Sûreté de fonctionnement informatique : un nécessaire changement d'échelle

Jean-Claude Laprie

Toulouse, 28-30 septembre 2005

- Sûreté de fonctionnement
- Etat de l'art en (quelques) statistiques
- Changement d'échelle de la sûreté de fonctionnement
- Le réseau d'excellence ReSIST
- Conclusion

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

Service délivré par un système : son comportement tel que perçu par son, ou ses utilisateurs

Utilisateur : autre système en interaction avec le système considéré

Fonction d'un système : ce à quoi le système est destiné, décrite par la spécification fonctionnelle

Service correct : le service délivré accomplit la fonction du système

Défaillance (du service) : événement qui survient lorsque le service délivré dévie du service correct, soit parce qu'il n'est plus conforme à la spécification, soit parce que la spécification ne décrit pas de manière adéquate la fonction du système

Erreur : partie de l'état susceptible d'entraîner une défaillance

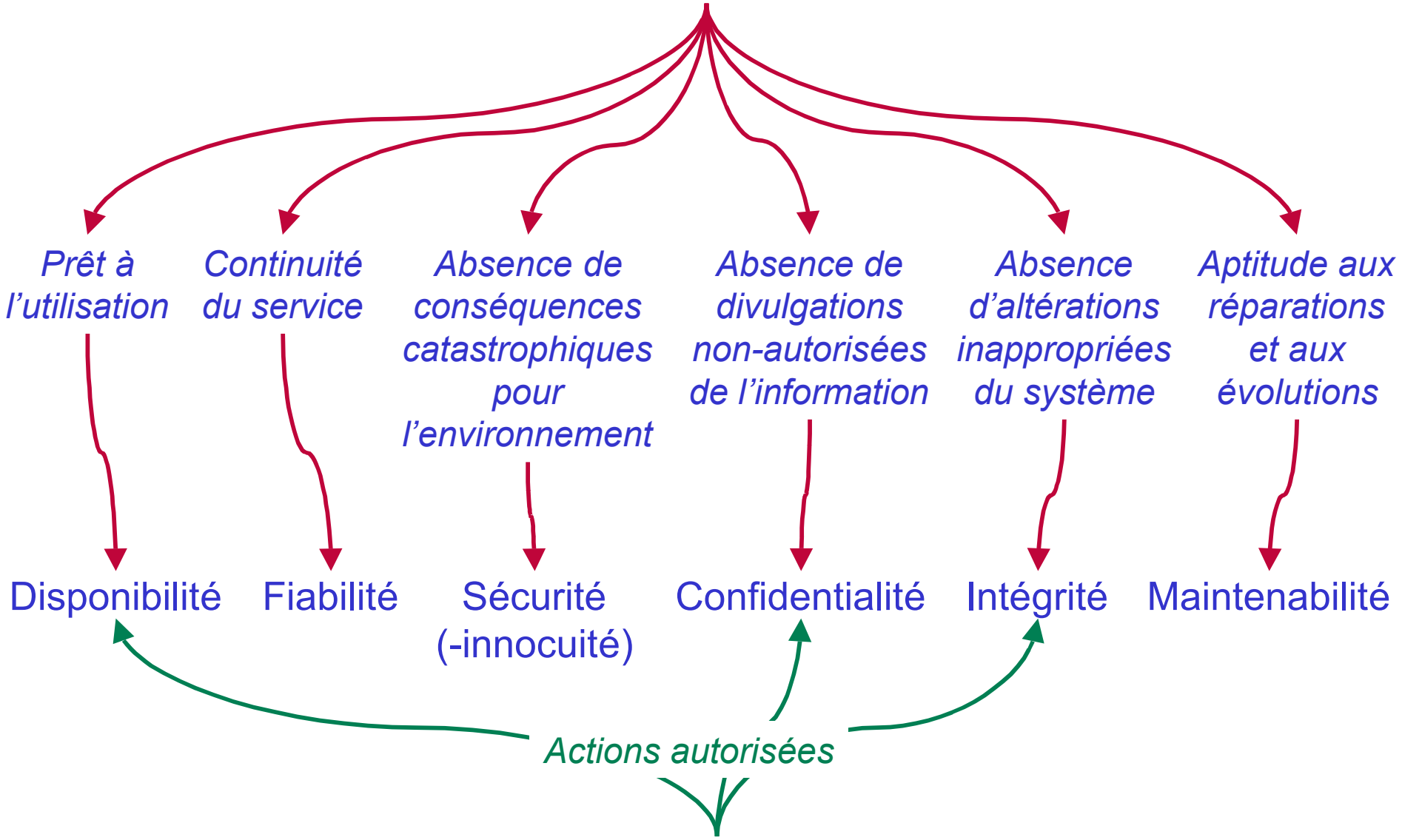
Faute : cause adjugée ou supposée d'une erreur

Modes de défaillance : manières selon lesquelles un système peut défaillir, classées selon leur gravité

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

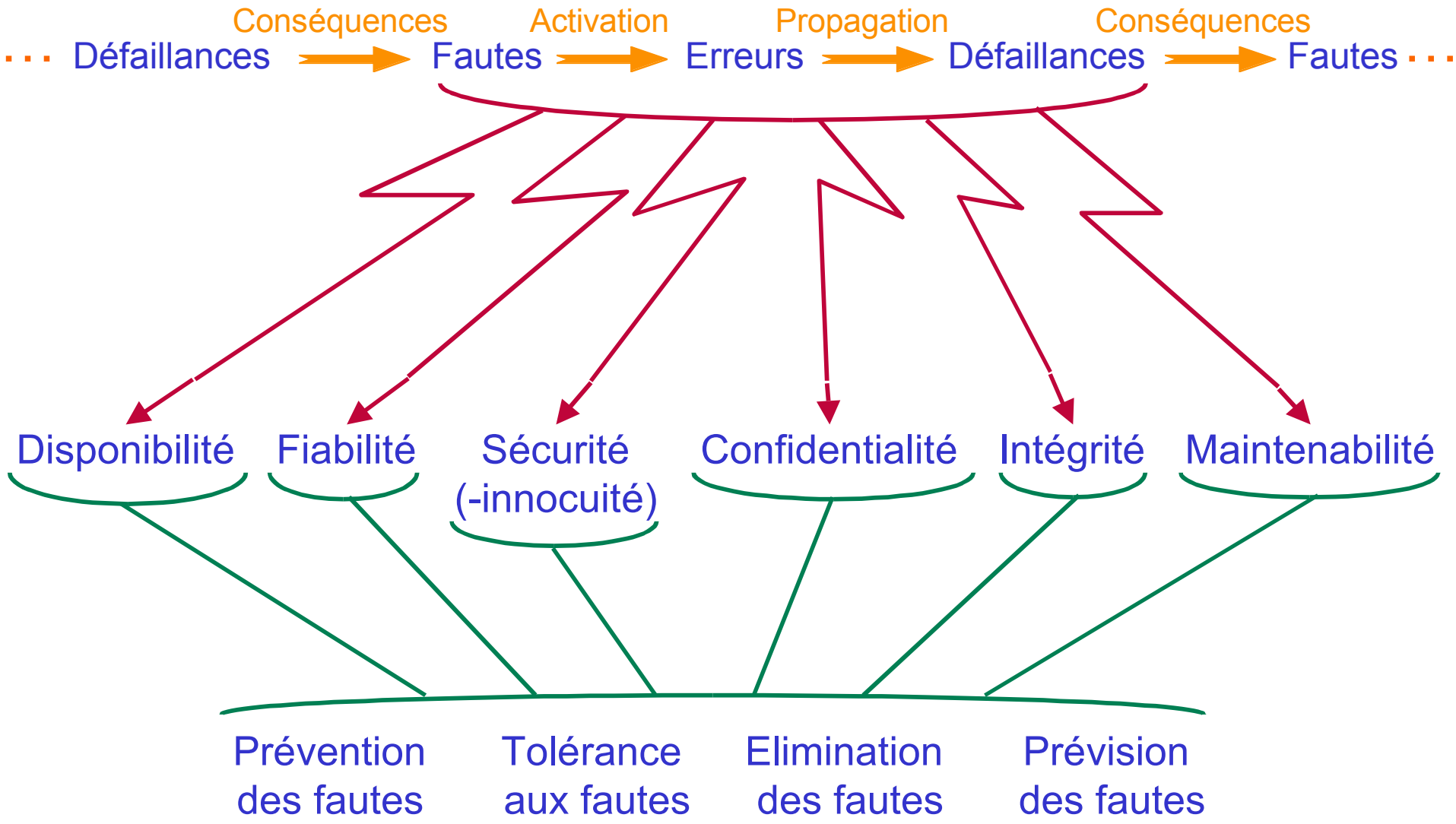
Défaillances du service plus fréquentes ou plus graves qu'acceptable: défaillances de la sûreté de fonctionnement

