

La gestion des risques : une approche systémique

Conférence GITI
Mardi 22 mai 2007
Cern, Genève

Prof. Emmanuel Fragnière, CIA

Emmanuel.Fragniere@hesge.ch

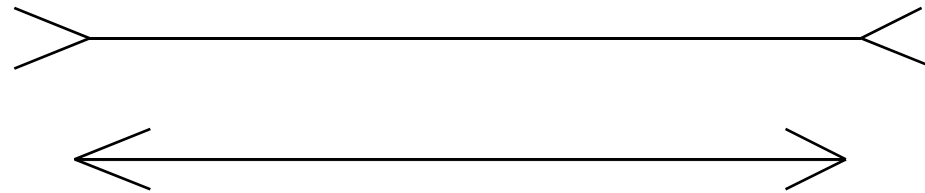
Sujets traités:

- Systémique et cybernétique : la notion d'autorégulation dans un contexte d'automatisation
- Contexte d'économie de la connaissance : des capteurs basés sur la perception humaine
- Méthodologies de gestion des risques : des approches peu influencées par la systémique
- La « chaîne des risques » : un système de contrôle adapté à l'intangibilité des services
- La gestion des risques comme outil de la sécurité des SI ? Approche normative versus expertise métier

Systemique et cybernetique

- Norbert Wiener, 1948
- Influence majeure de la science des systèmes sur l'automation
- Un contrôle de « contre-réaction » sur une chaîne de montage permet d'autoréguler la production (principe du thermostat)
- Les informations objectives collectées par les capteurs sont comparées à des tolérances

La notion de risque perçu



- D'une façon générale un service est perçu comme plus risqué qu'un produit
- Le service est sujet à plus grande variabilité
- Il y a souvent une méconnaissance des avantages à retirer inhérents au service

Définition du risque opérationnel

Le risque opérationnel correspond au risque de perte directe ou indirecte résultant de processus internes, de personnes, de systèmes inadéquats ou défectueux ou encore d'événements externes.

Caractéristiques du risque opérationnel dans les banques:

- Agrégation et quantification difficiles,
- Importance du système d'information,
- Implication des unités de gestion (décentralisation du risque),
- Risque d'origine humaine dans la plupart des cas.

Étapes de la gestion des risques

1. Identification des risques

2. Attribution de la responsabilité des risques

3. Gestion des risques :

- Procédures d'évitement
- Procédures de prévention
- Procédures de secours ou de sauvetage
- Assurance (traitement financier du risque)
- Sous-traitance

