retour à l'article

Défense en Profondeur et ingénierie système : une synergie au profit d'une approche globale des risques et des responsabilités

Auteurs	**Catherine LAVAL**.	**Alain COINTET**
Société :	APTE SYSTEM	R.A.T.P.
Adresse :	2 rue GARREAU 75018 PARIS	46 rue Roger SALENGRO 94724 FONTENAY SOUS BOIS
Téléphone :	(33) 1 42 51 21 70	(33) 1 58 76 96 66
Fax :	(33) 1 42 51 61 31	(33) 1 58 77 12 44
e-mail :	catherine.laval@apte-system.com	alain.cointet@ratp.fr

Objectifs

La Défense en profondeur constitue une approche globale et dynamique des risques que ce soit dans le cadre du développement d'un nouveau système, ou celui de la maîtrise d'un système existant.

Pour exploiter efficacement ce concept et les principes qui le définissent, une démarche d'analyse structurée d'un système de défense a été élaborée et est en cours d'application sur des éléments majeurs du système de transport RATP.

Notre souci est ici de montrer en quoi une telle méthodologie :

- Modifie radicalement le point de vue de l'analyste, en le positionnant dans une logique d'aide à la décision intégrant des notions d'efficacité, d'anticipation et d'amélioration.
- Impose, en amont, une clarification de la politique de maitrise des risques, par l'entreprise,
- Offre aux décideurs une vision synthétique du système de défense, associée à des indicateurs pertinents de suivi d'efficacité.

L'objectif principal de cette communication est ainsi, plus que de décrire la méthodologie développée, d'illustrer comment elle permet de clarifier les responsabilités de chaque acteur dans le processus de maîtrise des risques,

Contexte

Trois constats sont à l'origine des développements méthodologiques présentés ici :

Limites des approches classiques de maîtrise des risques

Les points de vue des analyses de risques se fondent sur des approches de maîtrise des risques, à partir d'événements redoutés et de leurs causes, et des notions d'occurrence et de gravité. Leur logique s'attache à la maîtrise des éléments pouvant contribuer à l'apparition de l'événement redouté et/ou à la variation de la gravité de ses conséquences.

- Dans le cadre d'une gestion des causes, la question initiale est « qu'est-ce que l'on redoute ? quel est l'événement à éviter ?»

Le retour d'expériences, permet, quant à lui, de comprendre un enchaînement de faits ayant conduit à un événement redouté, afin d'en dégager des recommandations d'amélioration d'un système. Il s'attache, lui aussi, à la compréhension des séquences de défaillances.

Il manque à ces approches un point de vue plus global et déterministe, s'attachant à la **maîtrise des effets finaux** vis-à-vis d'éléments (hommes, système, entreprise et/ou environnement) déclarés sensibles à des agressions. C'est ce que propose la Défense en profondeur, finalisée sur l'efficacité du système pour assurer le **maintien des effets dans des limites d'acceptabilité données.**

- Dans le cadre d'une gestion des effets finaux, la question initiale sera « qui ou quoi veut-on protéger ? de quoi ? jusqu'où ? » :

Difficulté d'appropriation du concept de défense en profondeur

Les domaines militaire, nucléaire et industriel sont fondateurs du concept de Défense en profondeur : d'autres domaines, tels que les systèmes d'informations, s'y intéressent depuis quelques années.

Ce concept présente des intérêts majeurs, car il se fonde sur une approche résolument systémique, en s'attachant aux menaces, à la globalité de défense d'un système, et en intégrant la complexité des situations et des éléments de défense.

Toutefois, peu d'appropriations de ce concept ont fait émerger une méthodologie structurée et des outils permettant de spécifier, modéliser et valider un système de défense, existant ou projeté.