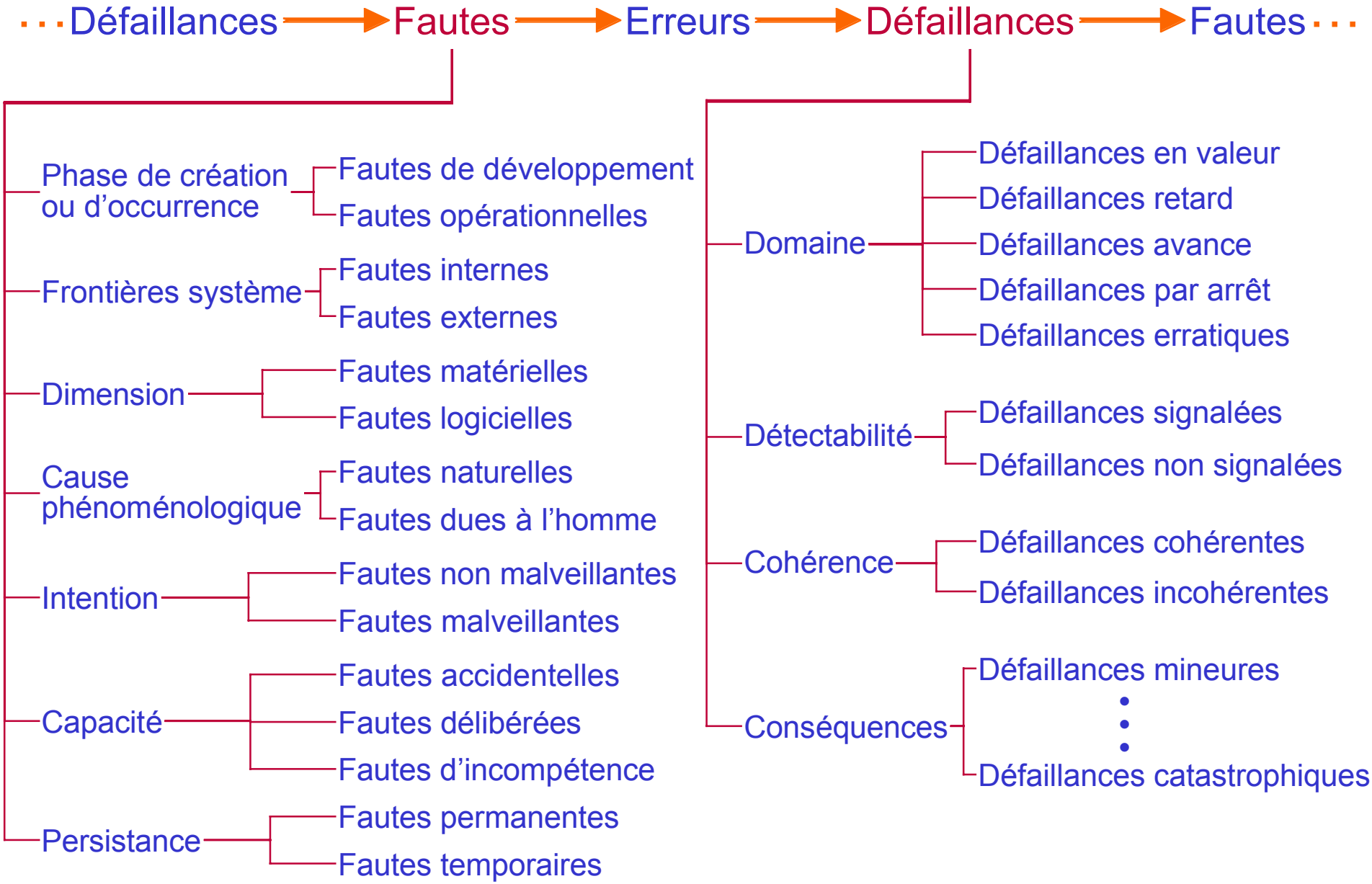
Sûreté de Fonctionnement

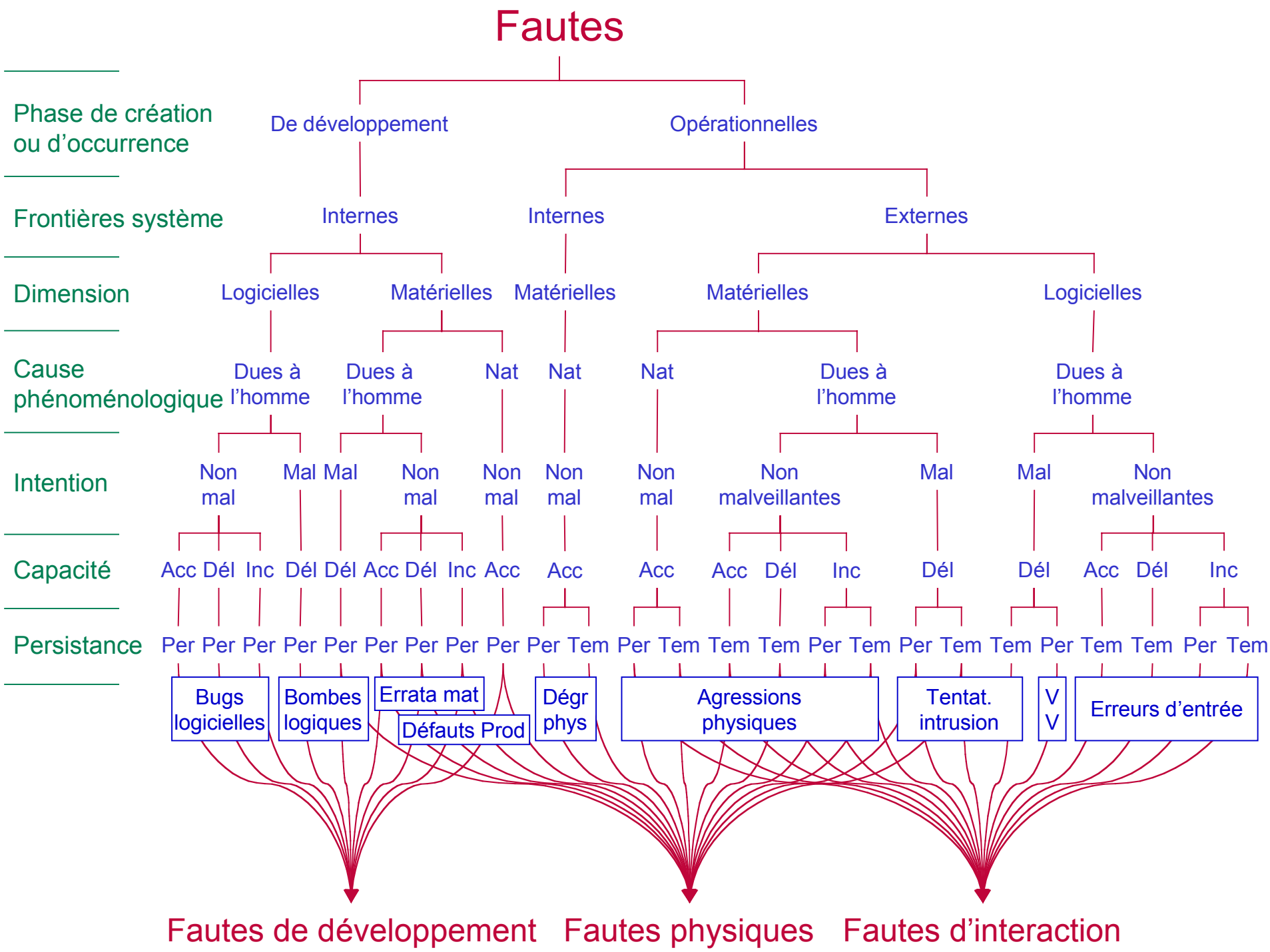


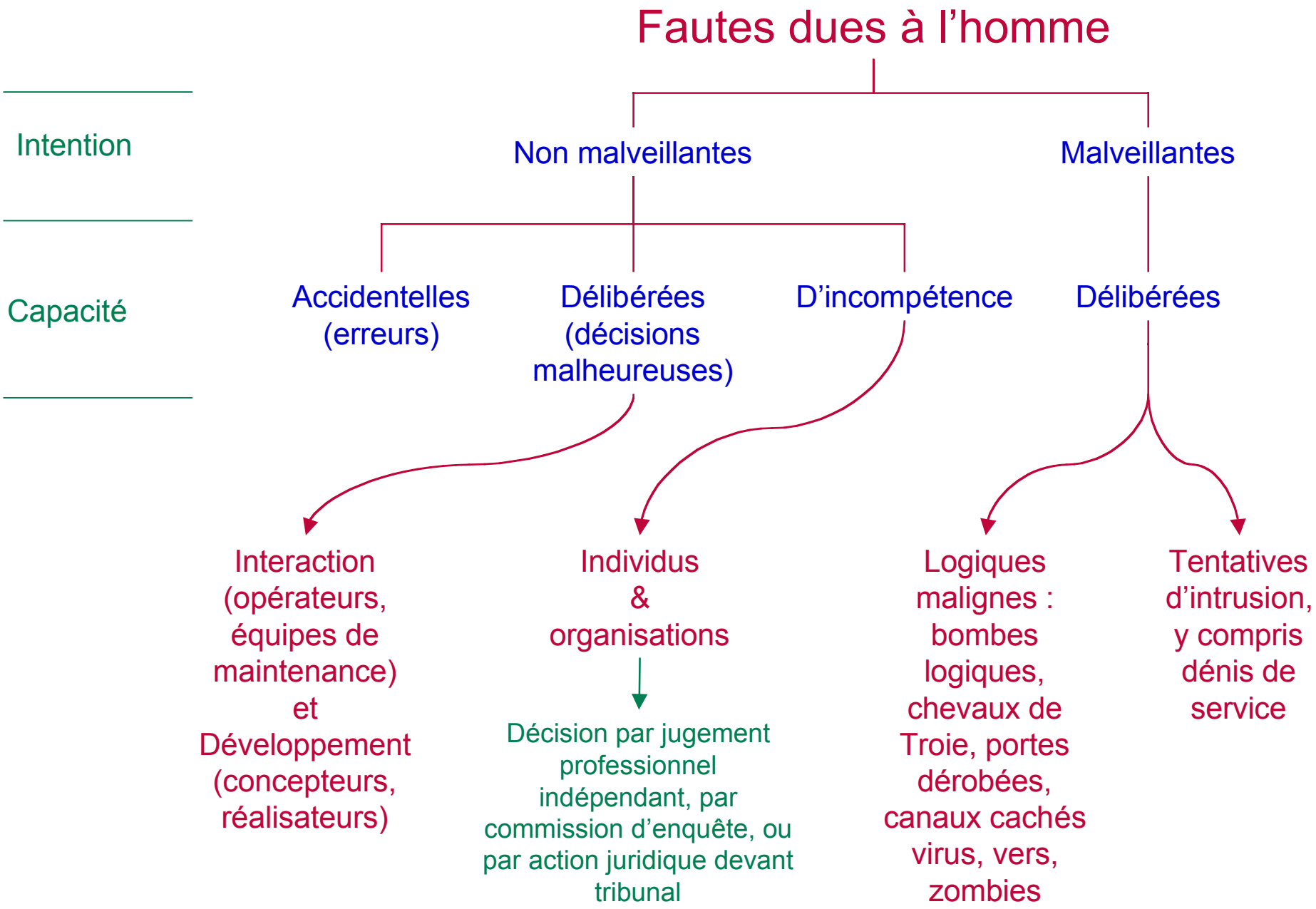
Sécurité (-immunité)