4. Système de contrôle interne

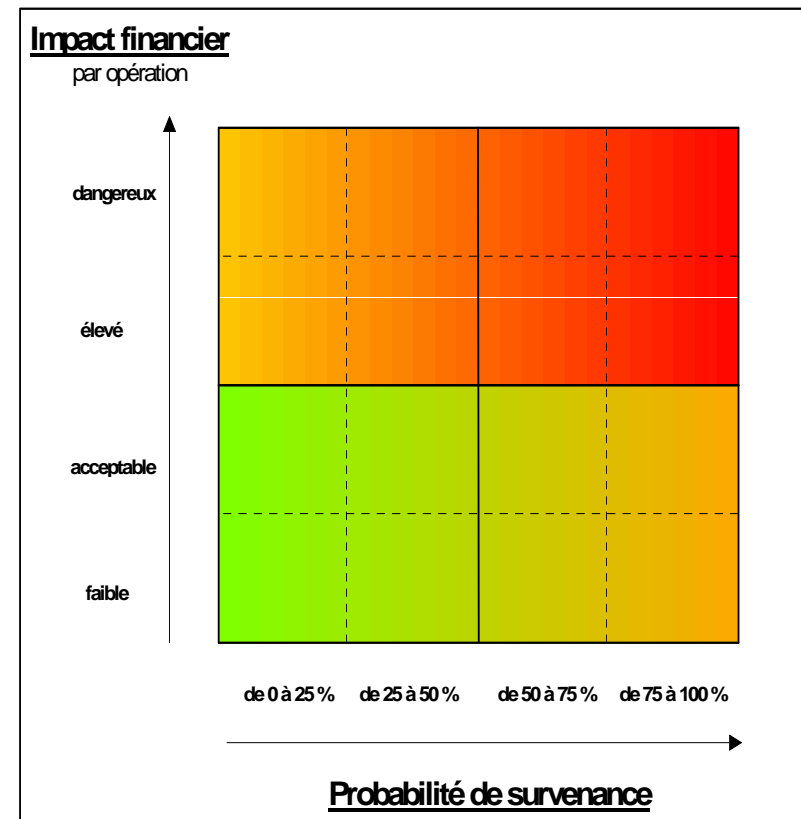


Cartographie des risques

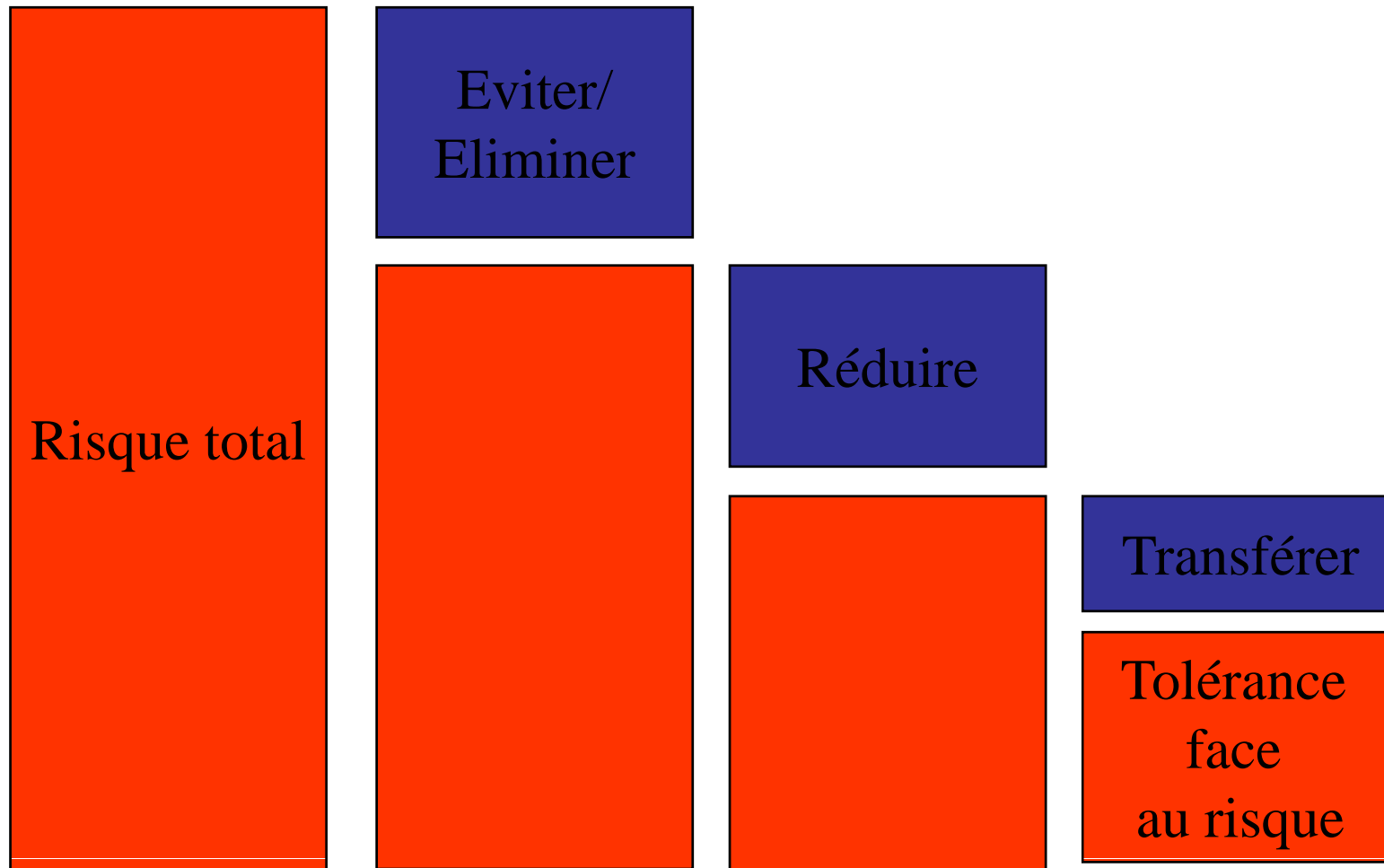
- Le plus souvent l'appréciation risque est présentée comme suit :

Risque = Dommage x probabilité

- Cette approche est toutefois limitative car
 - Les deux variables (dommage et probabilité) ne peuvent souvent pas être mesurées
 - Les cas extrêmes sont mal appréhendés