Complexité des systèmes et la nécessité de clarification des rôles des acteurs :

Dans le contexte concurrentiel où se situe aujourd'hui tout système de transport, la sécurité est un facteur dominant, mais il doit être maîtrisé conjointement à la qualité de service et à la compétitivité de l'entreprise. La maîtrise des risques se complexifie alors avec la prise en compte de facettes diverses et évolutives : technologique, informationnelle, humaine, organisationnelle, environnementale, économique, commerciale,…

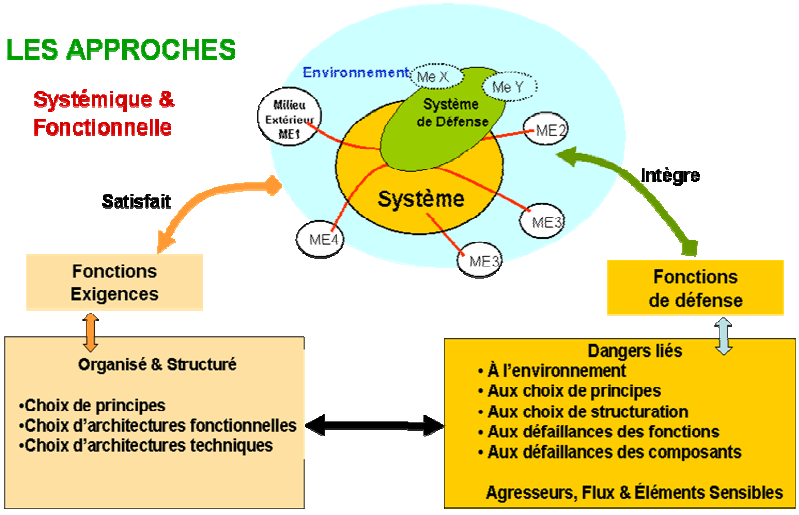
Cette complexité croissante impose, outre l'emploi d'outils de modélisation, une clarification du processus de décision lié au management des risques, et une clarification des champs respectifs de responsabilité des acteurs, impliqués dans ce processus.

Méthode

(Un rapide historique du concept de défense en profondeur, permettra tout d'abord d'en rappeler les notions fondatrices : lignes de défense, barrières,.).

La démarche proposée se fonde sur **une modélisation hiérarchique d'un système de défense**, sur base d'une approche d'ingénierie système intégrant l'analyse fonctionnelle.

L'ingénierie système apporte sa rigueur de représentation ; l'analyse fonctionnelle apporte sa démarche résolument systémique ainsi sa pertinence pour fonder toute modélisation sur des référents pérennes, que sont les finalités et les fonctions système.



Quatre niveaux structurent la modélisation :

Niveau 0 : Un préalable, l'expression des finalités de défense

La DEFENSE d'un système de transport a pour objet d'assurer en tous temps, en toutes circonstances et contre toutes formes d'agression, la sécurité et l'intégrité requises des hommes, du système, de l'entreprise et de son environnement.

Les finalités de défense, dans un contexte donné, s'expriment alors vis-à-vis :

- des trois types «d'acteurs» en présence : agresseurs potentiels, flux agressifs émis par ces agresseurs, éléments sensibles pouvant subir des dommages de par ces agressions.
- des effets finaux directs ou combinés, que l'on souhaite maîtriser, selon les types d'éléments sensibles et à leur domaine de sensibilité.

Cette définition impose de quantifier les niveaux d'acceptabilité associés à chaque effet final (sur le système, ses utilisateurs, les organisations impliquées et l'environnement) : quels sont les effets acceptables, les effets inacceptables, mais aussi les effets tolérés.

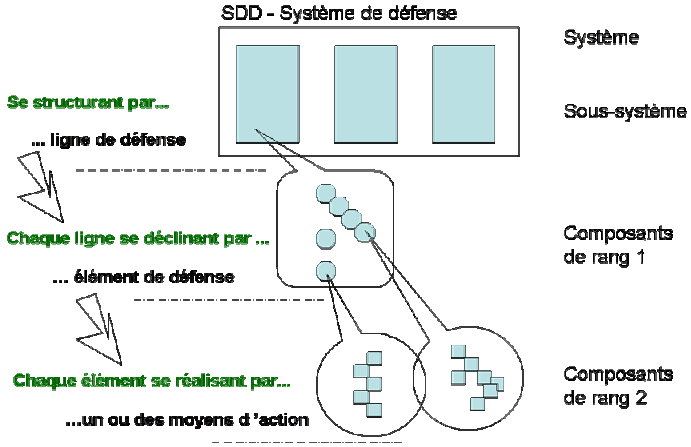
Ces niveaux d'acceptabilité **sont indépendants des situations et événements redoutés pouvant conduire à l'effet final considéré : ils dépendent strictement du système de valeurs retenu et relèvent alors clairement de choix de niveau « politique d'entreprise ».**

