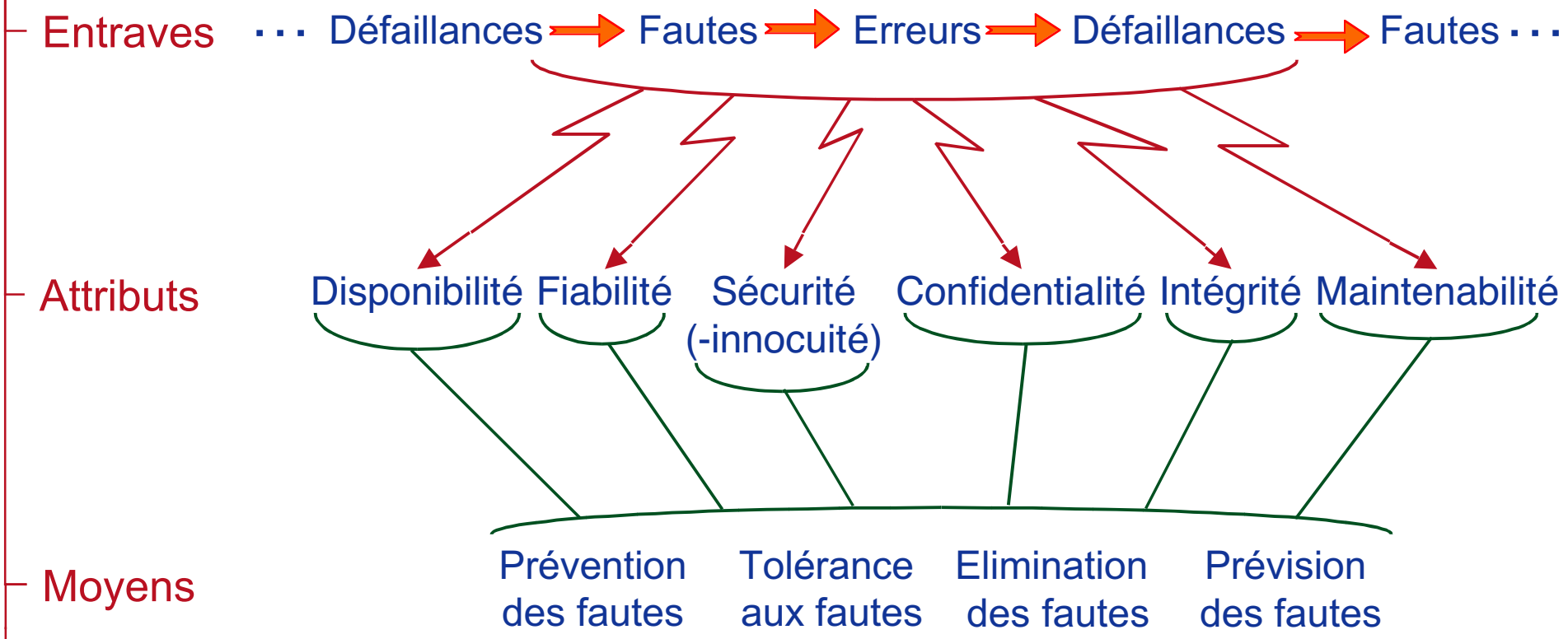
De la sûreté de fonctionnement à la résilience

Jean-Claude Laprie

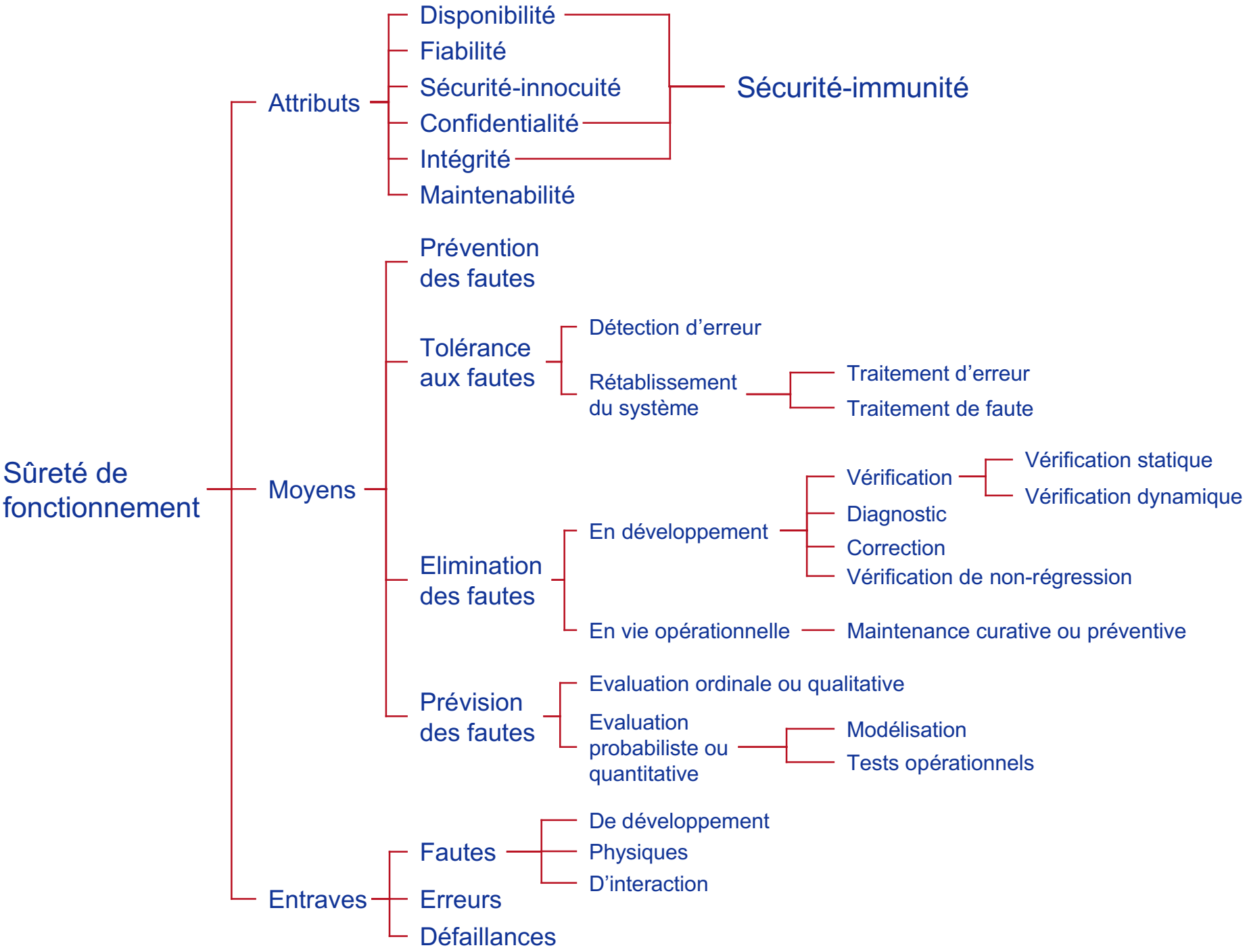
Problématiques scientifiques : avancées et défis
— 7, 8 et 9 octobre 2008 —

- La sûreté de fonctionnement : un concept intégrateur
- Quelques développements marquants
- Etat de l'art : statistiques
- Les systèmes ubiquitaires : le contexte émergent
- La résilience : un cadre pour affronter les défis ouverts
- Conclusion