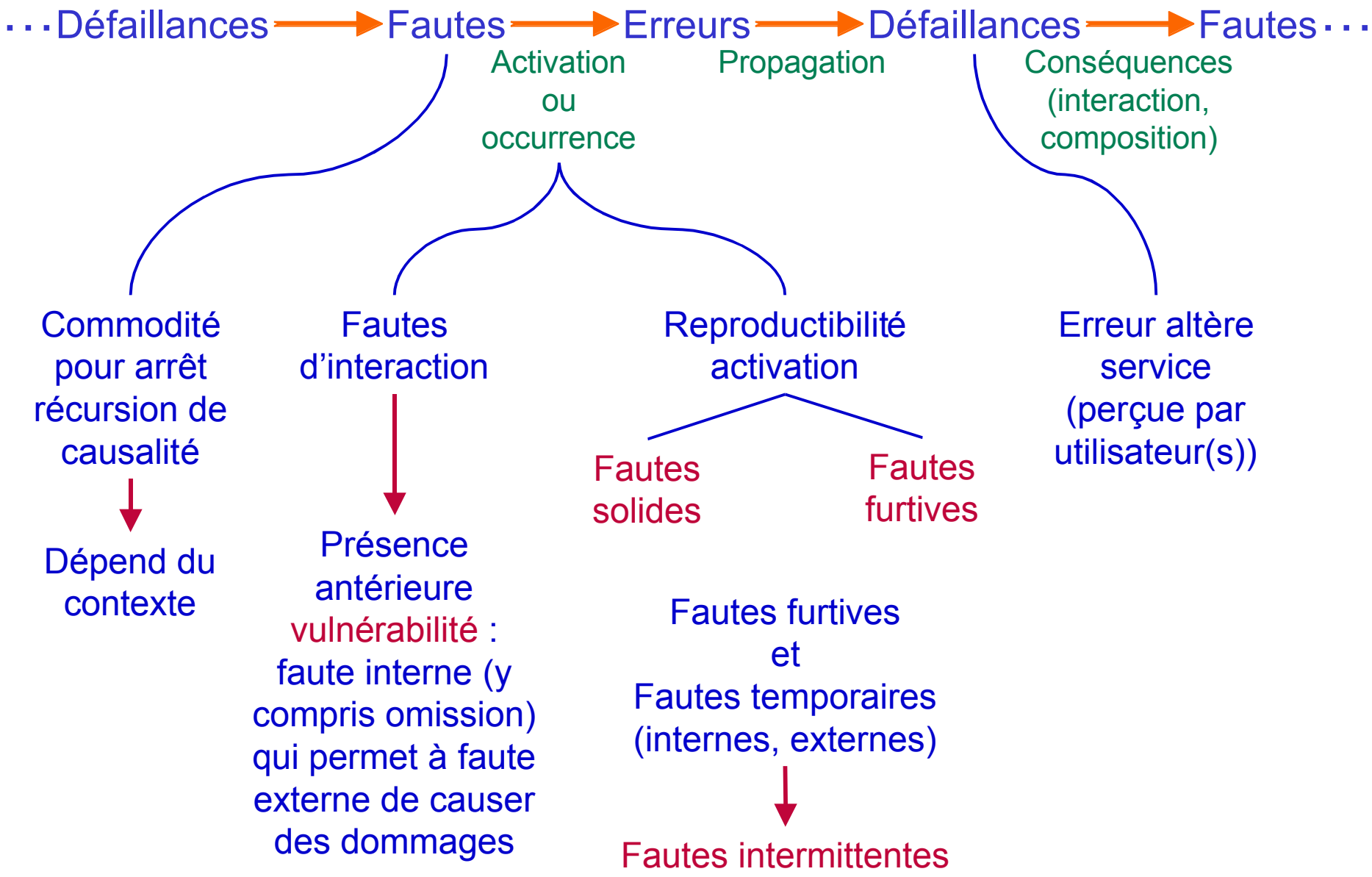
Absence d'accès ou de manipulations non-autorisés de l'état du système

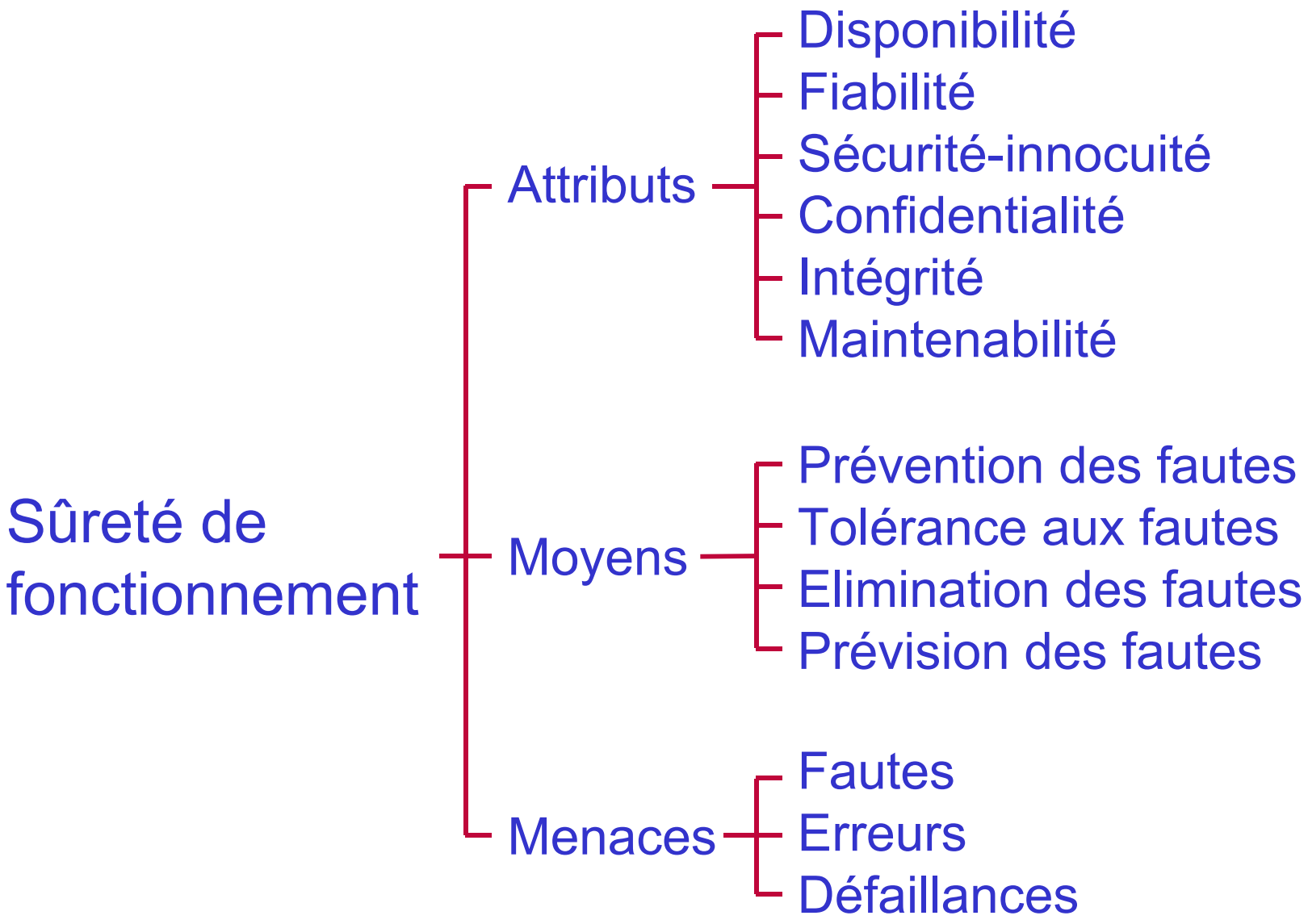

Conséquences
Activation
Propagation
Conséquences
Défaillances
Fautes
Erreurs
Défaillances
Fautes
Disponibilité
Fiabilité
Sécurité
(-innocuité)
Confidentialité
Intégrité
Maintenabilité
Prévention
des fautes
Tolérance
aux fautes
Elimination
des fautes
Prévision
des fautes

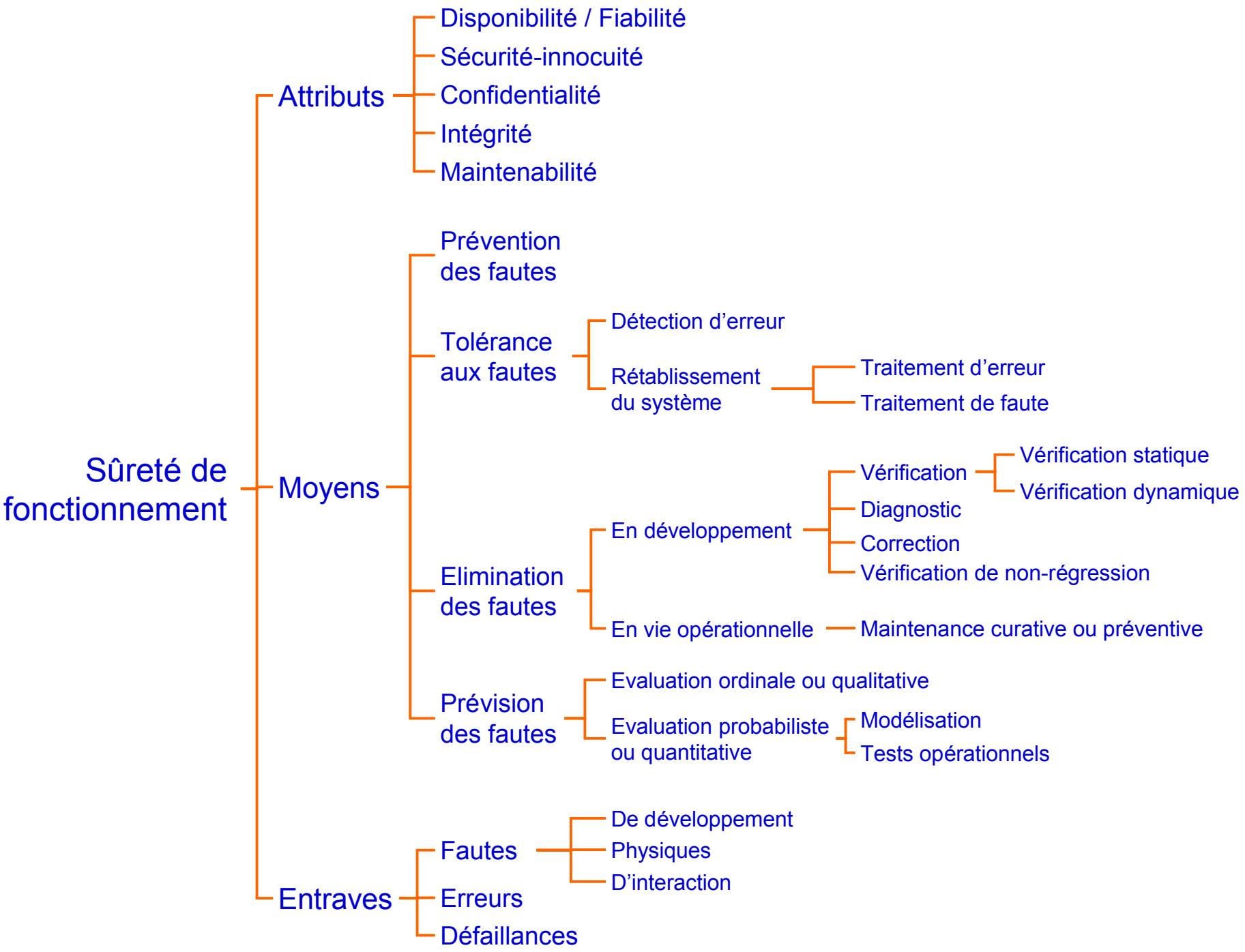

Défaillances
Fautes
Erreurs
Défaillances
Fautes
Phase de création ou d'occurrence
Fautes de développement
Fautes opérationnelles
Frontières système
Fautes internes
Fautes externes
Dimension
Fautes matérielles
Fautes logicielles
Cause phénoménologique
Fautes naturelles
Fautes dues à l'homme
Intention
Fautes non malveillantes
Fautes malveillantes
Capacité
Fautes accidentelles
Fautes délibérées
Fautes d'incompétence
Persistance
Fautes permanentes
Fautes temporaires
Domaine
Défaillances en valeur
Défaillances retard
Défaillances avance
Défaillances par arrêt
Défaillances erratiques
Détectabilité
Défaillances signalées
Défaillances non signalées
Cohérence
Défaillances cohérentes
Défaillances incohérentes
Conséquences
Défaillances mineures
Défaillances catastrophiques