Ainsi axée sur la maîtrise des effets finaux et la notion d'acceptabilité, la démarche proposée est cohérente avec les logiques de décision des décideurs :

- les effets finaux traitent des conséquences dans les domaines relevant de leur champ de responsabilité : services attendus du système de transport, sécurité des personnes, protection de l'environnement, pérennité financière de l'entreprise, image de l'entreprise.
- la notion d'acceptabilité intègre un **raisonnement multicritères, propre à tout processus de décision**. Par exemple, pour un effet final sur les personnes, sera considéré l'intégrité physique, mais aussi leur propre acceptation du risque subi, à un niveau individuel ou collectif, et dans le cadre d'effets combinés, également l'impact sur l'image de l'entreprise,…

La « cible » de défense ainsi choisie au niveau politique devient alors un référentiel des exigences à satisfaire pour toute conception, gestion ou amélioration du système.

Les trois niveaux suivants sont basés sur une approche d'ingénierie système :



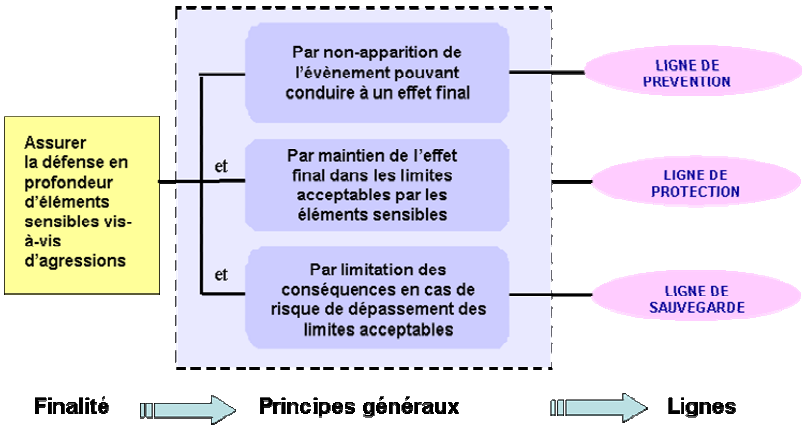
Niveau A • Une structuration par lignes de défense, en réponse aux finalités de défense

La DEFENSE EN PROFONDEUR met en œuvre, vis-à-vis d'agressions internes et externes, potentielles ou avérées, des parades successives et autonomes, et cela sur tout le cycle de vie du système.

La structuration proposée décline chaque finalité de défense en la précisant sous trois principes complémentaires, qui correspondent à des choix de stratégies d'action pour satisfaire les exigences précédemment caractérisées :

- **un principe de prévention**, consistant à agir sur la probabilité d'apparition d'un événement redouté,
- **un principe de protection**, devant maintenir les effets finaux dans les limites acceptables définies au sein de la politique de défense,
- **un principe de sauvegarde**, destiné à limiter l'ampleur des conséquences dans les cas où l'accident ne peut être évité, et donc à agir à la fois sur la gravité de l'effet final et la non-combinaison avec d'autres effets finaux.

Ces trois principes induisent une architecture du système en 3 sous-systèmes ou « lignes de défense », et la modélisation qui en découle est assimilable, en ingénierie système, à une architecture fonctionnelle du système de défense.



La notion de « profondeur » prend ici tout son sens en « affichant » **l'engagement de poursuivre les actions de défense au-delà des principes classiques de prévention et de protection**, en intégrant des actions de sauvegarde, après accident, que ce soit par des moyens internes, ou par transfert, total ou partiel, à des moyens externes.

