



Maitrise des risques

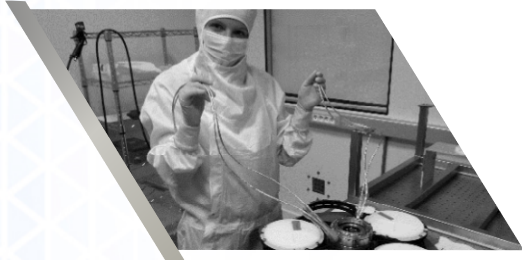
William REcart – Responsable Pôle Logiciel

william.recart@nexeya.com - 06 10 64 39 61

18/04/2019



- Définition de la gestion des risques
- Gestion d'un risque
- La documentation des risques





Définition de la gestion des risques

➤ Gestion des risques permet :

- d'identifier,
- d'évaluer ,
- de réduire,
- de surveiller et
- d'accepter.

les risques constituant une menace pour la réussite du projet

➤ Les types de risques :

- **Risques de non-obtention des exigences spécifiées;**
- **Risques techniques, de performance et de sûreté de fonctionnement;**
- **Risques liés aux technologies retenues, à la pérennité des fabricants, et à l'obsolescence des composants matériels et logiciels;**
- **Risques économiques (coûts) et calendaires (délais).**

➤ **Bénéfices de la gestion des risques :**

- **Maitriser et tirer parti du Design, de la fabrication, des tests, des opérations et de la maintenance;**
- **Contrôler les conséquences d'un risque;**
- **Maitriser les coûts, les délais et la gestion du projet;**



Gestion d'un risque

➤ **Quand réaliser la gestion des risques ?**

- **Dés le démarrage du projet ;**
- **Tout au long du projet ;**
- **Et même en maintenance / exploitation ;**

➤ Etapes de la gestion d'un risque :

1. Identification du risque;
2. Identification du scénario du risque;
3. Décision sur l'acceptabilité du risque;
4. Définition de l'action en réduction du risque;
5. Recommandation d'acceptation du risque;
6. Suivi et communication du risque;
7. Soumission de l'acceptation du risque;

**En cas de non-acceptation du risque,
l'étape 4 est reprise**

➤ **Caractérisation d'un risque :**

- **Description ;**
- **Analyse des causes;**
- **Analyse des conséquences;**
- **Action de surveillance;**
- **Evolution de la gravité du risque;**

➤ Analyse des causes:

Notion de sévérité du risque : (exemple à 5 niveaux)

- **Catastrophique: le projet / la mission n'aboutira pas;**
- **Critique : le projet / la mission sera fortement dégradé et une partie perdue;**
- **Majeur : le projet / la mission sera dégradé;**
- **Mineur : le projet / la mission sera impactée;**
- **Négligeable : L'impact sera minimal voire néant.**

➤ Analyse des conséquences:

**Notion de probabilité du risque :
(exemple à 5 niveaux)**

- **Maximum: le risque apparaîtra (1/1);**
- **fort : le risque apparaîtra fréquemment (1/10) ;**
- **moyen: le risque apparaîtra parfois (1/100);**
- **faible: le risque apparaîtra rarement (1/1 000);**
- **Minimum: le risque n'apparaîtra pas (< 1/10 000).**

➤ Gravité du risque :

Notion basée sur la sévérité et la probabilité:

Probabilité

Maximum	Faible	Moyenne	Forte	Très forte	Très forte
Fort	Faible	Faible	Moyenne	Forte	Très forte
Moyen	Très Faible	Faible	Faible	Moyenne	Forte
Faible	Très Faible	Très Faible	Faible	Faible	Moyenne
Minimum	Très Faible	Très Faible	Très Faible	Très Faible	Faible

Négligeable Mineur Majeur Critique Catastrophique Sévérité

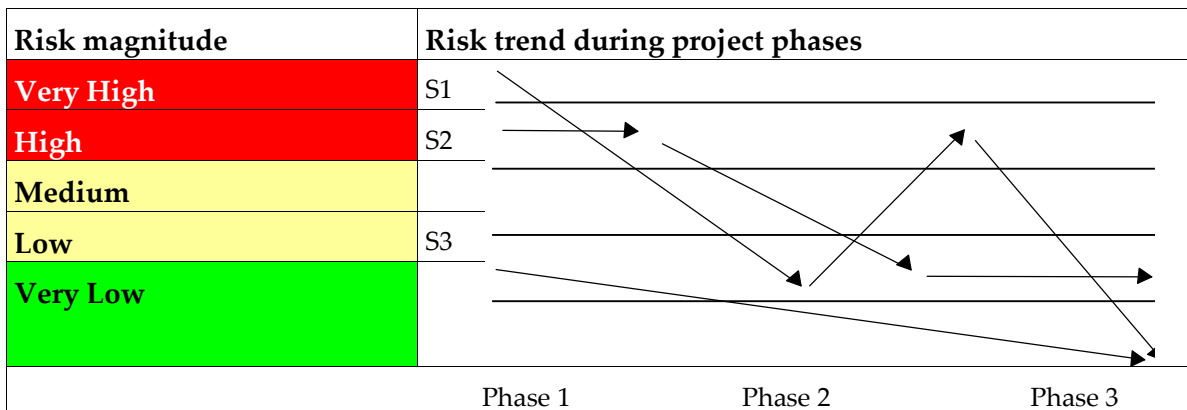
➤ Proposition d'actions liées à la gravité du risque:

- **Très forte et forte :**
le risque est inacceptable : modification de la baseline ou des process. Le risque est à remonter au plus haut niveau du projet.
- **Moyenne :**
le risque est inacceptable : il doit être suivi de très près. Des alternatives à la baseline ou aux process peuvent être envisagées.
- **Faible et très faible :**
le risque est acceptable : il doit être suivi et contrôlé.

➤ Suivi des risques:

Doit être évalué régulièrement :

- Réévaluation de la sévérité et de la probabilité d'un risque à chaque élément nouveau.



- Ne pas hésiter à évaluer de nouveaux risques à chaque nouvel événement (changement de baseline, de design, de RH, etc ...)



La documentation des risques

➤ **Le portefeuille des risques :**

- **Présenté sous forme de tableau:**

ID du risque

Description du risque

Sévérité

Probabilité

Gravité

Evolution du risque

Domaine du risque (coût, délais, technique, ...)

Actions (préventives et correctives)

Responsable du risque

➤ Cas des risques techniques et éléments critiques:

- **FMEA (Failure Modes and Effects Analysis):**
Document présentant les modes de défaillance identifiés et leurs effets

=> Permet de prendre les décisions de redondance, d'inhibition, cas de tests, contraintes opérationnelles, etc ..

➤ Cas des risques techniques et éléments critiques:

- **HSIA (Hardware Software Interaction Analysis)**
Document présentant les réactions du logiciel à une défaillance matérielle

=> Permet de définir les réactions du logiciel pour chaque mode de défaillance de la FMEA, dans les cas de redondance, d'inhibition, cas de tests, contraintes opérationnelles, etc ...

➤ Cas des risques techniques et éléments critiques:

- **FDIR (Failure Detection, Isolation and Recovery)**
Document découlant de la FEMA pour présenter:
 - Les paramètres à surveiller pour détecter l'erreur;
 - Les vérifications à réaliser pour s'assurer de la récupération;
 - La proposition de solution alternatives
 - L'identification des modes de défaillance non suivis.



Questions ?