Fautes
Phase de création ou d'occurrence
Frontières système
Dimension
Cause phénoménologique
Intention
Capacité
Persistance
De développement
Opérationnelles
Internes
Internes
Externes
Logicielles
Matérielles
Matérielles
Matérielles
Logicielles
Dues à l'homme
Dues à l'homme
Nat
Nat
Nat
Dues à l'homme
Dues à l'homme
Non mal
Mal
Mal
Non mal
Non mal
Non mal
Non mal
Non malveillantes
Mal
Mal
Non malveillantes
Acc Dél Inc Dél Dél Acc Dél Inc Acc Acc Acc Acc Dél Inc Dél Dél Acc Dél Inc
Per Per Per Per Per Per Per Per Per Per Tem Per Tem Tem Tem Per Tem Per Tem Tem Per Tem Tem Per Tem
Bugs logicielles
Bombes logiques
Errata mat
Défauts Prod
Dégr phys
Agressions physiques
Tentat. intrusion
V V
Erreurs d'entrée
Fautes de développement
Fautes physiques
Fautes d'interaction


Fautes dues à l'homme
Intention
Non malveillantes
Malveillantes
Capacité
Accidentelles (erreurs)
Délibérées (décisions malheureuses)
D'incompétence
Délibérées
Interaction (opérateurs, équipes de maintenance) et Développement (concepteurs, réalisateurs)
Individus & organisations
Décision par jugement professionnel indépendant, par commission d'enquête, ou par action juridique devant tribunal
Logiques malignes : bombes logiques, chevaux de Troie, portes dérobées, canaux cachés virus, vers, zombies
Tentatives d'intrusion, y compris dénis de service


· · · Défaillances
Fautes
Erreurs
Défaillances
Fautes · · ·
Activation ou occurrence
Propagation
Conséquences (interaction, composition)
Commodité pour arrêt récursion de causalité
Dépend du contexte
Fautes d'interaction
Présence antérieure vulnérabilité : faute interne (y compris omission) qui permet à faute externe de causer des dommages
Reproductibilité activation
Fautes solides
Fautes furtives
Fautes furtives et Fautes temporaires (internes, externes)
Fautes intermittentes
Erreur altère service (perçue par utilisateur(s))

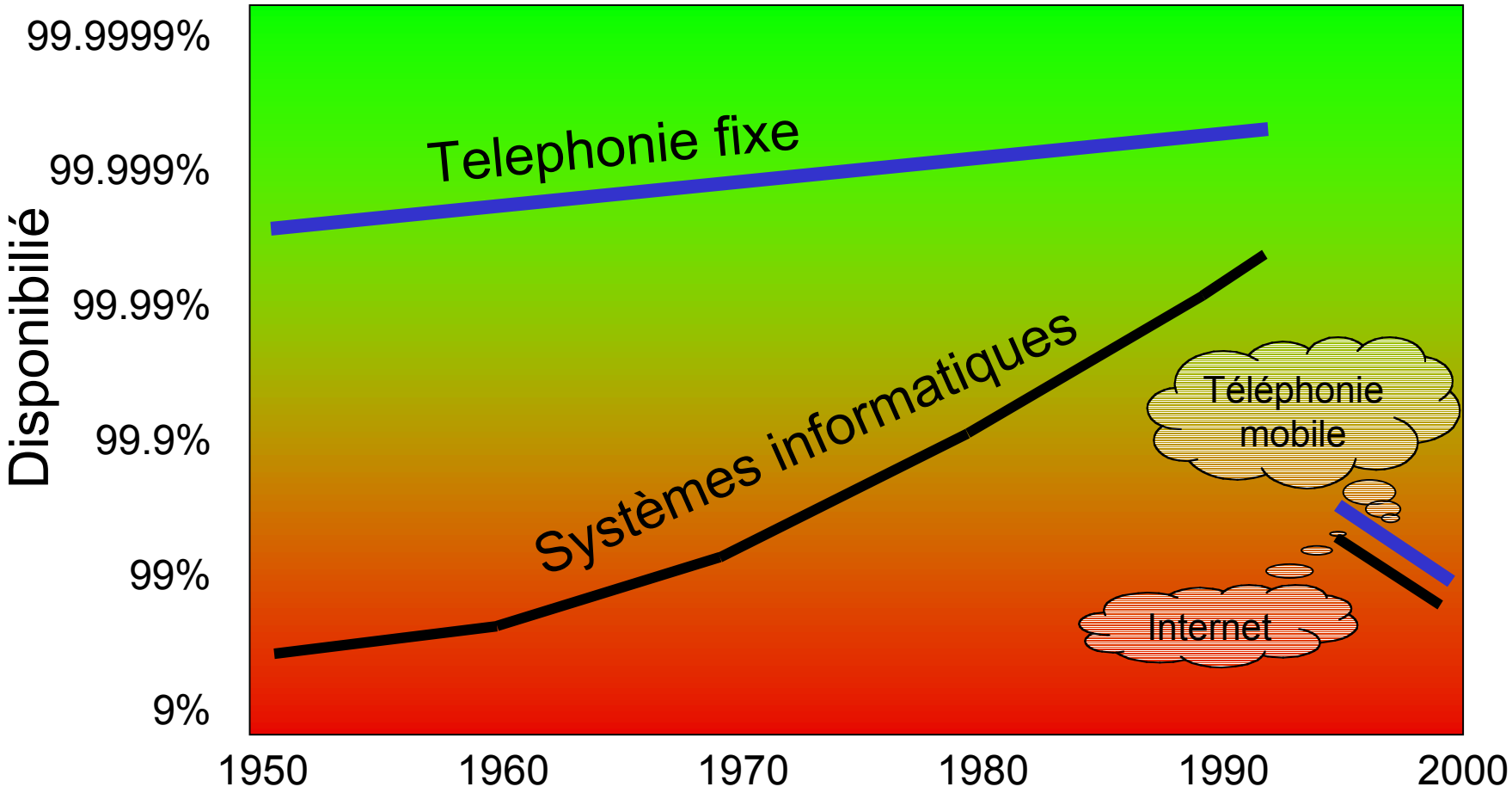

Sûreté de fonctionnement
Attributs
Disponibilité
Fiabilité
Sécurité-innocuité
Confidentialité
Intégrité
Maintenabilité
Moyens
Prévention des fautes
Tolérance aux fautes
Elimination des fautes
Prévision des fautes
Menaces
Fautes
Erreurs
Défaillances


Sûreté de fonctionnement
Attributs
Disponibilité / Fiabilité
Sécurité-innocuité
Confidentialité
Intégrité
Maintenabilité
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

	Fautes			Défail.				
	Physiques	Développement	Interaction	Localisées	Distribuées	Disponibilité/Fiabilité	Sécurité-innocuité	Confidentialité
Juin 1980 : Fausses alertes à des attaques massives de fusées soviétiques au NORAD	✔			✔		✔		
Juin 1985 - Janvier 1987 : Doses excessives de radiothérapie (Therac-25)		✔		✔			✔	
Août 1986 - 1987 : Le "Wily hacker" pénètre des dizaines de centres informatiques sensibles		✔	✔	✔				✔
15 Janvier 1990 : Indisponibilité totale du téléphone interurbain aux Etats-Unis, pendant 9h		✔			✔	✔		
Février 1991 : Scud raté par un Patriot à Dhahran		✔	✔	✔		✔	✔	
Novembre 1992 : Ecroulement des communications du service d'ambulances de Londres		✔	✔		✔	✔	✔	
26 et 27 Juin 1993 : Refus des cartes de crédit dans les distributeurs de monnaie en France	✔	✔			✔	✔		
4 Juin 1996 : Défaillance du vol 501 d'Ariane 5		✔		✔		✔		
17 Juillet 1997: Mélange des adresses du domaine internet .com			✔		✔	✔		
13 Avril 1998 : Ecroulement réseau de données d'AT&T		✔	✔		✔	✔		
Février 2000 : Engorgement de grands portails Web		✔	✔		✔	✔		
Mai 2000 : Virus "I love you"		✔	✔		✔	✔		
Juillet 2001 : Ver "Code Red"		✔	✔		✔	✔		
Août 2003 : Propagation de panne électrique dans le Nord-Est des USA et le Canada		✔	✔		✔	✔		

Nombre de défaillances en fonction classes fautes [conséquences et durée de panne largement dépendantes de l'application]	Systèmes cœur (par ex., traitements transactionnels, commutation électronique, serveurs Internet dorsaux)		Systèmes contrôlés (par ex., avions commerciaux, réseau téléphonique, serveurs Internet frontaux)	
Fautes	Rang	Proportion	Rang	Proportion
Physiques internes	3	~ 10%	2	15-20%
Physiques externes	3	~ 10%	2	15-20%
D'interactions humaines *	2	~ 30%	1	40-50%
Développement	1	~ 50%	2	15-20%

* Recherche des causes premières montre qu'elles peuvent être souvent attribuées à des fautes de développement, elles-même consécutives à une sous-estimation des interactions homme-système dans le processus de développement