Sûreté de fonctionnement : aptitude à délivrer un service de confiance justifiée

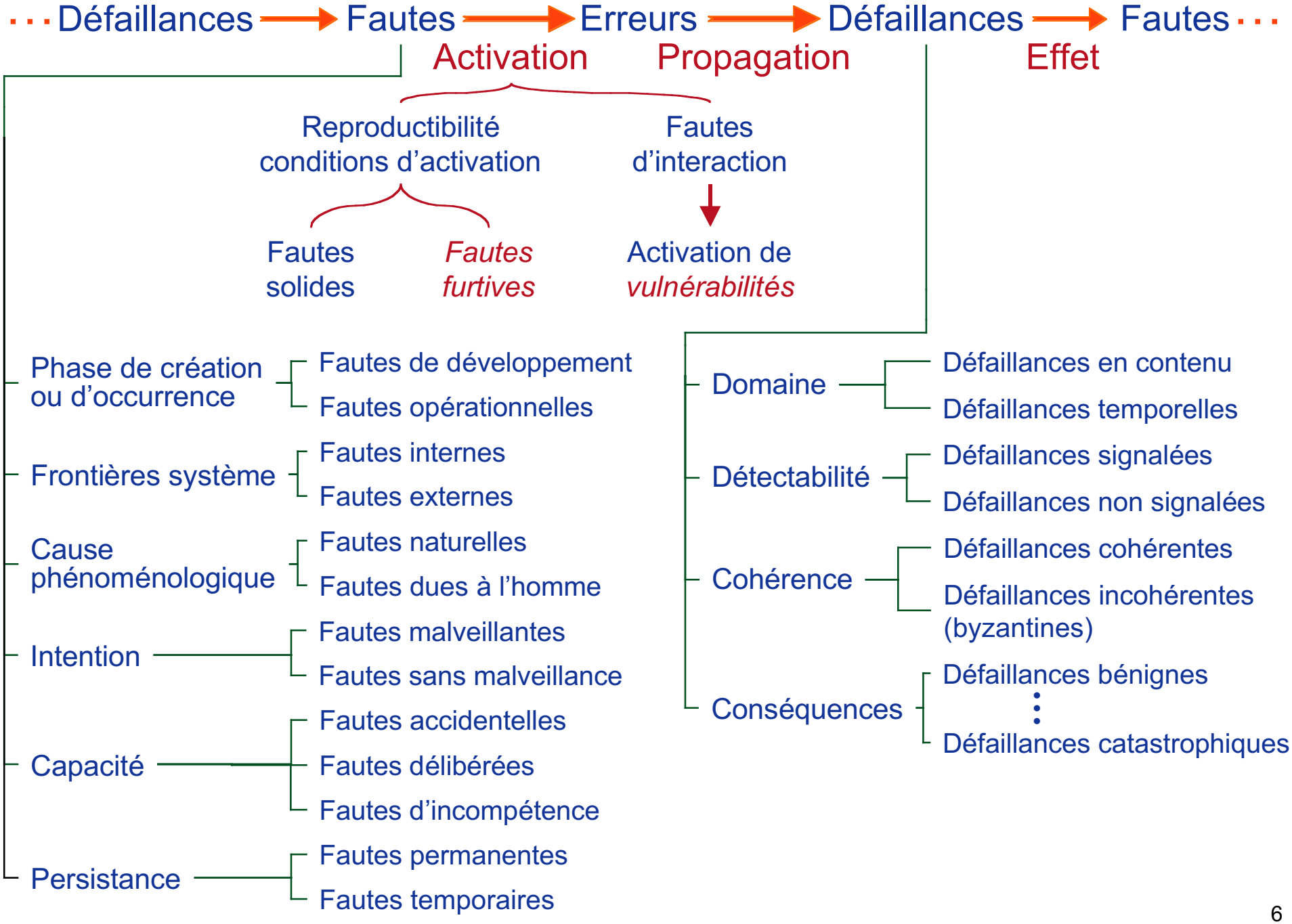


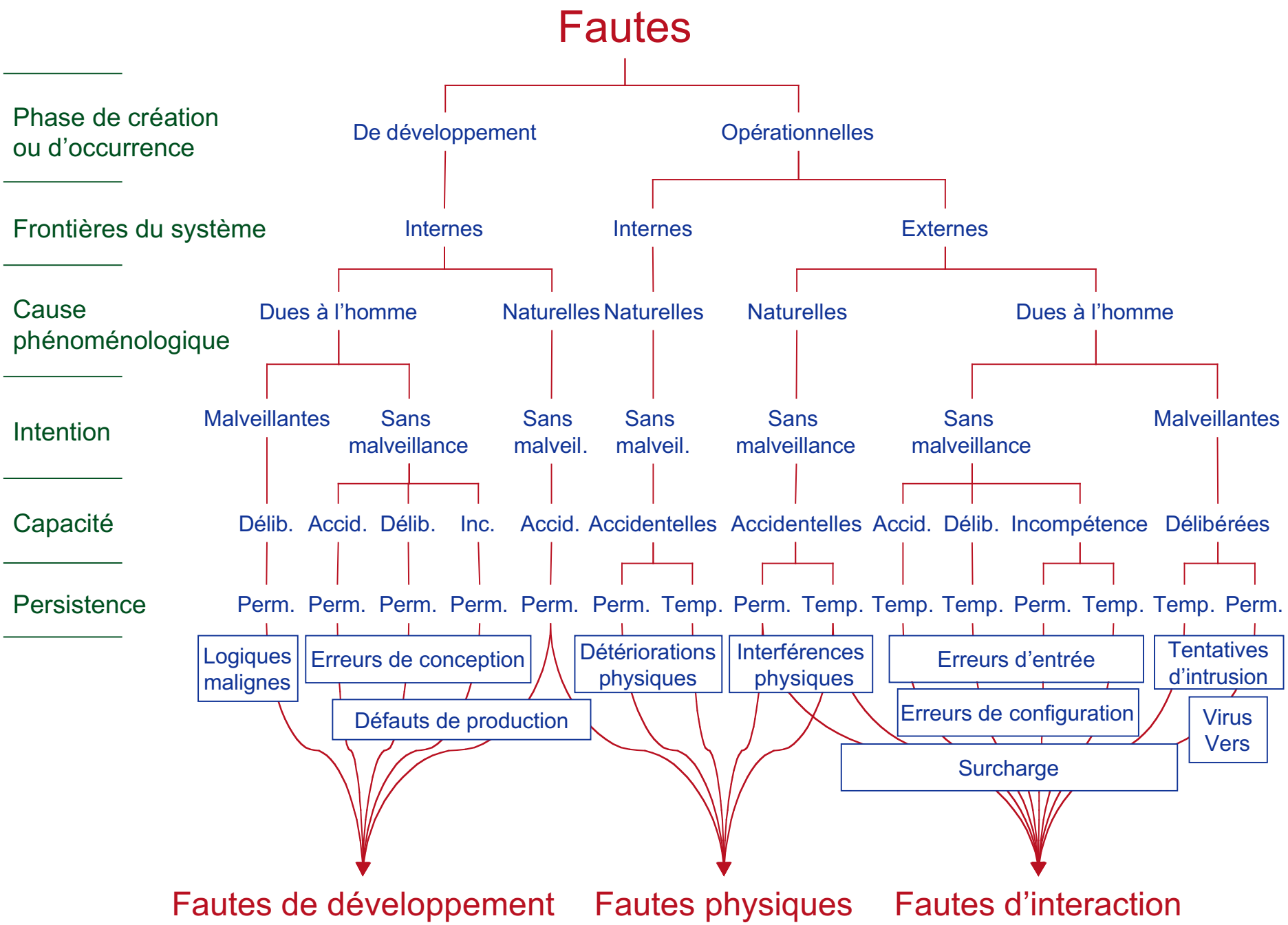
Sûreté de fonctionnement : Aptitude à éviter des défaillances du service plus fréquentes ou plus graves qu'acceptable


