANTS AUX FAUTES :
  - o Isermann (2006)
  - o Venkatasubramanian (2006)
  - o Zhang et al. (2008)
- TOLÉRANCE AUX FAUTES ET ROBOTS AUTONOMES :
  - o Rapport Shakhimardanov (2006)
  - o Thèse Lussier – LAAS (2007)
  - o Thèse Durand – LIRMM (2011)
  - o Articles LAAS – Chatila / Ingrand et al.
- TOLÉRANCE AUX FAUTES : QUESTIONS OUVERTES
  - o Carlson (2004)
  - o Steinbauer et Wotawa (2011)
  - o Thèse Durand – LIRMM (2011)

PLAN DE L'EXPOSÉ

- FIABILITÉ DES ROBOTS MOBILES
- SÛRETÉ DE FONCTIONNEMENT ET TOLÉRANCE AUX FAUTES
    - o Vocabulaire – Définitions - ….
- PRINCIPES DE LA TOLÉRANCE AUX FAUTES
- TOLÉRANCE ET AUTOMATIQUE
- TOLÉRANCE ET ARCHITECTURES DE CONTRÔLE
    - o Principes
    - o Limitations
    - o Exemples
- DU RÊVE À LA REALITÉ

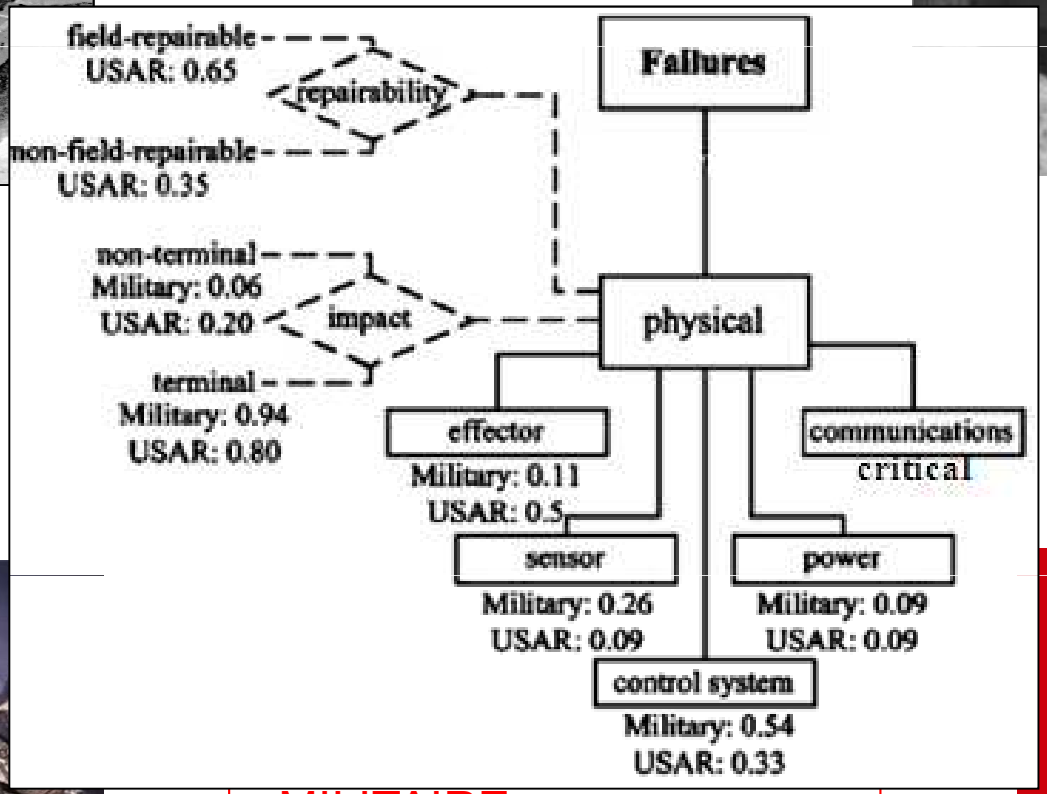
FIABILITÉ DES ROBOTS MOBILES



15 robots mobiles

Sauvetage

Militaire



World Trade Center

- MILITAIRE :
  - 1.6 faute / jour
  - 94 % terminales

Déminage (Bosnie)

SÛRETÉ DE FONCTIONNEMENT

ÉVITER LES FAUTES

ACCEPTER LES FAUTES

- **PRÉVENTION**

(fault prevention)

o Ingénierie

o Modularité

- **ÉLIMINATION**

(fault removal)

o Tests

o Validation formelle

- **PRÉVISION**

(fault forecasting)

o Quelle faute ?

o Quelle incidence ?