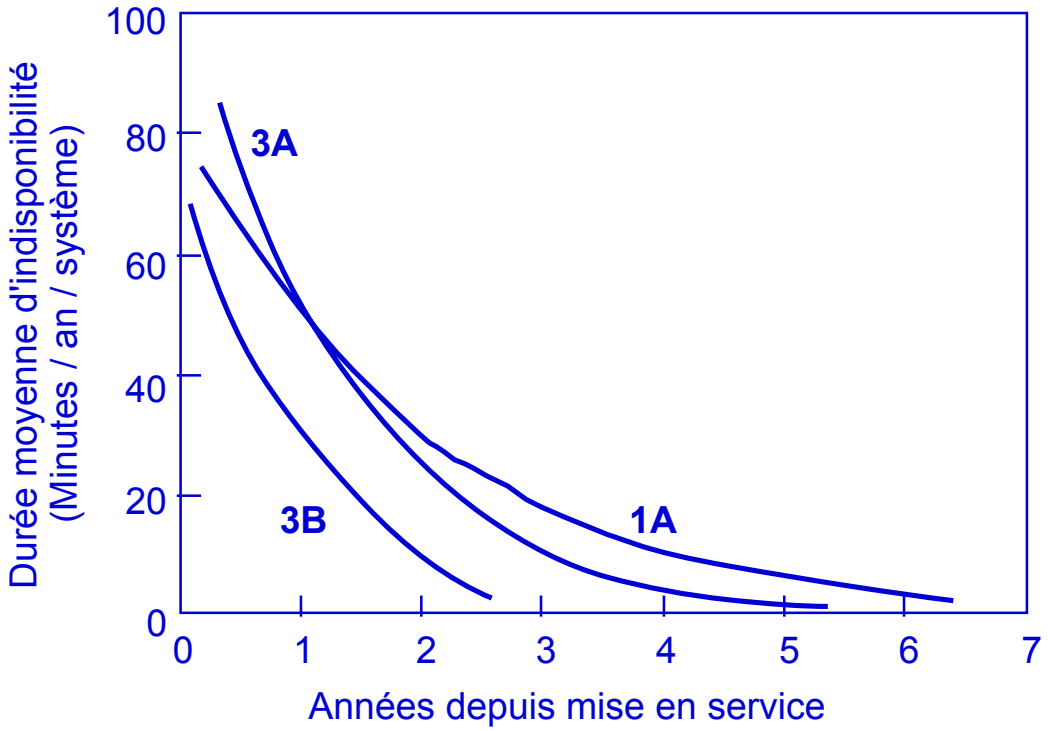


D'après J. Gray, *Dependability in the Internet era*

- Complexité
- Pression économique

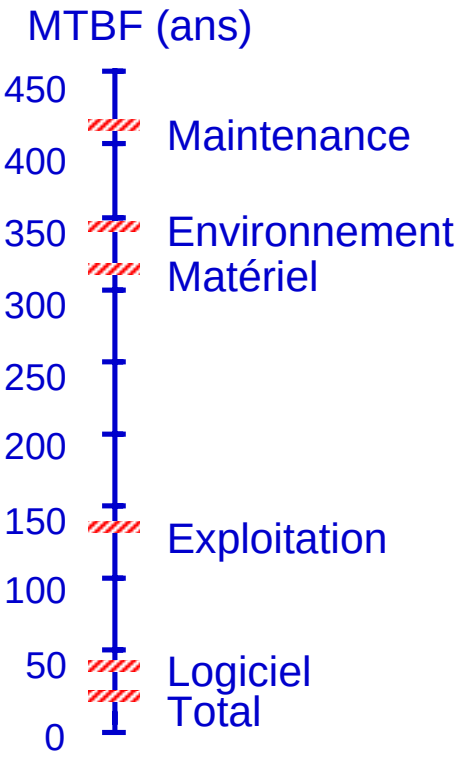
Disponibilité	Durée indisponibilité/an
0,999999	32s
0,99999	5mn 15s
0,9999	52mn 34s
0,999	8h 46mn
0,99	3j 16h
0,9	36j 12h

Autocommutateurs AT&T

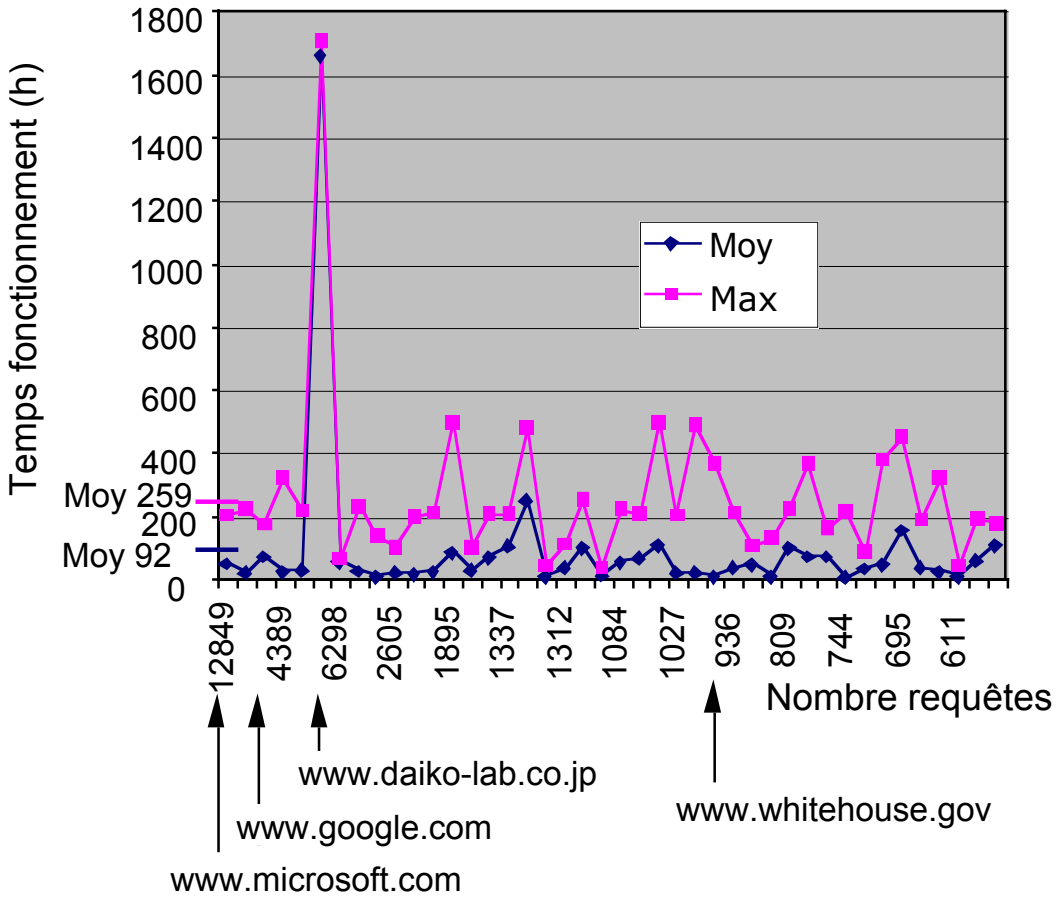


Tandem Computers

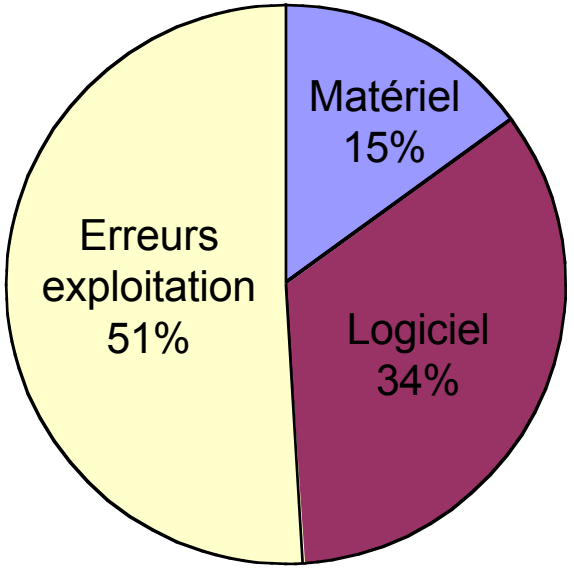
	Nombre	Durée (ans)
Clients	2000	7000
Systèmes	9000	30000
Processeurs	25500	80000
Disques	74000	200000
Indisponibilités rapportées		438
MTBF Système		21 ans



NetCraft
Statistiques temps fonctionnement sites Web



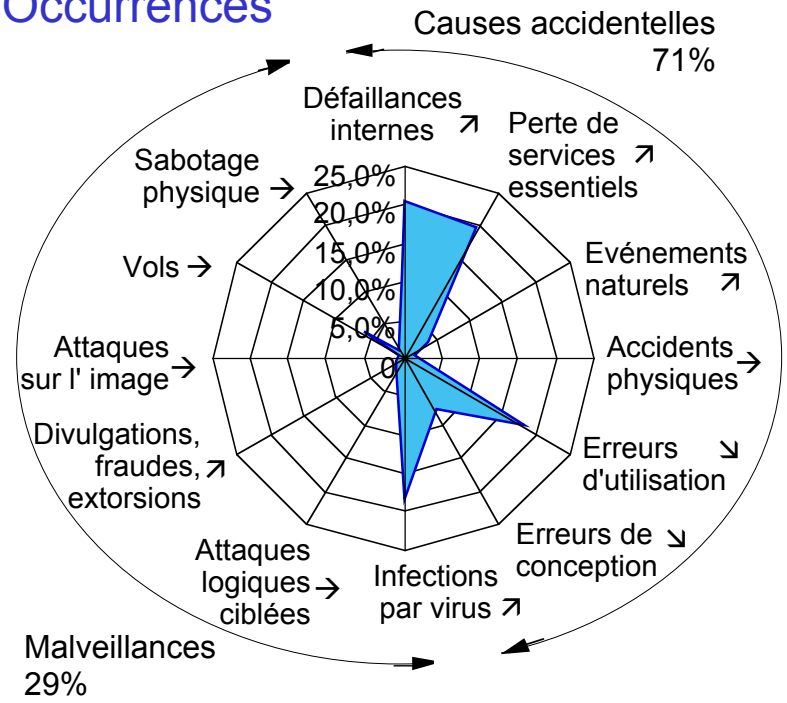
Sources de défaillance sites Web
(3 sites, 6 mois, 500-5000 serveurs/sites)



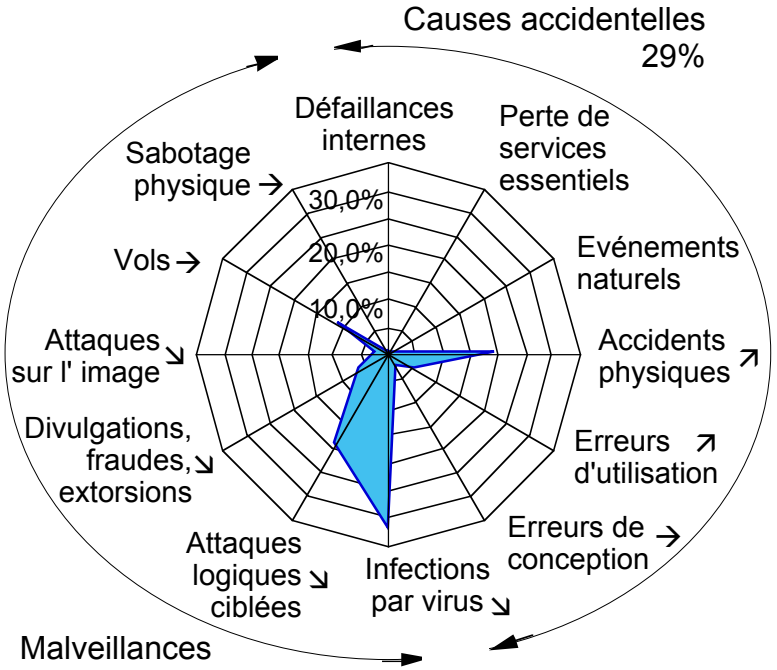
D'après D. Patterson, A. Brown, A. Fox, 'Recovery-oriented computing'