Sûreté de fonctionnement
Attributs
Disponibilité
Fiabilité
Sécurité-innocuité
Confidentialité
Intégrité
Maintenabilité
Sécurité-immunité
Moyens
Prévention des fautes
Tolérance aux fautes
Détection d'erreur
Rétablissement du système
Traitement d'erreur
Traitement de faute
Elimination des fautes
En développement
Vérification
Vérification statique
Vérification dynamique
Diagnostic
Correction
Vérification de non-régression
En vie opérationnelle
Maintenance curative ou préventive
Prévision des fautes
Evaluation ordinale ou qualitative
Evaluation probabiliste ou quantitative
Modélisation
Tests opérationnels
Entraves
Fautes
De développement
Physiques
D'interaction
Erreurs
Défaillances

Attributs de la sûreté de fonctionnement

- Disponibilité, fiabilité, sécurité, confidentialité, intégrité, maintenabilité : attributs primaires
- Attributs secondaires
  - Spécialisation
    - ✓ Robustesse : persistance de la sûreté de fonctionnement en présence de fautes externes
    - ✓ Survivabilité : persistance de la sûreté de fonctionnement en présence de fautes actives
    - ✓ Résilience : persistance de la sûreté de fonctionnement en face de changements fonctionnels, environnementaux, technologiques
  - Distinction de divers types de (meta-)information
    - ✓ Responsabilité : disponibilité et intégrité de la personne qui a effectué une opération
    - ✓ Authenticité : intégrité du contenu et de l'origine d'un message, et éventuellement d'autres informations, comme l'instant d'émission
    - ✓ Non-réfutabilité : disponibilité et intégrité de l'identité de l'émetteur d'un message (non-réfutation de l'origine), ou du destinataire (non-réfutation de la destination)


· · · Défaillances
Fautes
Erreurs
Défaillances
Fautes · · ·
Activation
Propagation
Effet
Reproductibilité
conditions d'activation
Fautes
d'interaction
Fautes
solides
Fautes
furtives
Activation de
vulnérabilités
Phase de création
ou d'occurrence
Fautes de développement
Fautes opérationnelles
Frontières système
Fautes internes
Fautes externes
Cause
phénoménologique
Fautes naturelles
Fautes dues à l'homme
Intention
Fautes malveillantes
Fautes sans malveillance
Capacité
Fautes accidentelles
Fautes délibérées
Fautes d'incompétence
Persistance
Fautes permanentes
Fautes temporaires
Domaine
Défaillances en contenu
Défaillances temporelles
Détectabilité
Défaillances signalées
Défaillances non signalées
Cohérence
Défaillances cohérentes
Défaillances incohérentes
(byzantines)
Conséquences
Défaillances bénignes
Défaillances catastrophiques


Fautes
Phase de création ou d'occurrence
Frontières du système
Cause phénoménologique
Intention
Capacité
Persistence
De développement
Opérationnelles
Internes
Internes
Externes
Dues à l'homme
Naturelles
Naturelles
Naturelles
Dues à l'homme
Malveillantes
Sans malveillance
Sans malveil.
Sans malveil.
Sans malveillance
Sans malveillance
Malveillantes
Délib.
Accid.
Délib.
Inc.
Accid.
Accidentelles
Accidentelles
Accid.
Délib.
Incompétence
Délibérées
Perm.
Perm.
Perm.
Perm.
Perm.
Perm.
Temp.
Perm.
Temp.
Temp.
Temp.
Perm.
Temp.
Temp.
Perm.
Logiques malignes
Erreurs de conception
Défauts de production
Détériorations physiques
Interférences physiques
Erreurs d'entrée
Erreurs de configuration
Surcharge
Tentatives d'intrusion
Virus Vers
Fautes de développement
Fautes physiques
Fautes d'interaction

- Force du concept de sûreté de fonctionnement
  - Caractère intégrateur
    - ✓ Mise en perspective de disponibilité, fiabilité, sécurité, confidentialité, maintenabilité, etc., en tant qu'attributs
    - ✓ Expression des inévitables compromis, rendus nécessaires par les conflits entre attributs
  - Modèle faute-erreur-défaillance
    - ✓ Compréhension et maîtrise des entraves
    - ✓ Présentation unifiée
- Concept et terminologie largement adoptés par la communauté internationale
  - IEEE Fault-Tolerant Computing Symposium + IFIP Dependable Computing for Critical Applications Conference ➠ IEEE/IFIP Conference on Dependable Systems and Network

- La sûreté de fonctionnement : un concept intégrateur
- Quelques développements marquants
- Etat de l'art : statistiques
- Les systèmes ubiquitaires : le contexte émergent
- La résilience : un cadre pour affronter les défis ouverts
- Conclusion

Prévention des fautes

- Développement mathématiquement formel : méthode B
- Amélioration processus de développement

Tolérance aux fautes

- Protocoles d'accord 'byzantin' ⟷ Processeurs à silence sur défaillance ✳
- Fautes de développement
  - Fautes solides : développement diversifié ✳
  - Fautes furtives : points de reprise dans architectures faiblement couplées
  - Rajeunissement du logiciel
  - Vérification en ligne d'assertions
- Tolérance aux intrusions ✳
- Tolérance adaptative ✳

✳ Sujets auxquels le groupe Tolérance aux fautes et Sûreté de Fonctionnement a contribué, souvent comme pionnier

Elimination des fautes

- Vérification de modèle
- Test du logiciel
  - Test statistique
  - Test formel
  - Test de robustesse

Prévision des fautes

- Construction, validation et traitement de modèles de grande taille (qq. 10^5 états)
  - Réseaux de Petri stochastiques
  - Raideur des modèles
- Théorie unifiée fiabilité matériel et logiciel et évaluation de systèmes matériel-et-logiciel
- Evaluation de la sécurité (-immunité)
- Injection de fautes
- Etalonnage de la sûreté de fonctionnement