- **TOLÉRANCE**

(fault tolerance)

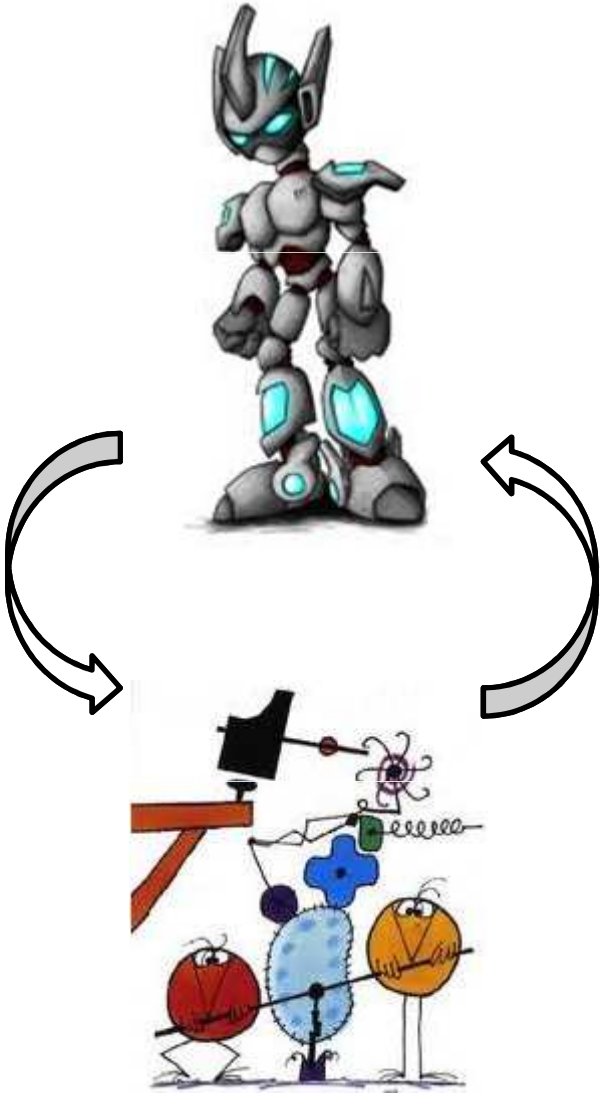
o Détection erreur

o Recouvrement

TOLÉRANCE AUX FAUTES

Capacité à délivrer un service correct en dépit de fautes affectant les différentes ressources d'un système