Enquête annuelle sur les dommages informatiques en France — CLUSIF (2000, 2001, 2002)

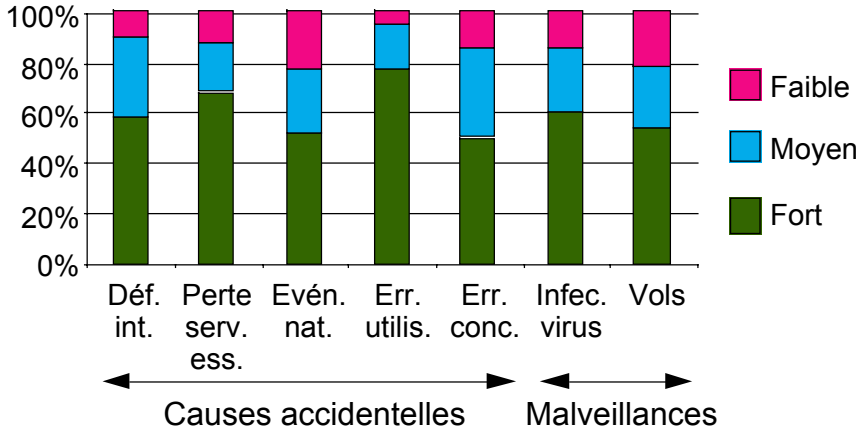
Occurrences



Perception des risques



Impact des occurrences

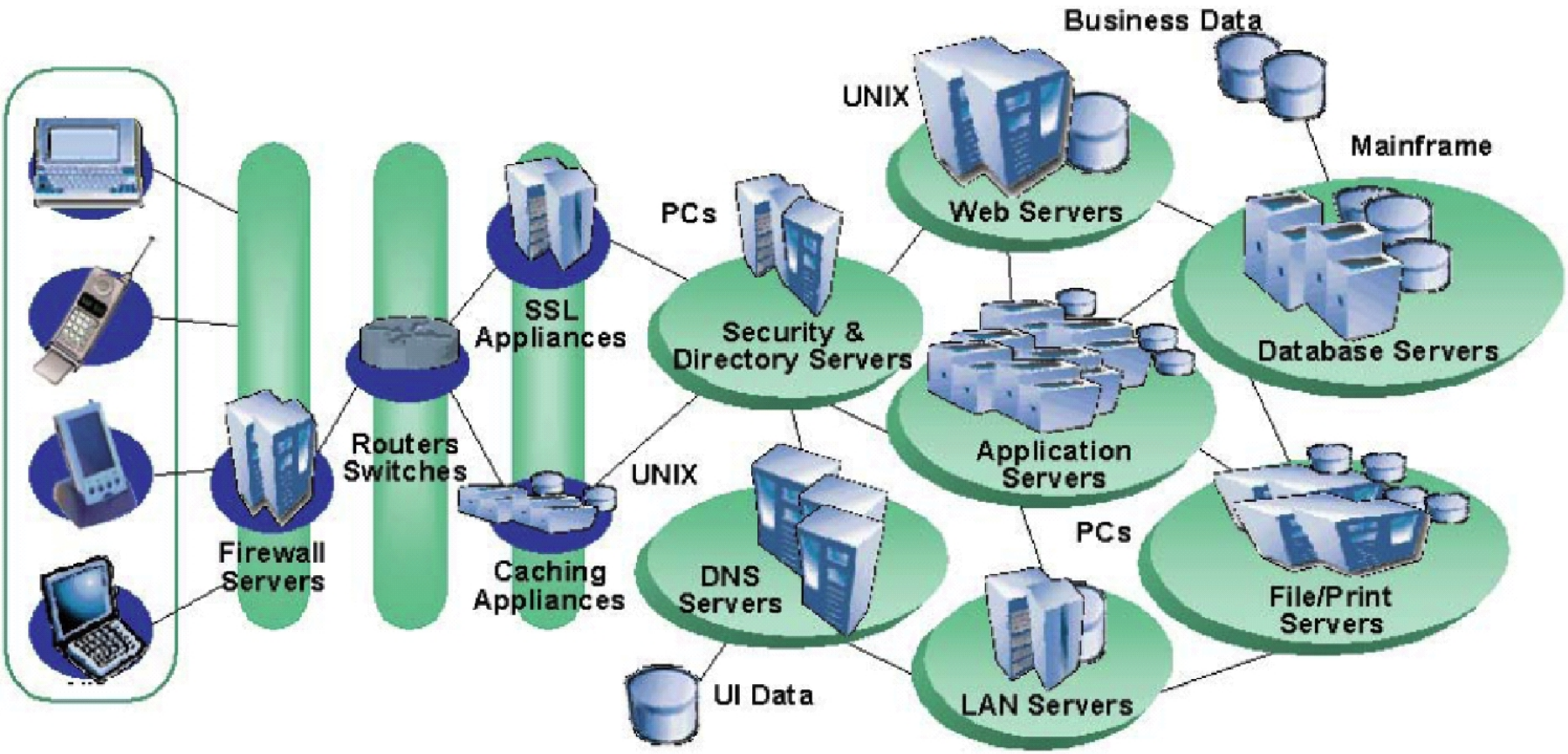


Tendances sur 3 ans

→ stable

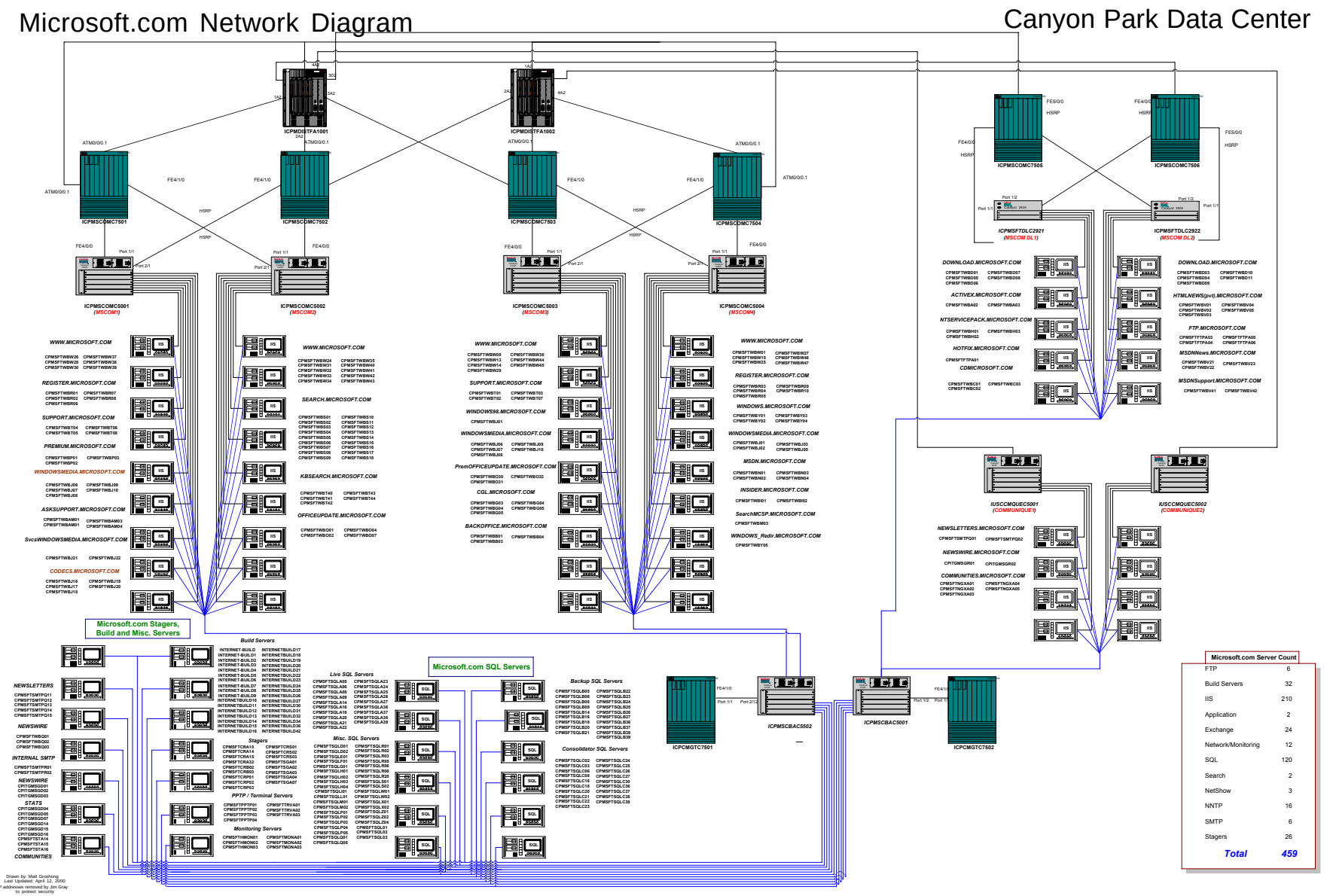
↗ accroissement

↘ diminution



D’après N. Bowen (IBM), *Autonomic Computing*

Ferme de serveurs (500 serveurs)



D'après J. Gray, *Dependability in the Internet era*

(Raisonnablement) maîtrisé: haute sûreté de fonctionnement pour systèmes critiques vis-à-vis sécurité-innocuité ou disponibilité

Avionique, signalisation ferroviaire, commande-contôle nucléaire, etc.

Traitement transactionnel, serveurs dorsaux, etc.