Jean Arlat

Christian Beounes †

Yves Crouzet

Yves Deswarte

Jean-Charles Fabre

Mohamed Kâaniche

Karama Kanoun

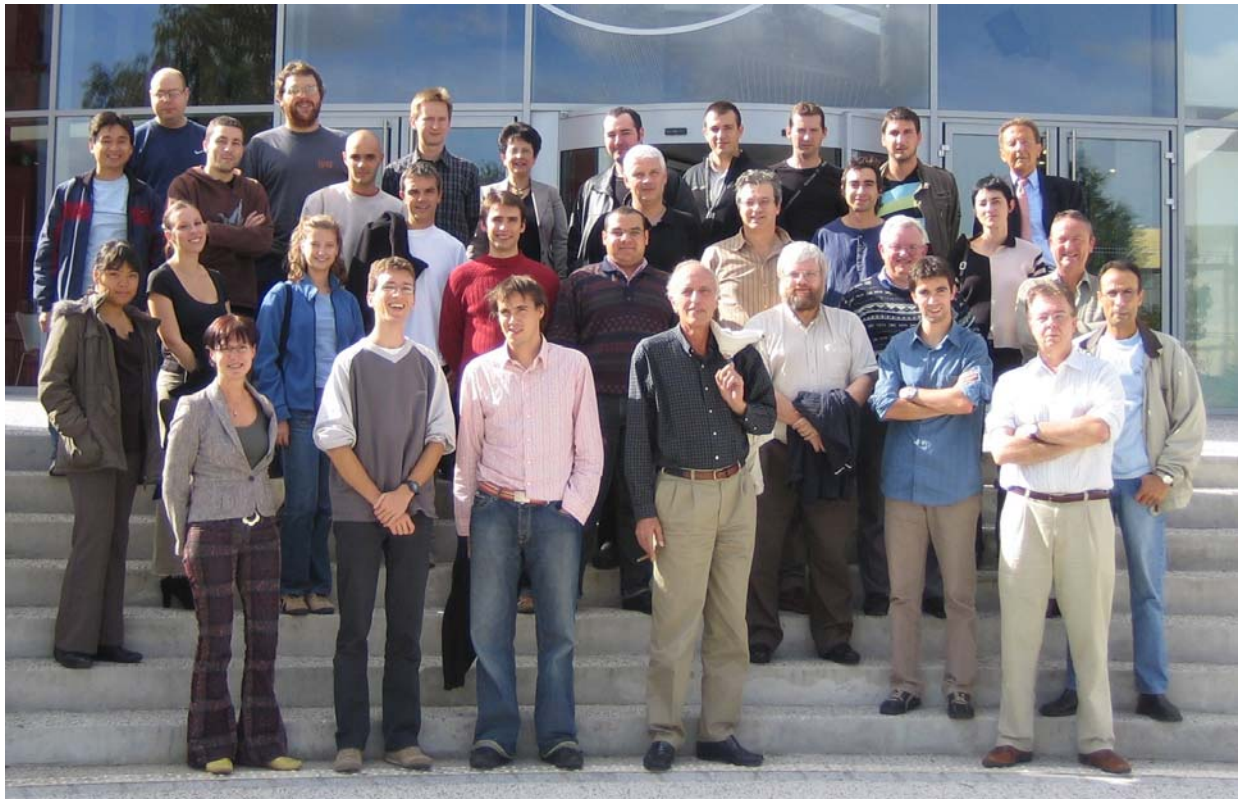
Jean-Claude Laprie

Vincent Nicomette

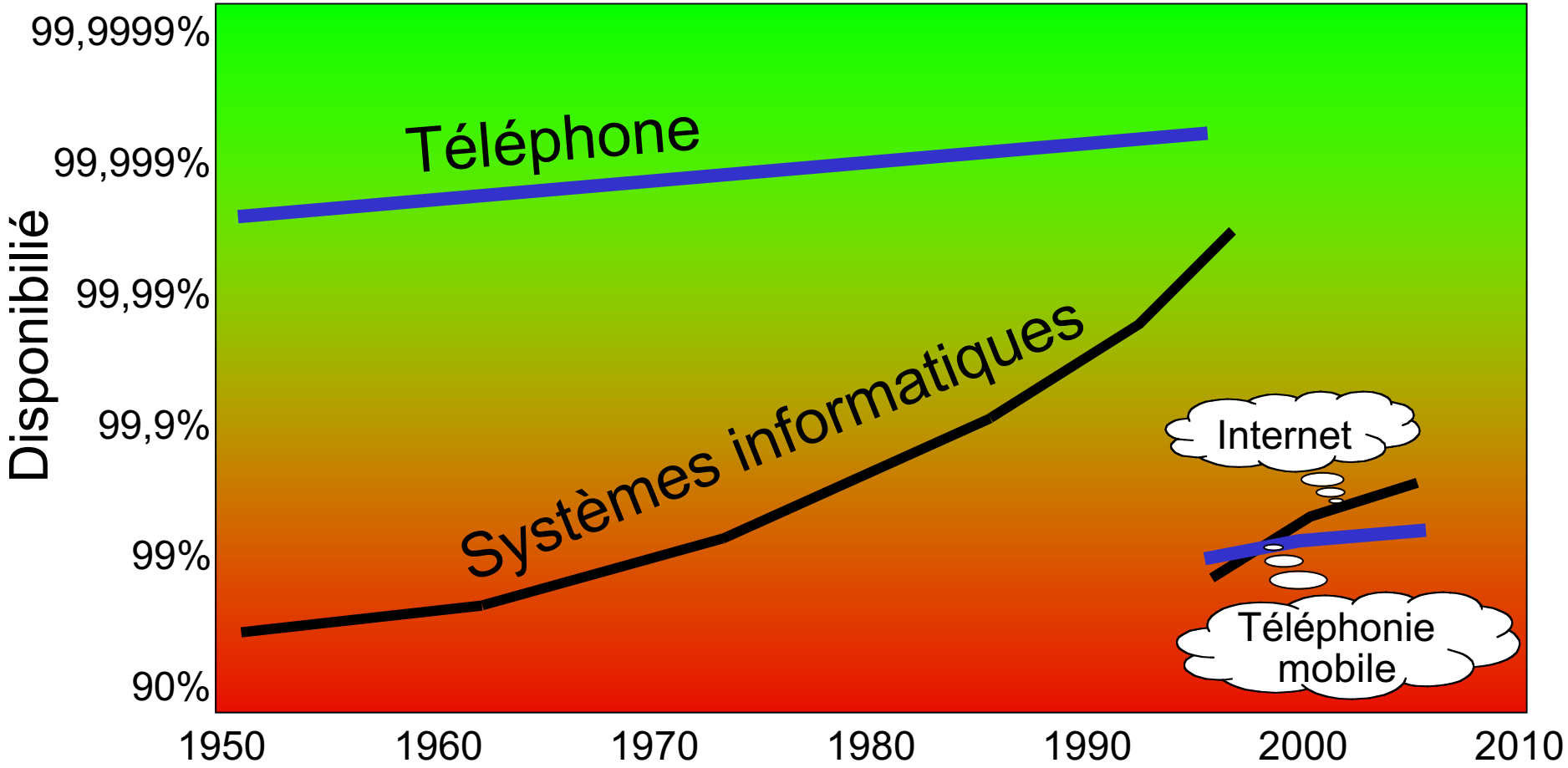
David Powell

Pascale Thévenod

Hélène Waeselynck



- La sûreté de fonctionnement : un concept intégrateur
- Quelques développements marquants
- Etat de l'art : statistiques
- Les systèmes ubiquitaires : le contexte émergent
- La résilience : un cadre pour affronter les défis ouverts
- Conclusion