TOLÉRANCE AUX FAUTES ET ROBOTIQUE



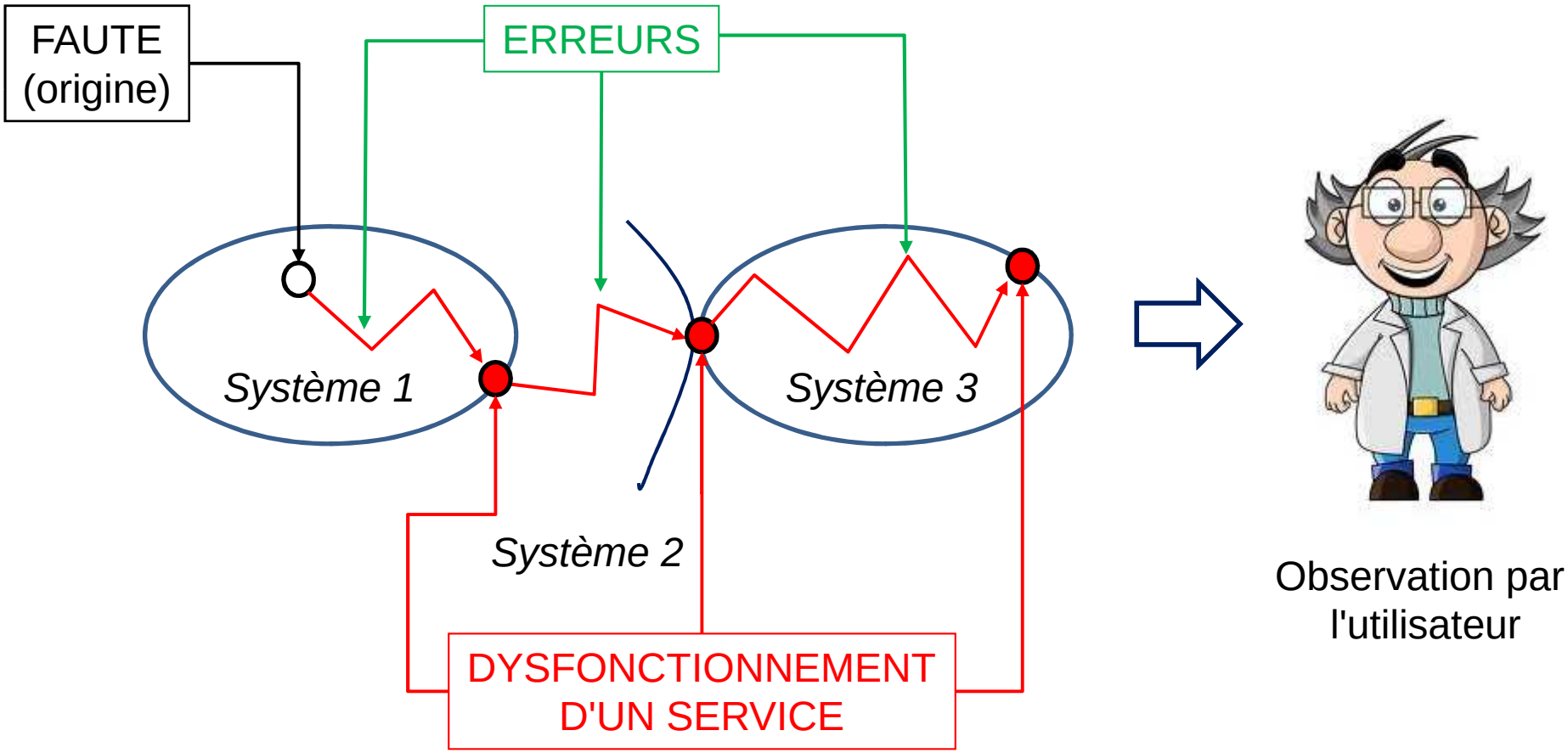
TOLÉRANCE AUX FAUTES

Capacité à délivrer un service correct en dépit de fautes matérielle ou logicielle affectant le système autonome même