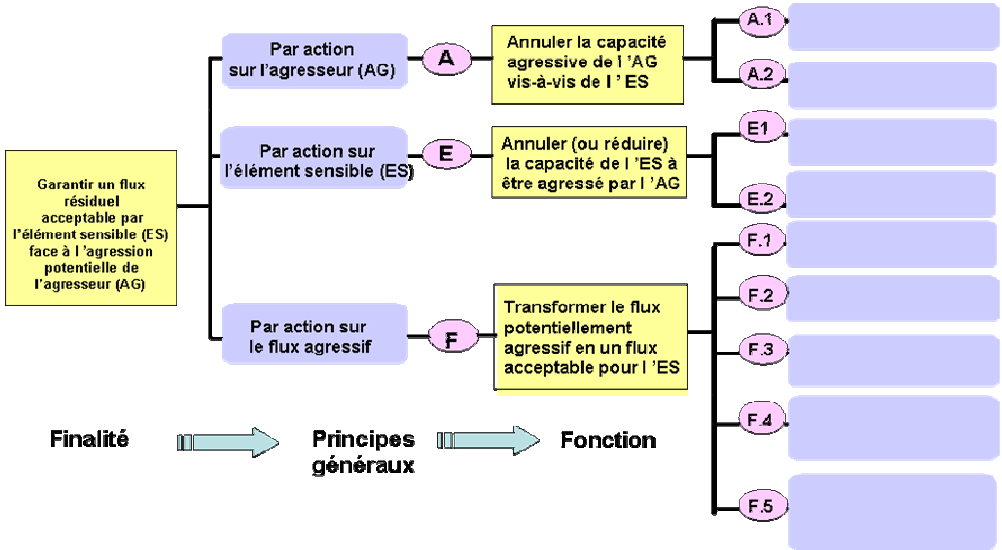
Niveau B • Une identification des éléments de défense constituant chaque ligne de défense

Les éléments constituant chaque ligne de défense (qu'ils soient existants ou projetés) sont définis via la détermination des choix de principes d'action face à l'agression, et aux interactions entre éléments de défense, d'une même ligne et entre lignes.

Ce niveau d'analyse, assimilable, en ingénierie système, à la définition d'une architecture logique du système de défense, impose de justifier chaque élément en regard de la pertinence du mode d'action retenu pour satisfaire la fonction de prévention, *de* protection ou *de* sauvegarde : action sur l'agresseur, action sur l'élément sensible ou action sur le flux.

La détermination de ce mode d'action permet alors de définir (ou valider) les performances attendues de l'élément, dans le cadre de sa contribution à la ligne de défense considérée.

Une arborescence générique des principes d'action permet de situer le mode d'action considéré : un extrait de cette arborescence est fourni ci-après.



Niveau C • Une définition de chaque élément de défense

Chaque élément de défense se définit concrètement alors à travers :

- les **moyens d'action** mis en œuvre : moyens internes ou externes au système, équipement et/ou système d'informations (de type automatismes), et/ou homme(s) avec ou sans procédure(s).
- les modes d'activation et de contrôle de ces moyens,
- les fonctions attendues de l'élément de défense, et les exigences associées,

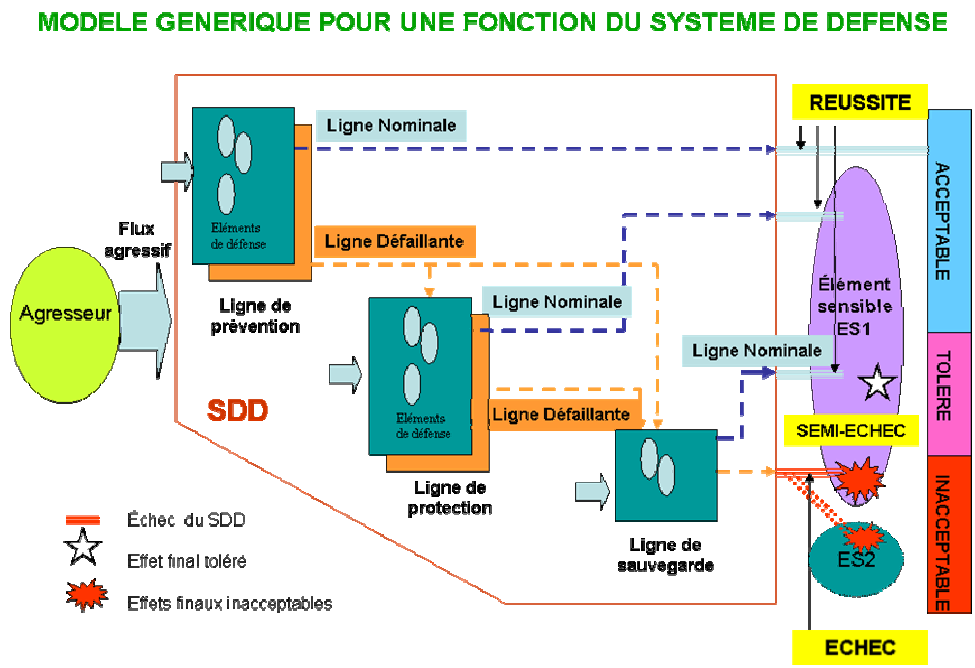
Ces définitions permettent de modéliser l'architecture technique du système de défense. Si besoin, ces analyses peuvent se poursuivre, compte tenu de la démarche d'ingénierie systèmes qu'elles intègrent, à des niveaux plus fins : fonctions élémentaires des moyens d'action, technologies mises en œuvre,…