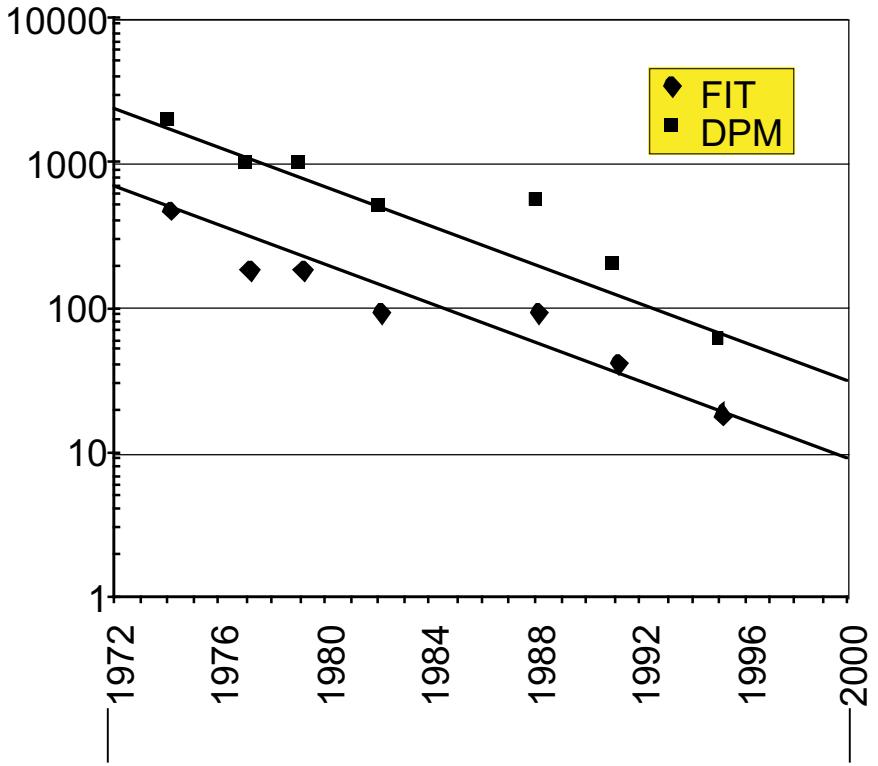


- Complexité
- Pression économique
- Malveillances

[D'après J. Gray, *Dependability in the Internet era,* Stanford, 2006]

Disponibilité		Durée indisponibilité/an
Six 9	0,999999	32s
Cinq 9	0,99999	5mn 15s
Quatre 9	0,9999	52mn 34s
Trois 9	0,999	8h 46mn
Deux 9	0,99	3j 16h
Un 9	0,9	36j 12h

Défaillances permanentes et défauts de production des microprocesseurs Intel



4004
2300 transistors

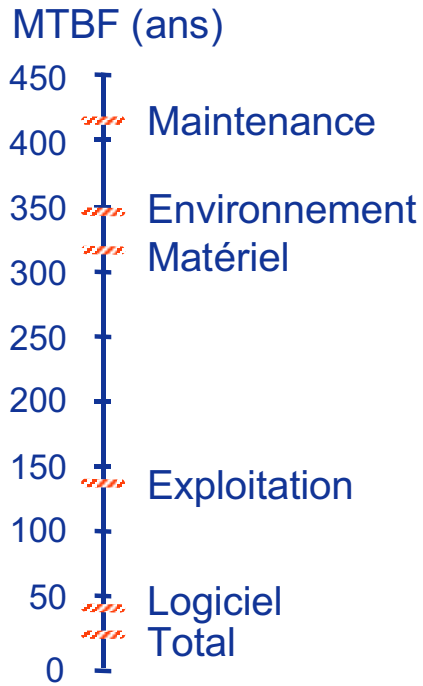
Pentium 3
15 10^6 transistors

1 FIT = 10^{-9}/h
DPM : défauts par million

[D'après *Intel's Quality System Databook*, Jan. 1998]

Tandem

	Nombre	Durée (ans)
Clients	2000	7000
Systèmes	9000	30000
Processeurs	25500	80000
Disques	74000	200000
Défaillances rapportées		438
MTBF système		21 ans

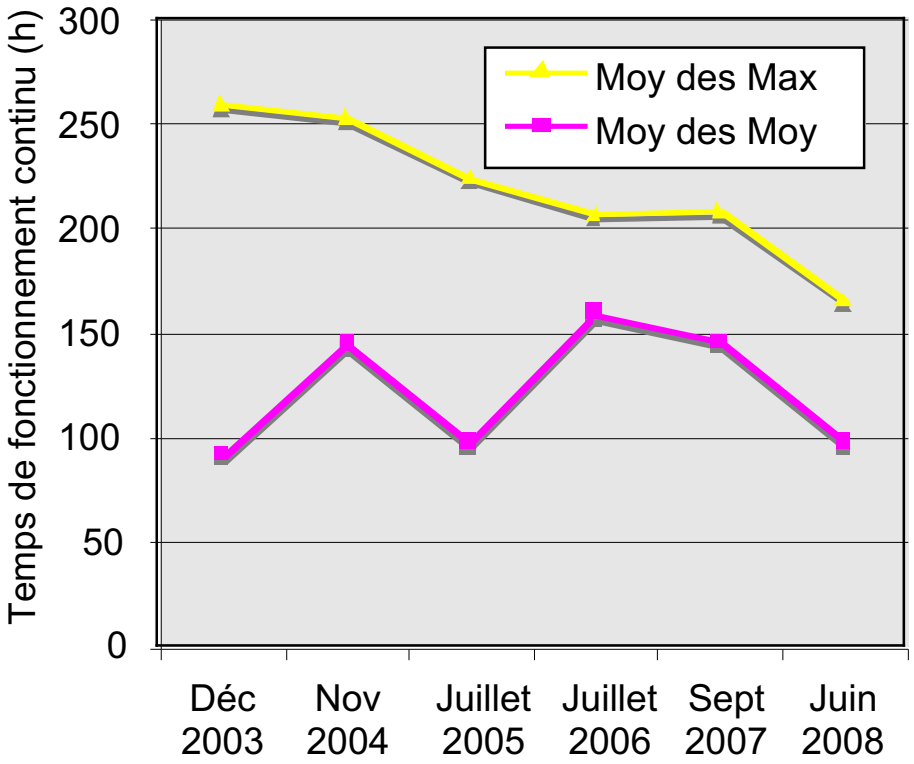


[D'après J. Gray, *A Census of Tandem System Availability Between 1985 and 1990*, IEEE Tr. On reliability, Oct.1990]

Statistiques temps de fonctionnement sites Web — NetCraft

[D'après: http://uptime.netcraft.com/up/today/top.avg.html]

50 sites les plus visités



	Temps moyen de restauration	Disponibilité
Disponibilité pour temps moyen jusqu'à défaillance de 100h	1 min	99.98
	10 mins	99.83
	1 heure	99.01
	8 heures	98.59

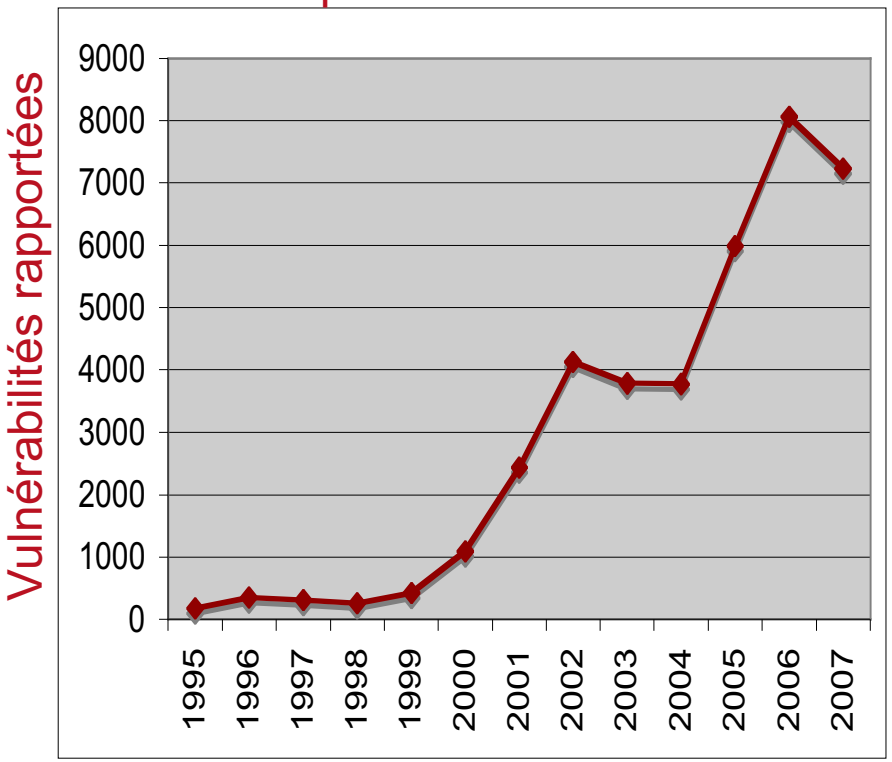
Trois grands sites web

Visites par jour	7 - 100 million
Nbre de machines et de sites	500 - 2000 machines, 2 - 15 sites
Architecture	x86
Période recueil données	3 - 7 mois
Défaill. composants	205 - 296
Défaill. service	21 - 56
MTTF	39 - 206 heures
MTTR	0,2 - 14 heures
Disponibilité moyenne	93.5 - 97,8 %