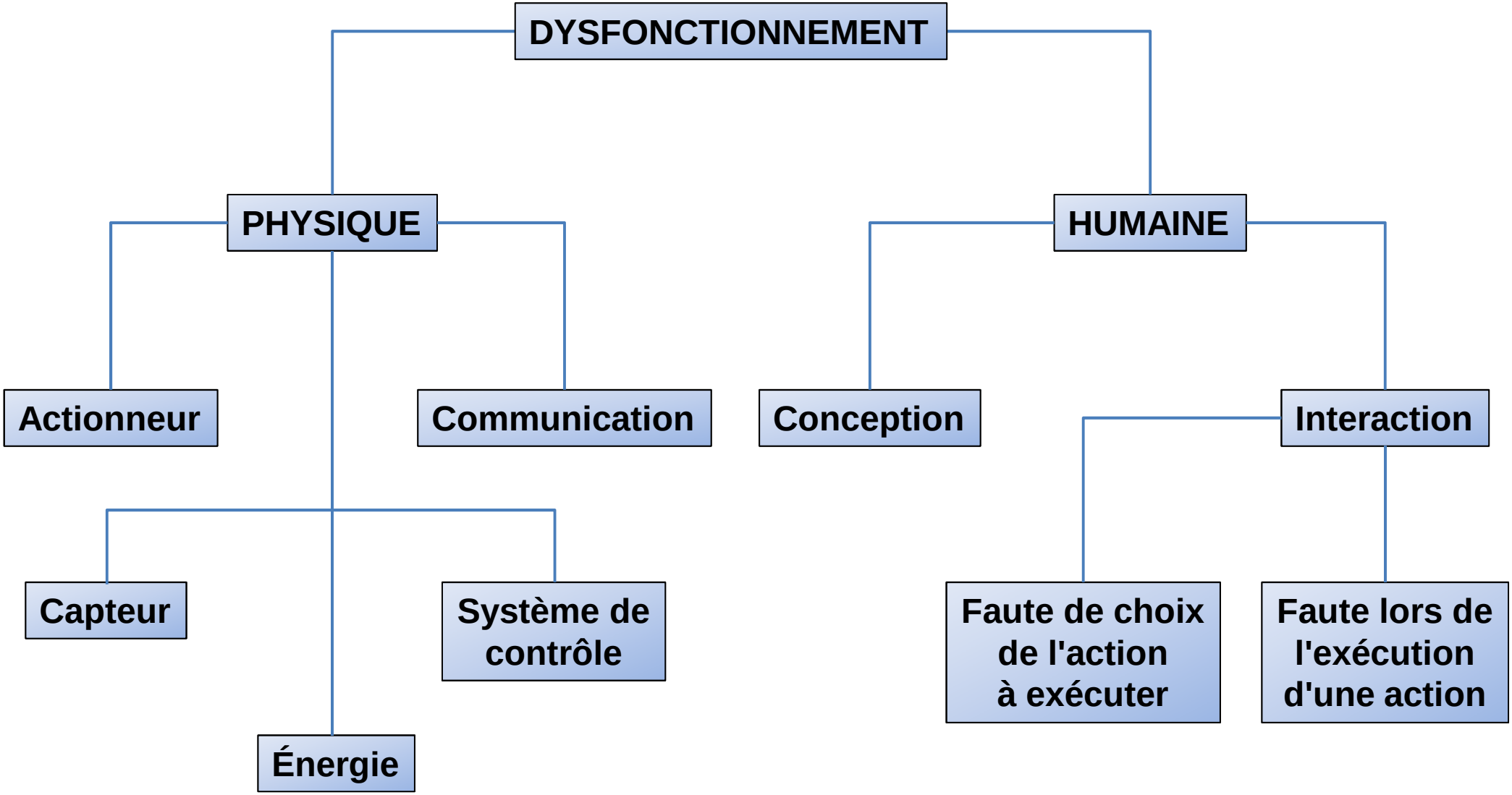
ROBUSTESSE

Capacité d'un système autonome à délivrer un service correct en dépit de fautes induites par la variabilité de son environnement