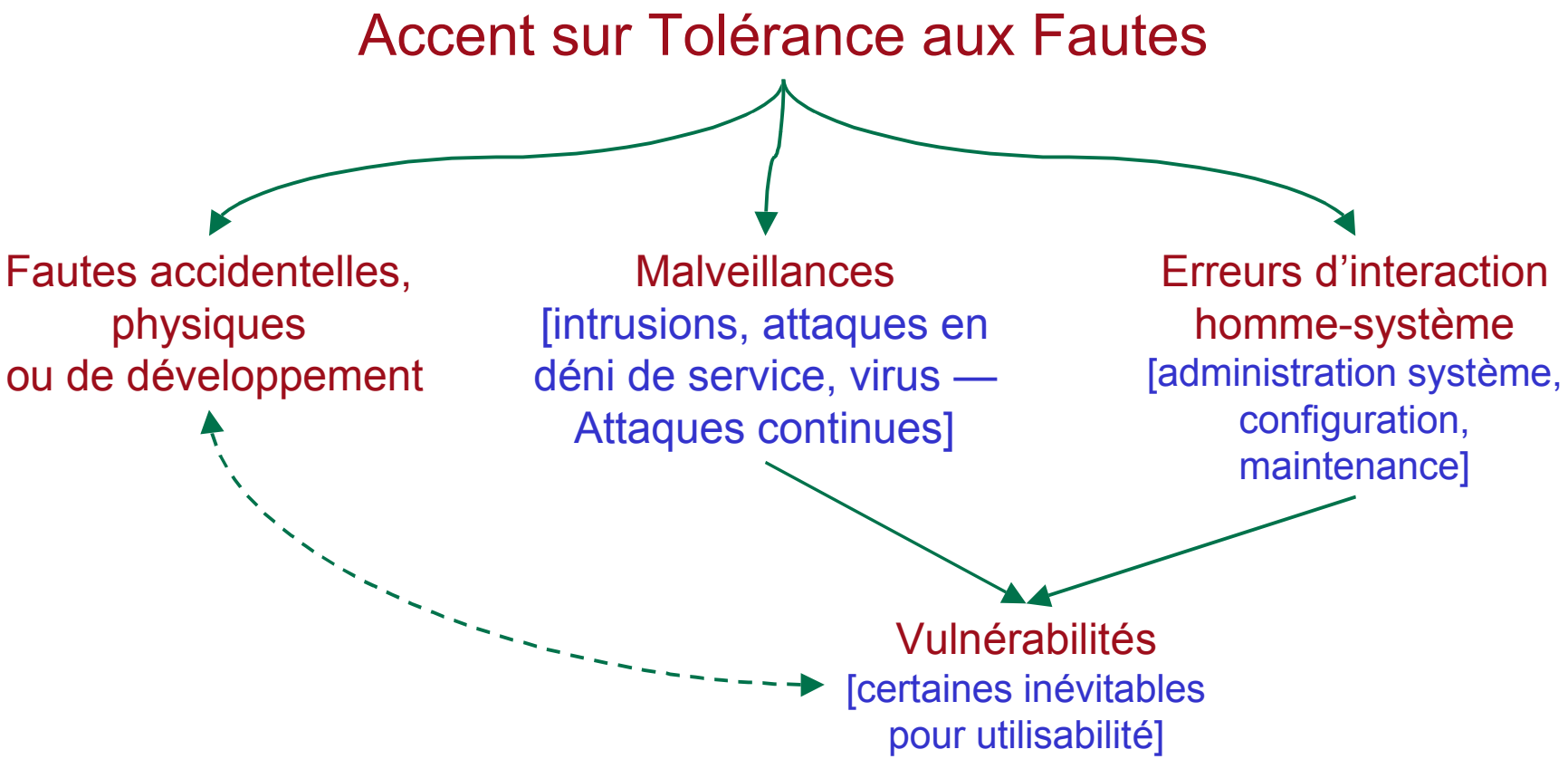
Croissance continue de la complexité
(applications web, serveurs frontaux, réseaux de systèmes enfouis ; fixes ou mobiles)

Ecart en sûreté de fonctionnement
entre confiance attendue par utilisateurs et réalité statistique