Traitement du risque



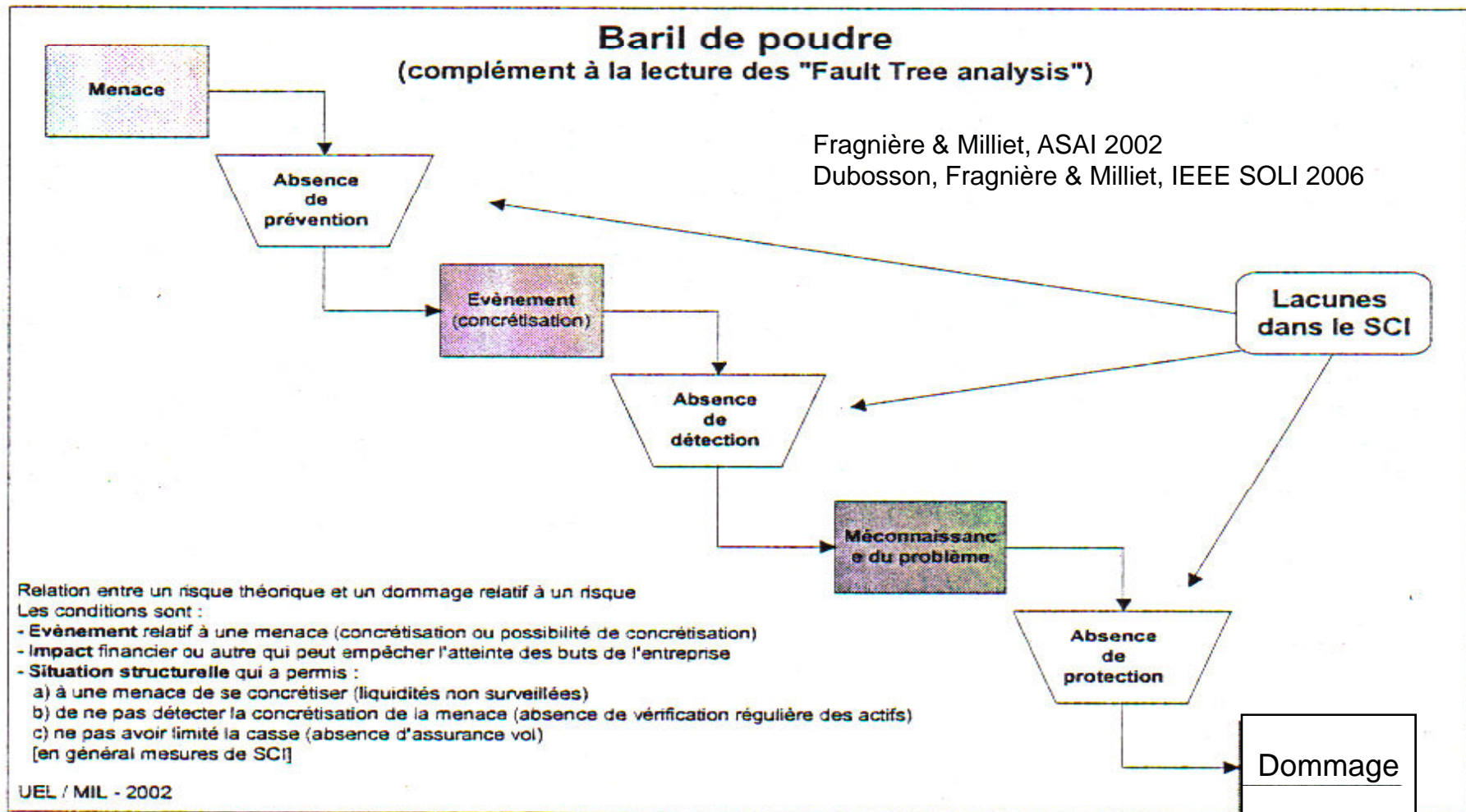
Étapes du processus de contrôle :

- Fixation des standards,
- Mesure et communication des résultats,
- Actions correctrices (ne rien faire, corriger l'objectif, amélioration).

Type de contrôle :

- *Contrôle a posteriori* : le résultat est comparé à l'objectif et une mesure corrective est éventuellement proposée. Un contrôle a posteriori est typiquement utilisé dans des situations à court terme (ex. contrôle budgétaire).
- *Contrôle anticipé* : dans le cas de décisions stratégiques (i.e. risque à long terme), les résultats ne se feront sentir que dans quelques années. Ainsi, nous devons recourir à un contrôle d'un type différent. Ce dernier, appelé "aussi contrôle anticipé", tente de comparer la prévision du résultat à l'objectif.

Modèle de détection des risques



COSO II + COBIT

Les thèmes développés dans les normes « Internal Control – Integrated Framework » sont intégralement repris dans le projet « Enterprise Risk Management Framework ». Cependant, trois nouvelles dimensions sont traitées :

- Définition des objectifs
- **Identification des événements**
- Réaction face aux risques

Normes vs expertise métier

- Thèse : réserve stratégique au sens militaire pour gérer les risques des SI
- Illustration : le samouraï qui passe ses journées à s'occuper de ses bonzaïs
- Paradoxe : l'économie de la connaissance reposera plus sur la connaissance tacite que sur l'information (connaissance codifiable)
- Débat : l'expert SI doit-il se fier à son instinct ou à des normes standardisées ?