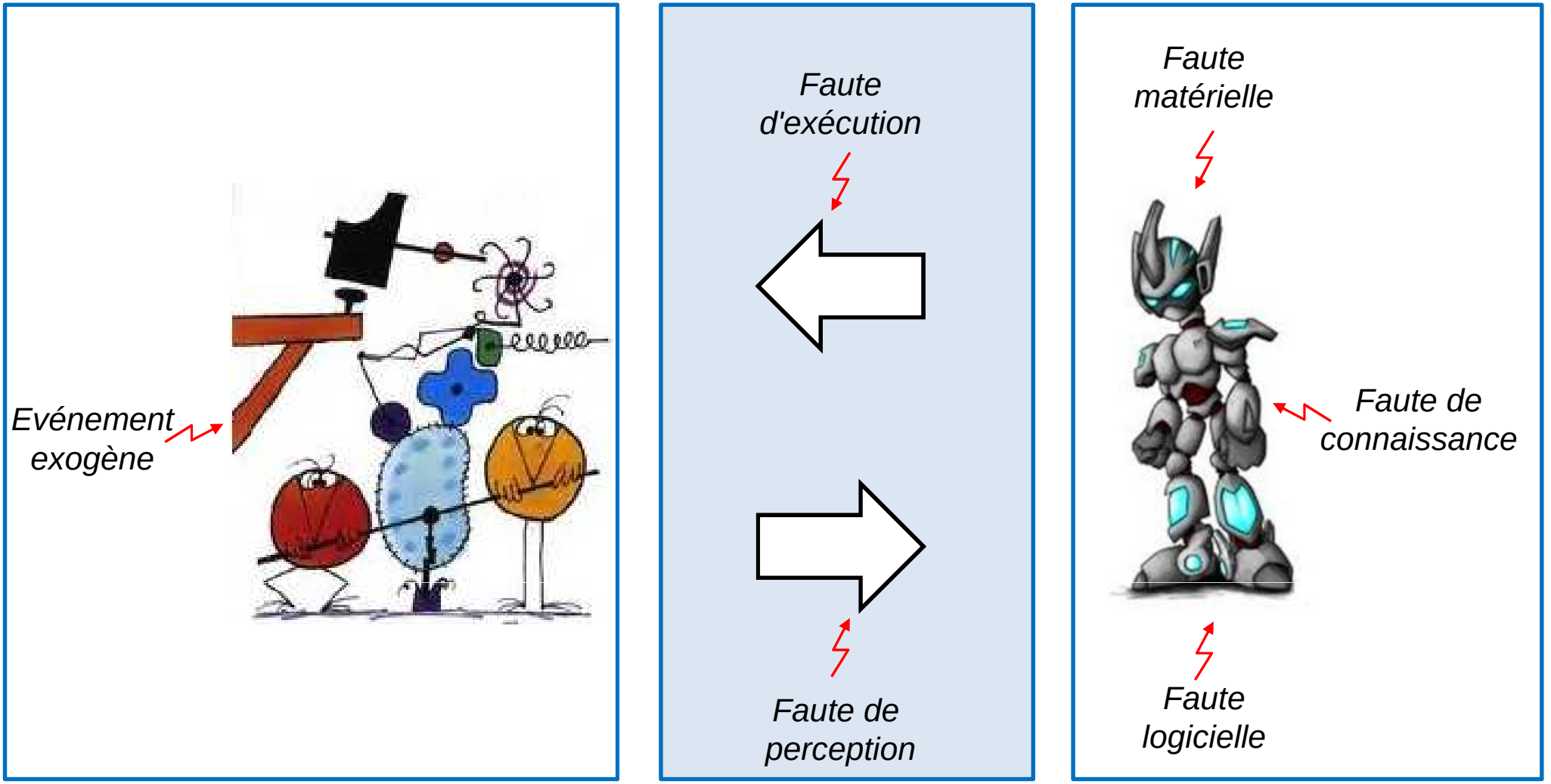
DE LA FAUTE AU DYSFONCTIONNEMENT



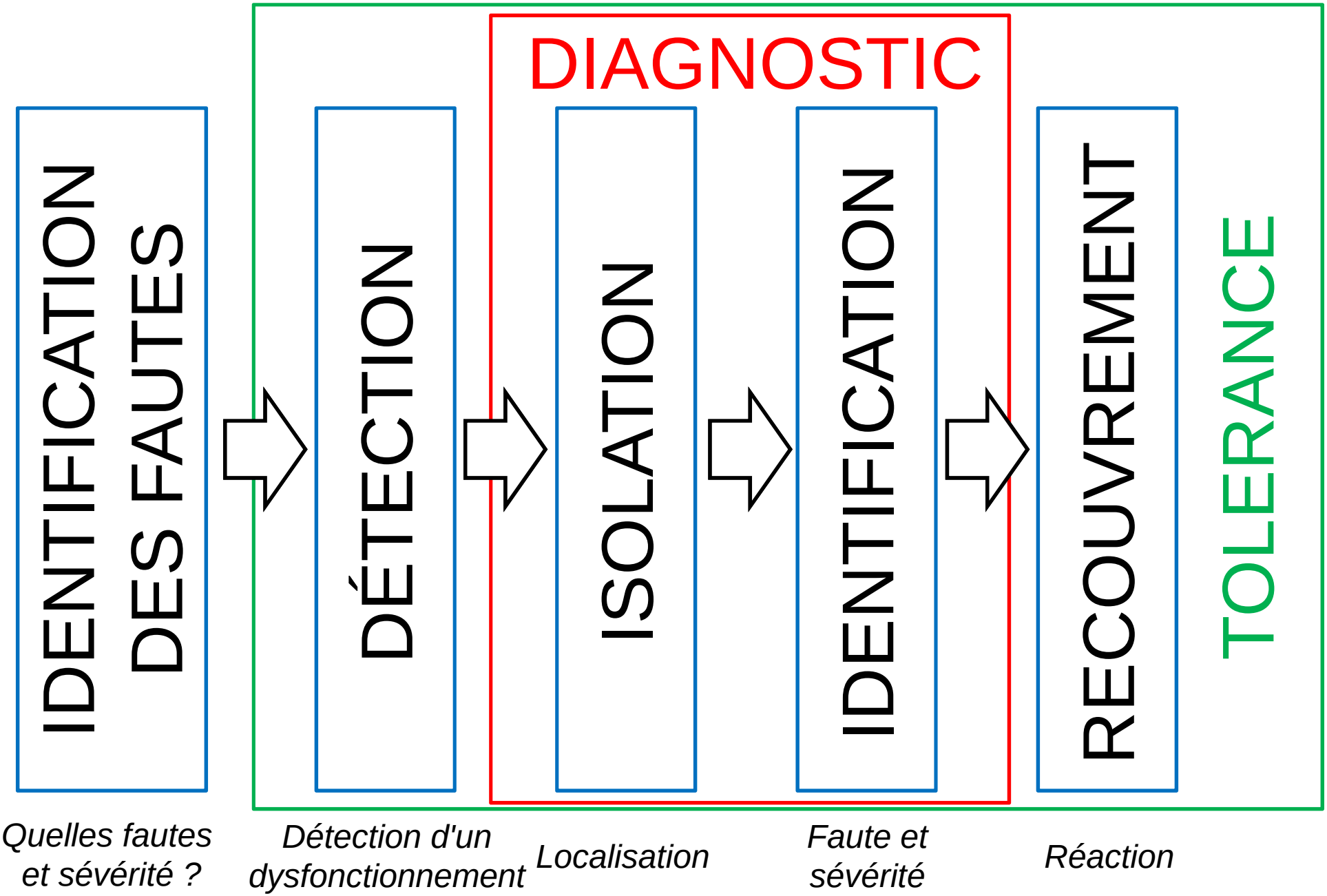
TAXONOMIE DES FAUTES



LOCALISATION DES FAUTES



PRINCIPES DE LA TOLÉRANCE AUX FAUTES



TOLÉRANCE ET AUTOMATIQUE

- **DÉTECTION ET DIAGNOSTIC**

o Méthodes basées modèle
  - Observateur d'états
  - M.M.K.F.
  - Equations de parité
  - Identification paramétrique

o Méthodes basées données
  - Systèmes experts
  - Réseaux de neurones

- **RECOUVREMENT**

o Passif – *contrôleur robuste*