Ainsi l'analyste peut :

- Etablir (ou retrouver) la traçabilité entre les éléments de défense considérés et les finalités de défense auxquelles ces éléments contribuent.
- Valider la pertinence des moyens mis en œuvre en regard des performances attendues de l'élément.

(NOTA : au cours de la communication, cette structuration sera illustrée à travers son exploitation en tant que grille de lecture d'exemples connus : le plan Canicule, les plans de prévention des risques d'inondation,…)

Résultats



Outre le fait d'offrir aux décideurs et autres acteurs une représentation commune et synthétique du système de défense, trois types de résultats ressortent de l'application de cette méthodologie structurée de défense en profondeur :

Une clarification des notions d'indicateurs et précurseurs

Sur la base de ce modèle, ont été définies des notions d'indicateurs et de précurseurs.

- Le premier s'inscrit dans un objectif de suivi de l'efficacité des éléments de défense dans un environnement donné,

- Le second est, quant à lui, axé sur l'apparition d'un élément contextuel dont la combinaison avec d'autres éléments contextuels peut aboutir à des effets finaux inacceptables.

Des indicateurs peuvent ainsi être définis aux différents niveaux de responsabilité : au niveau politique (respect des effets finaux acceptables), au niveau stratégique (fonctionnement des lignes) et au niveau technique (efficacité des éléments de défense).

Des aides aux diagnostics de systèmes et aux études d'impacts:

Sur la base de cette modélisation, l'analyse d'un système de défense (existant ou projeté) se structure alors en différents volets :

- un diagnostic des insuffisances potentielles des lignes et des éléments de défense (écart entre les exigences et les performances atteintes par les éléments prévus),
- un diagnostic des risques de non-respect des exigences (potentialité des défaillances des fonctions attendues des lignes et des éléments la constituant),
- une analyse de pertinence des indicateurs de suivi d'efficacité, et de suivi des précurseurs mis en place ou prévus.

Des définitions génériques des fonctions à assurer par chaque type de ligne de défense, et par un élément de défense ont été faites afin de structurer ces diagnostics.

Les analyses d'impact d'évolutions sont aussi facilitées, qu'il s'agisse d'évolution de l'environnement, de la politique d'entreprise, des technologies ou des organisations et donc d'évolutions :

- de l'agresseur, du flux, des éléments sensibles ou de leur environnement,
- des niveaux d'acceptabilité des effets finaux,
- des principes et moyens mis en œuvre.

Une aide à la définition des responsabilités des acteurs

A chaque niveau, les choix relèvent de domaines technologiques, économiques et organisationnels mais ne portent pas sur les mêmes champs.

Chaque acteur peut ainsi situer son rôle et son champ de responsabilités, en regard du niveau d'action où il intervient (et des exigences définies par le niveau précédent).

Ainsi, la détermination des finalités de défense et des niveaux d'acceptabilité des effets finaux relève d'une responsabilité « politique » ; le choix des stratégies d'action – prévention, protection et surtout sauvegarde, relève d'une responsabilité globale de définition du système de défense ; le choix des moyens d'action relève davantage d'une responsabilité technique et organisationnelle.

Références

[1] INERIS, Analyse des risques et prévention des accidents majeurs (DRA-07), juin 2001.

[2] Guy Planchette, Jacques Valancogne, Jean Louis Nicolet – Et si les risques m'étaient comptés "Editions Octarès 2002.

[3] INERIS, Eléments importants pour la sécurité (DRA-35), mai 2003

[4] SGDN/DCSSI, La défense en profondeur appliquée aux systèmes 'informations, juillet 2004