Changement d'échelle de la sûreté de fonctionnement

En complément de la prévention et de l'élimination des fautes,

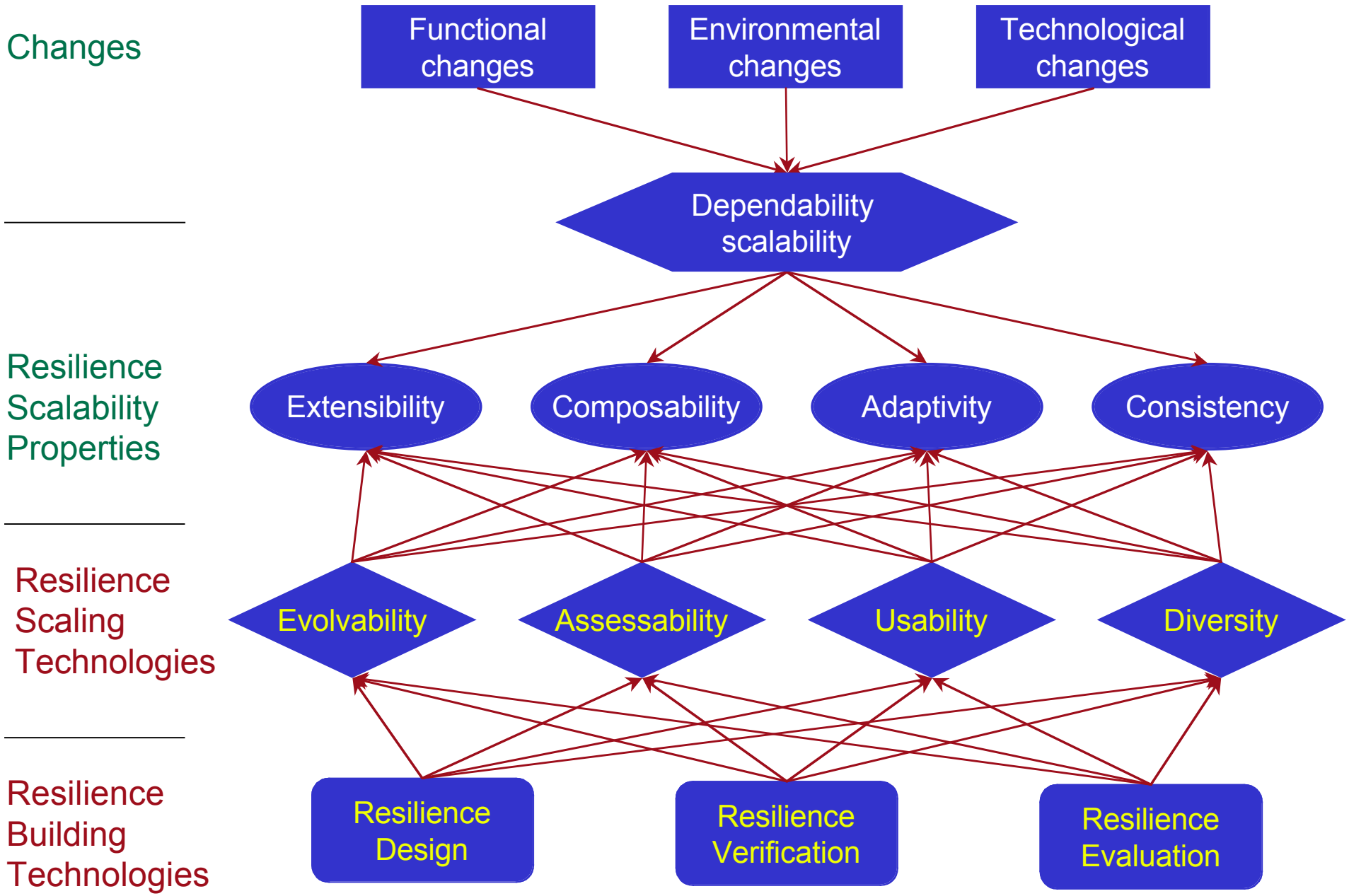
Accent sur Tolérance aux Fautes

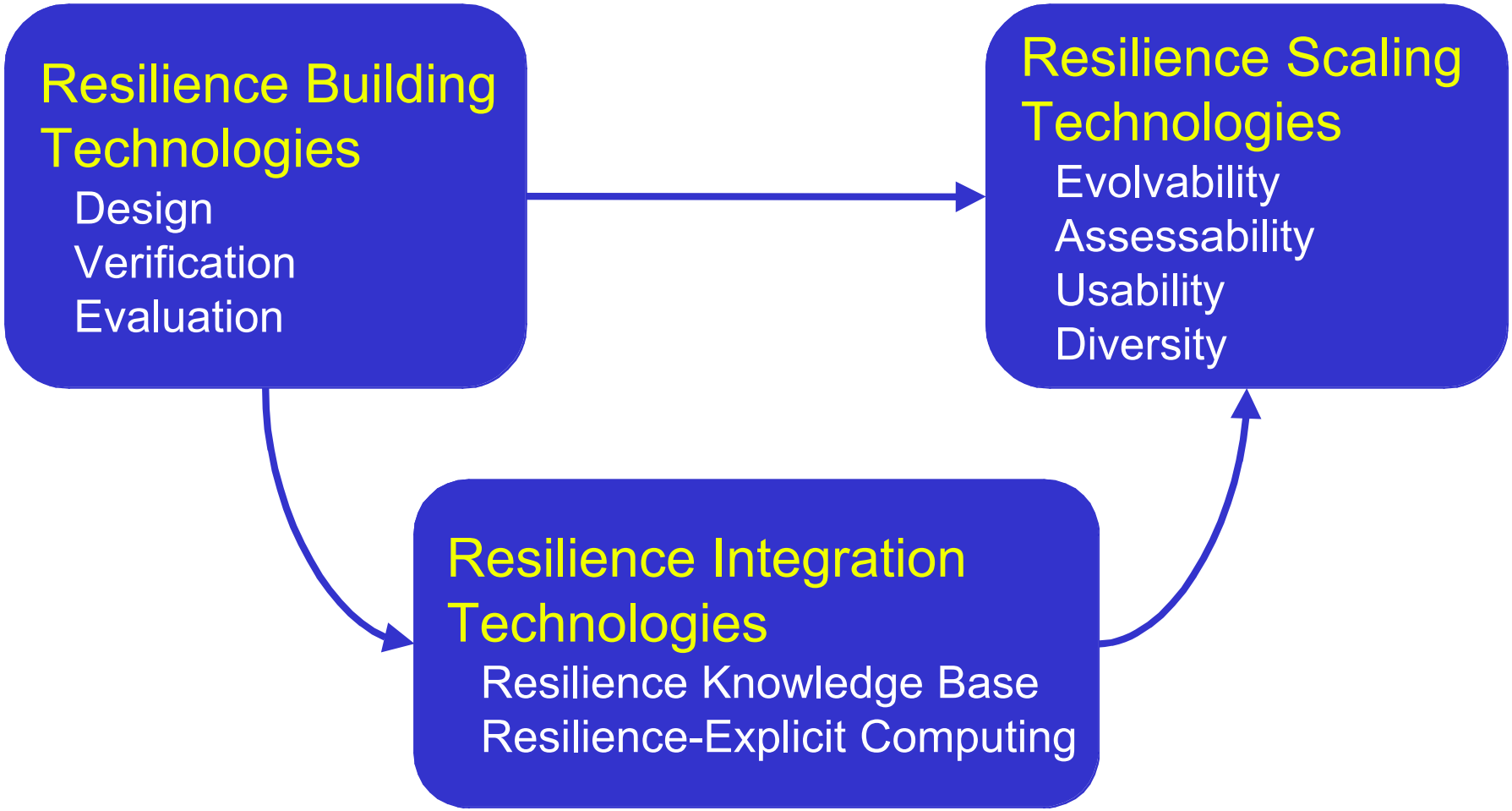


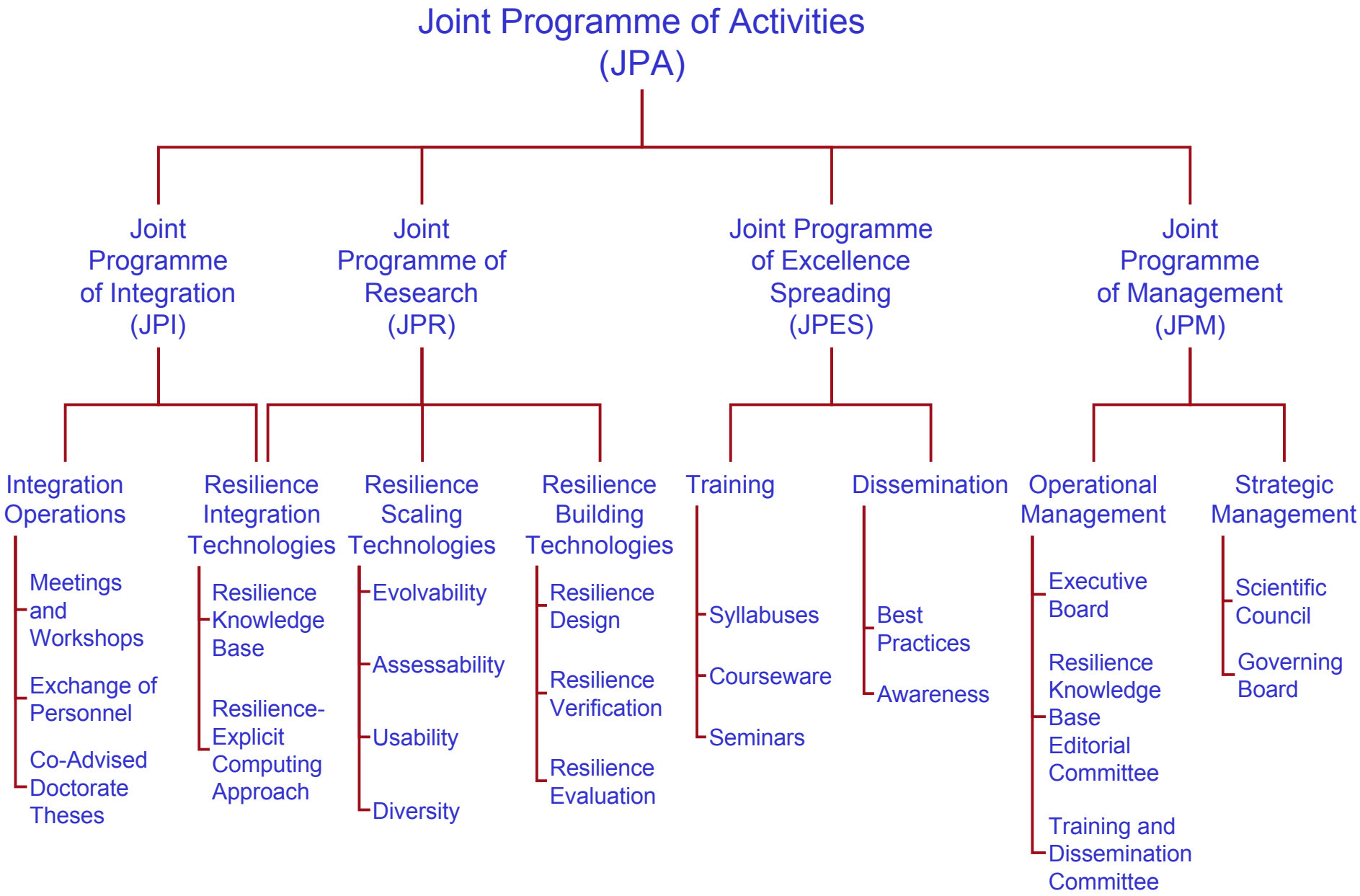
Réseau d'excellence européen

ReSIST

[Resilience for Survivability in Information Society Technologies]


Changes
Functional changes
Environmental changes
Technological changes
Dependability scalability
Resilience Scalability Properties
Extensibility
Composability
Adaptivity
Consistency
Resilience Scaling Technologies
Evolvability
Assessability
Usability
Diversity
Resilience Building Technologies
Resilience Design
Resilience Verification
Resilience Evaluation

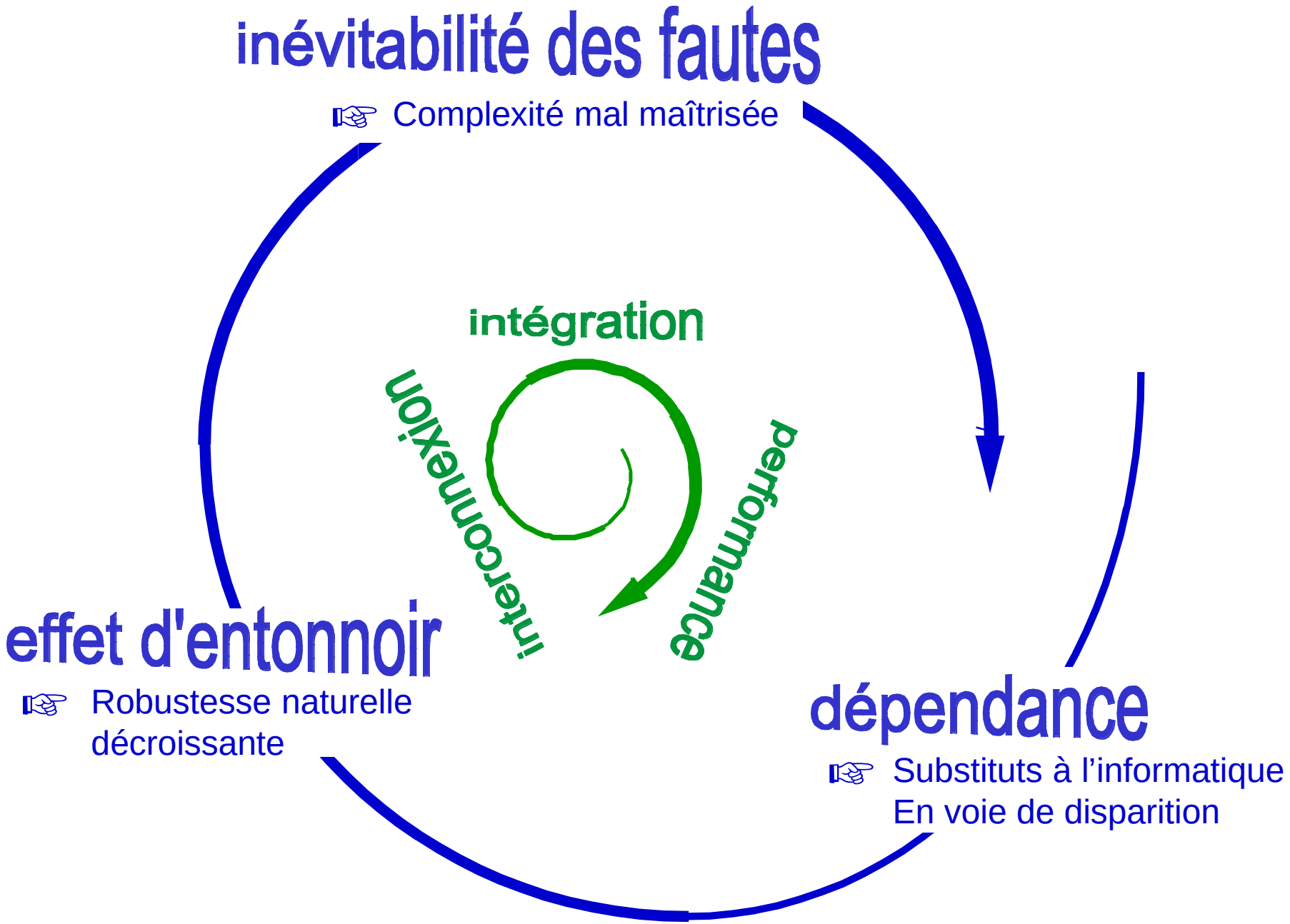

Resilience Building Technologies
Design
Verification
Evaluation
Resilience Scaling Technologies
Evolvability
Assessability
Usability
Diversity
Resilience Integration Technologies
Resilience Knowledge Base
Resilience-Explicit Computing


Joint Programme of Activities (JPA)
Joint Programme of Integration (JPI)
Joint Programme of Research (JPR)
Joint Programme of Excellence Spreading (JPES)
Joint Programme of Management (JPM)
Integration Operations
Meetings and Workshops
Exchange of Personnel
Co-Advised Doctorate Theses
Resilience Integration Technologies
Resilience Knowledge Base
Resilience-Explicit Computing Approach
Resilience Scaling Technologies
Evolvability
Assessability
Usability
Diversity
Resilience Building Technologies
Resilience Design
Resilience Verification
Resilience Evaluation
Training
Syllabuses
Courseware
Seminars
Dissemination
Best Practices
Awareness
Operational Management
Executive Board
Resilience Knowledge Base Editorial Committee
Training and Dissemination Committee
Strategic Management
Scientific Council
Governing Board

Partners

	Fault class resilience				Mobility	Country	Academia (A) / Industry (I)
	Accidental			Malic-ious (M)			
	Physical (PA)	Devel-opment (DA)	Inter-action (IA)				
	PA	DA	IA	M			
Budapest	PA					HU	A
City University		DA	IA	M		UK	A
Darmstadt	PA	DA				DE	A
DeepBlue			IA			IT	I
Eurecom				M	x	FR	A
France Telecom	PA			M	x	FR	I
IBM Zurich				M		CH	I
IRISA	PA	DA			x	FR	A
IRIT			IA			FR	A
Kaunas	PA	DA				LT	A
LAAS [coordinator]	PA	DA		M	x	FR	A
Lisbon	PA			M	x	PT	A
Newcastle		DA	IA	M		UK	A
Pisa	PA	DA	IA			IT	A
Qinetiq		DA		M		UK	I
Roma-La Sapienza	PA				x	IT	A
Ulm		DA				DE	A

71 researchers plus 44 students, 3 year (initial) duration


inévitabilité des fautes
☞ Complexité mal maîtrisée
intégration
interconnexion
performance
dépendance
☞ Substituts à l'informatique
En voie de disparition
effet d'entonnoir
☞ Robustesse naturelle
décroissante