  - Contrôle CRONE
  - H_∞

o Actif
  - Approches multi-modèles
  - Synthèse en ligne

- **LIMITATIONS**

oTraitement temps réel

o Très orientée fautes capteurs et actionneurs

o Manque d'adaptabilité et de flexibilité

TOLÉRANCE ET ARCHITECTURE : PRINCIPES DE DÉTECTION ET DIAGNOSTIC

- **CONTRÔLE DE VRAISSEMBLANCE**

(Reasonableness check)

o Vérification domaine de validité des données

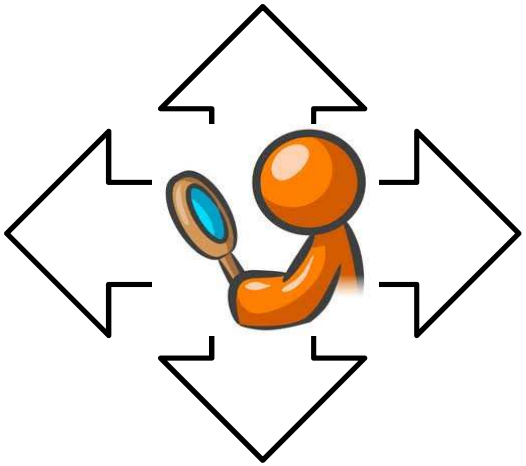
o Respect contraintes matérielles ou logicielles