[D'après D. Oppenheimer, A. Ganapathi, D.A. Patterson, *Why do Internet services fail, and what can be done about it?*, USISTS '03]

Fautes accidentelles ↔ Malveillances

Statistiques SEI/CERT



[D'après : http://www.cert.org/stats/fullstats.html]

Ver Slammer/Sapphire

- Au moins 75000 machines infectés, 90% en 10 minutes, le 25 janvier 2003
- Exploitation vulnérabilité ('buffer overflow') du SQL Server de Microsoft, découverte en juillet 2002, patch publié avant annonce vulnérabilité

  [D'après : http://www.caida.org/publications/papers/2003/sapphire/sapphire.html]

	Causes	
	Accidentelles	Malveillantes
Global Information Security Survey 2004 — Ernst & Young	Perte de disponibilité	
	76%	24%
Enquête annuelle sur les dommages informatiques en France — CLUSIF (2000, 2001, 2002)	Occurrence de défaillances	
	71%	29%
	Perception des risques	
	29%	71%

[D'après :

- http://www.ey.com/global/Content.nsf/International/Assurance_&_Advisory_-_Technology_and_Security_Risk_-_Global_Information_Security_Survey_2004
- http://www.clusif.asso.fr/fr/production/sinistralite/index.asp]

- La sûreté de fonctionnement : un concept intégrateur
- Quelques développements marquants
- Etat de l'art : statistiques
- Les systèmes ubiquitaires : le contexte émergent
- La résilience : un cadre pour affronter les défis ouverts
- Conclusion

Systèmes ubiquitaires : immenses systèmes d'information, incorporant tout, depuis des super-ordinateurs et de gigantesques fermes de serveurs jusqu'à des myriades de petits ordinateurs mobiles et de minuscules objets 'embarqués'

☞ Evolutions déjà perceptibles

- Une tendance lourde : le génie logiciel dynamique
  - ➠ Assemblage de services existants découverts sur l'Internet
    - ✓ Architectures orientées service
    - ✓ Manuel → automatique : 'composantisation' extrême
- Une résurgence : la virtualisation
- Une certitude : la convergence du Web et des objets embarqués
- Des interrogations :
  - ✓ Migration des systèmes d'exploitation vers le Web
  - ✓ Communication
    - ➠ Echanges de messages → Essaims de contenus en vagues

Sûreté de fonctionnement ?

- ☞ Zones de confinement d'erreur ?
- ☞ Analyse, modélisation, prévision du comportement avant déploiement opérationnel hors de portée

changements incessants

comportements émergents issus de la multitude des interactions

Complémentées par

Approches classiques, essentiellement *réactives* — détection d'anomalies et recouvrement : détection d'erreur et récupération système par traitement d'erreurs et de fautes

Approches *proactives*, permettant de détecter causes possibles de défaillance lorsqu'elles sont encore potentielles, avant qu'elles ne provoquent des anomalies dans comportement système et délivrance service

Approches proactives déjà explorées

- Rajeunissement du logiciel
- Architectures et algorithmes pour tolérance aux fautes, par ex.
  - ✓ Fautes accidentelles : migration de tâches avant occurrence de défaillances dues à des fautes accidentelles
  - ✓ Fautes accidentelles et malveillantes : réduction de la fenêtre temporelle de vulnérabilité, via algorithmes accord byzantin

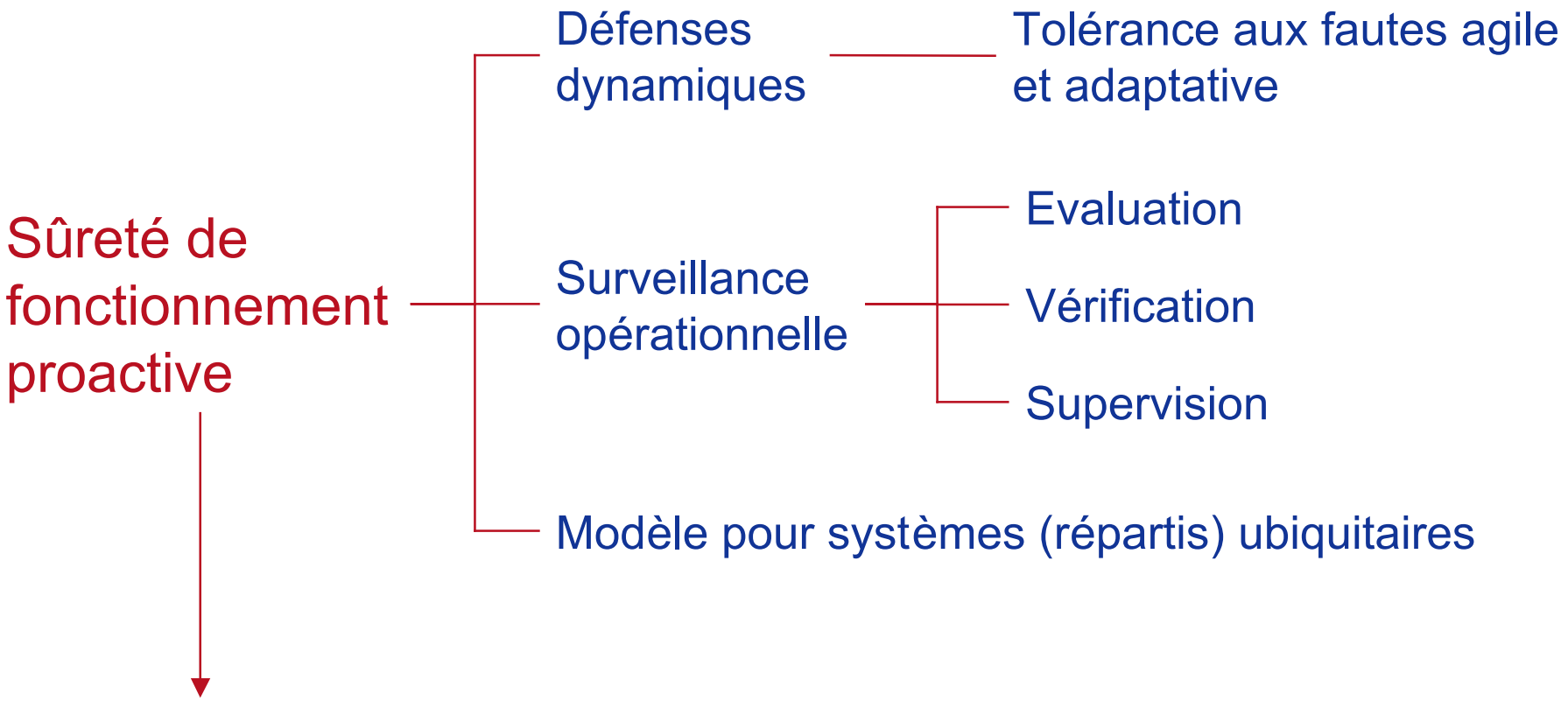
Proactivité indissociable d'une surveillance opérationnelle