- **CONTRÔLE TEMPOREL**

(Timing check)

o Rupture de service

o Watch-dog



- **CONTRÔLE DE COMMANDE**

(Safety bag check)

o Respect de propriétés de sécurité

- **SURVEILLANCE POUR LE DIAGNOSTIC**

(Monitoring for diagnosis)

o Approches basées modèle

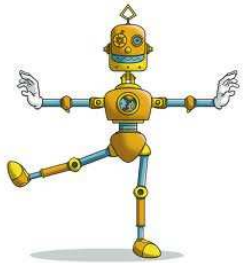
o Fautes capteurs et actionneurs

TOLÉRANCE ET ARCHITECTURE : PRINCIPES DE RECOUVREMENT

NIVEAU PLANIFICATION

NIVEAU EXÉCUTIF

NIVEAU FONCTIONNEL



- **NIVEAU MISSION**
  - o Ajustement du niveau d'autonomie

- **NIVEAU PLANIFICATION**
  - o Re-planification
  - o Réparation de plan

- **NIVEAU EXÉCUTIF**
  - o Traitement spécifique
  - o Re-exécution d'action
  - o Re-exécution d'action avec redondance fonctionnelle
  - o Changement de modalité de fonctionnement

LA TOLÉRANCE DANS LES ARCHITECTURES

- 11 ARCHITECTURES ET FRAMEWORKS ANALYSÉS
- TOLERANCE AUX FAUTES TOUJOURS PRESENTE
- PRISE EN COMPTE DISSEMINÉE DANS LE CODE
- PAS D'IDENTIFICATION PREALABLE DES FAUTES : COTAMA FFT
- PAS DE DIAGNOSTIC : COTAMA FFT / REMOTE AGENT
  - Faute Unique
  - Dysfonctionnement = Faute
- RECOUVREMENT
  - Exécutif : Error Handling – Mise en état sûr
  - Planification : Re-planification
  - Mission : Rare - COTAMA FFT

- **LIMITATIONS**

o Manque d'**intégration** et de **réification** des principes de tolérance aux fautes

ARCHITECTURES ET TOLÉRANCE : EXEMPLES

• REMOTE AGENT (Livingstone)

Domaine spatial (JPL)
Modélisation déclarative

o Détection
- Observation qualitative des capteurs

o Diagnostic : Mode Identification
- Identification du mode : Nominal – Fautif
- Diagnostic : Consistance avec observation
- Algorithme de type best-first search
- Possibilité de *faute inconnue*

o Recouvrement : Mode Reconfiguration
- Re-configuration / Re-Planification / Etat sûr
- Mission : Possible

Principe repris dans l'architecture IDEA

• COTAMA FFT

Conception pour la tolérance

o AMDEC pour la tolérance
- Fautes et sévérité

o Détection
- Techniques usuelles

o Diagnostic
- Analyse de signature

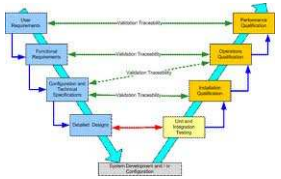
o Recouvrement
- Exécutif : Modalités
- Mission : Ajustement du niveau d'autonomie

Réification des mécanismes de tolérance dans l'architecture

TOLÉRANCE : DU RÊVE À LA RÉALITÉ

- **TOLÉRANCE ORIENTÉE DOMAINE APPLICATIF**
  - Type environnement / sécurité / coût
  - Limitation du nombre et du type de fautes

- **CONCEPTION POUR LA TOLÉRANCE AUX FAUTES**
  - Démarche globale
    - Mécanique – Matériel – Automatique – Logiciel (Architecture)



- **CONCEPTION D'UNE ARCHITECTURE POUR LA TOLÉRANCE**
  - Méthodologie d'intégration
  - Analyse approfondie des fautes à envisager
  - Spectre de détection plus large (capteur / actionneur)
  - Un véritable diagnostic (raisonnement – mono/multi fautes)
  - Une palette plus large (exécutif – planification – mission) et pertinente (performance) de méthodes de recouvrement

- **MÉTRIQUES ET BENCHMARKS POUR LA CERTIFICATION**
  - Indispensable pour l'industrialisation des robots mobiles autonomes