↓

Surveillance opérationnelle déjà explorée

- Evaluation
  - ✓ Disponibilité statistique ➜ 'Service level agreement' (SLA)
  - ✓ Anticipation des défaillances
    - analyse de déviations significatives de mesures apparentées performance, ou de profils d'utilisation de comportements 'normaux'
    - identification de motifs d'erreur caractéristiques
- Vérification en ligne d'assertions

Inadéquation aux changements incessants des systèmes ubiquitaires



Classes majeures de fautes

- ➢ Fautes logicielles furtives
- ➢ Fautes de configuration
- ➢ Vulnérabilités
- ✢ Incompatibilités dans évolutions
- ✢ Comportements émergents indésirables

- La sûreté de fonctionnement : un concept intégrateur
- Quelques développements marquants
- Etat de l'art : statistiques
- Les systèmes ubiquitaires : le contexte émergent
- La résilience : un cadre pour affronter les défis ouverts
- Conclusion

Résilience

➠ En sûreté de fonctionnement des systèmes informatiques

- Adjectif résilient
  - En usage depuis plus de trois décennies
  - Récemment, utilisation croissante
  - Utilisé essentiellement comme synonyme de tolérant aux fautes

- Tolérance aux fautes et aux changements

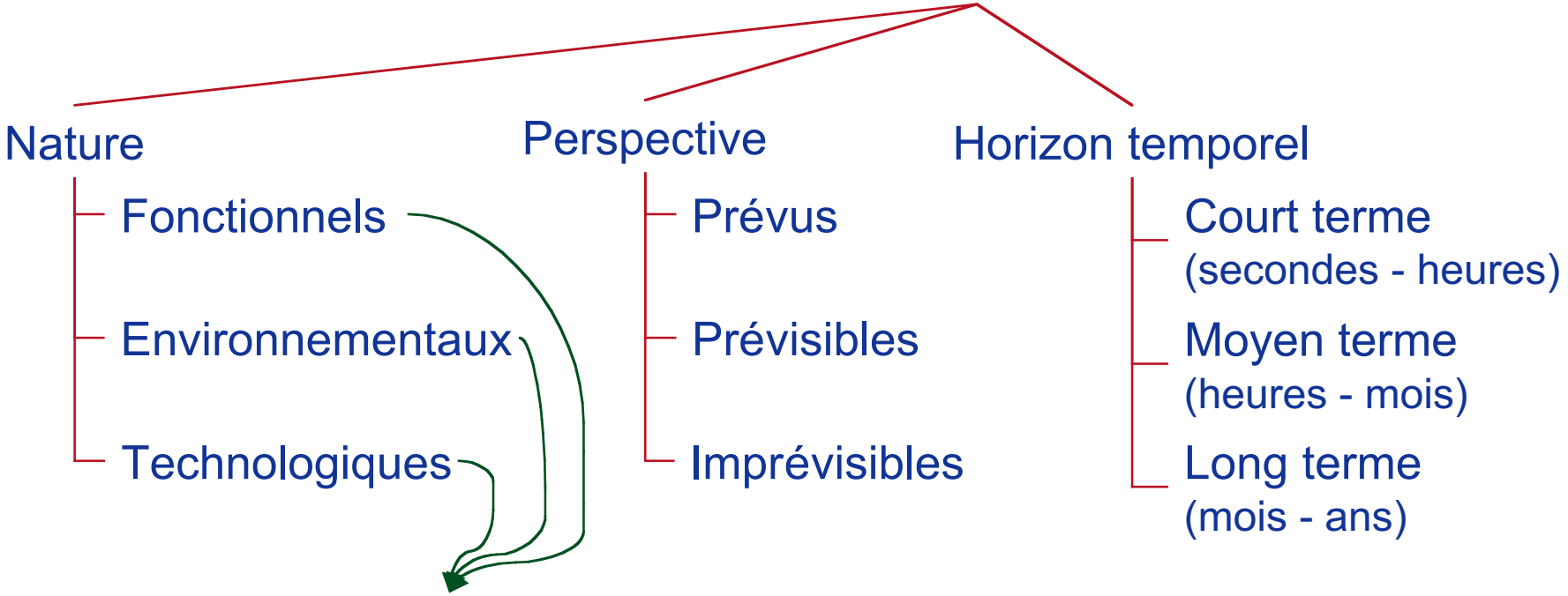
➠ Dans d'autres domaines

Adaptation aux changements, et capacité à rebondir après un revers ou un échec

- Résistance des matériaux
- Psychologie sociale
- Pédo-psychiatrie
- Ecologie
- Economie
- Sécurité industrielle

En jeu : maintien de la sûreté de fonctionnement malgré les changements

Résilience d'un système : persistance de la sûreté de fonctionnement en face de changements



Evolution des entraves

- Attaques
- Incompatibilités dans évolutions
- Comportements émergents indésirables
- Proportion croissante de fautes temporaires du matériel

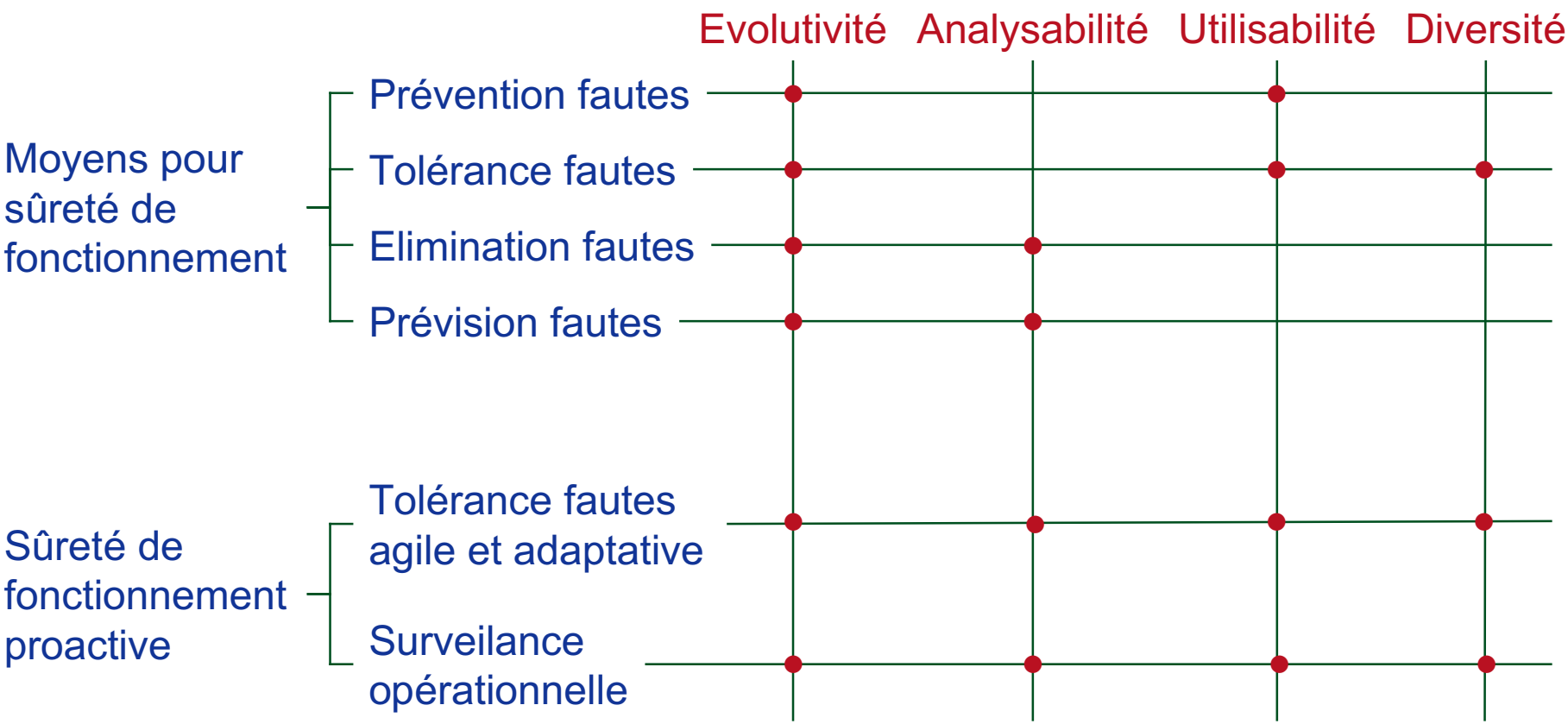
Technologies de la résilience

Changements → Evolutivité
- ☞ Adaptativité

Service de confiance justifiée → Analysabilité
- ☞ Vérification et évaluation

Systèmes ubiquitaires → Utilisabilité
- ☞ Utilisateurs humains et techniques

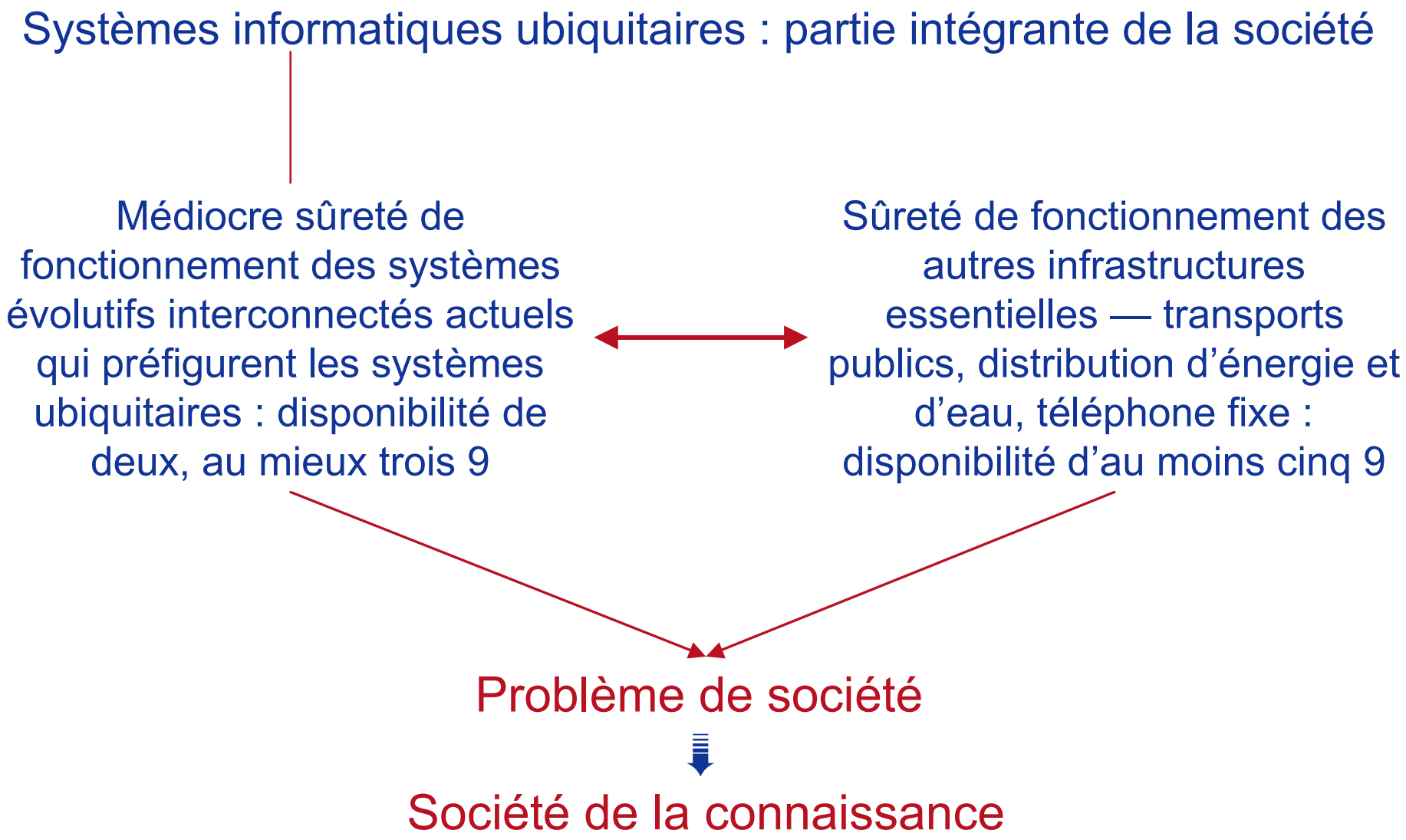
Systèmes complexes → Diversité
- ☞ Tirer partie de la diversité existante et l'accroître


Evolutivité
Analysabilité
Utilisabilité
Diversité
Moyens pour sûreté de fonctionnement
Prévention fautes
Tolérance fautes
Elimination fautes
Prévision fautes
Sûreté de fonctionnement proactive
Tolérance fautes agile et adaptative
Surveilance opérationnelle

- La sûreté de fonctionnement : un concept intégrateur
- Quelques développements marquants
- Etat de l'art : statistiques
- Les systèmes ubiquitaires : le contexte émergent
- La résilience : un cadre pour affronter les défis ouverts
- Conclusion

Attentes de la communauté informatique

- Numéro 50ème anniversaire de Communications of the ACM (janvier 2008) : la plupart des articles mentionnent la sûreté de fonctionnement ou la résilience comme un facteur majeur (Jeannette Wing, Rodney Brooks, Gul Agha, John Crowcroft, Gordon Bell)
  - ☞ Rodney Brooks : « New formalisms will let us analyze complex distributed systems, producing new theoretical insights that lead to practical real-world payoffs. Exactly what the basis for these formalisms will be is, of course impossible to guess. My own bet is on resilience and adaptability »
- Cahier de fond d'IEEE Computer de mars 2008, consacré au génie logiciel au 21ème siècle
  - ☞ Barry Boehm : « In the 21st century, software engineers face the often formidable challenges of simultaneously dealing with rapid change, uncertainty and emergence, dependability, diversity, and interdependence »


Systèmes informatiques ubiquitaires : partie intégrante de la société
Médiocre sûreté de fonctionnement des systèmes évolutifs interconnectés actuels qui préfigurent les systèmes ubiquitaires : disponibilité de deux, au mieux trois 9
Sûreté de fonctionnement des autres infrastructures essentielles — transports publics, distribution d'énergie et d'eau, téléphone fixe : disponibilité d'au moins cinq 9
Problème de société
Société de la connaissance