



**MINISTÈRE
DES ARMÉES**

*Liberté
Égalité
Fraternité*



La vulnérabilité humaine dans les SoSTS

Quand l'humain est la vulnérabilité



Paul Perrotin (24/09/2026)

PLAN

1. LE VERROU : UN OPÉRATEUR N'EST PAS UNE BOÎTE NOIRE
2. RENDRE L'HUMAIN VISIBLE DANS L'ARCHITECTURE
3. EST-CE QUE ÇA MARCHE ? DEUX CAS D'ÉTUDE
4. DEPUIS LA THÈSE : PASSER À L'ÉCHELLE



QUI SUIS-JE ?

Parcours

- Docteur en informatique, thèse soutenue en 2022, menée dans le cadre de la Chaire
- Encadrement : S. Sadou (UBS) , N. Belloir(St-Cyr), D. Hairion (Naval Group), A. Beugnard(IMTA)

Aujourd'hui

- Rlab a la DGA,
- Chercheur associé IRISA / SecReizh



SOMMAIRE

1. LE VERROU : UN OPÉRATEUR N'EST PAS UNE BOÎTE NOIRE

2. RENDRE L'HUMAIN VISIBLE DANS L'ARCHITECTURE

3. EST-CE QUE ÇA MARCHE ? DEUX CAS D'ÉTUDE

4. DEPUIS LA THÈSE : PASSER À L'ÉCHELLE

L'HUMAIN : PREMIER VECTEUR D'ATTAQUE

- L'humain est le **vecteur principal** des attaques sur les systèmes
- Jusqu'à **93 %** des compromissions impliquent une responsabilité humaine
- Et ce n'est pas qu'une question de malveillance

LE PARADOXE

On durcit les machines, on audite les réseaux, on chiffre les liaisons. . .

. . . et on décrit l'opérateur par une case vide dans le schéma d'architecture.



Involontaire



Ignorance



Malveillance

2/43

[1] Data Breach Investigations Report, Verizon, 2016.

DE QUOI PARLE-T-ON ? LES SYSTÈMES DE SYSTÈMES SOCIO-TECHNIQUES

- **Système** : des composants en interaction, organisés pour un objectif
- **Système de systèmes (SoS)** : une capacité qu'aucun système seul n'atteint
- **Socio-technique (SoSTS)** : une partie des sous-systèmes **sont des humains**

DES EXEMPLES QUE VOUS CONNAISSEZ

Une passerelle et son CO en opération • une chaîne de lutte anti-piraterie • une tour de contrôle aérien • un hôpital



Retirer l'humain du modèle, c'est retirer la moitié du système.



CE QUI MANQUAIT — ET LA THÈSE DÉFENDUE

Bilan de l'état de l'art (SoS, socio-technique, facteurs humains)

- L'intégration de l'humain est **superficielle ou inexistante**
- L'estimation de la vulnérabilité est **parcellaire**
- La propagation, quand elle existe, est **linéaire**
- L'impact réel de l'humain n'est **pas défini**

THÈSE SOUTENUE

Il est possible de **caractériser la vulnérabilité d'un opérateur humain** dans un SoSTS et d'en **déduire son impact** — dès la conception, sur le modèle d'architecture.



SOMMAIRE

1. LE VERROU : UN OPÉRATEUR N'EST PAS UNE BOÎTE NOIRE

2. RENDRE L'HUMAIN VISIBLE DANS L'ARCHITECTURE

3. EST-CE QUE ÇA MARCHE ? DEUX CAS D'ÉTUDE

4. DEPUIS LA THÈSE : PASSER À L'ÉCHELLE

BRIQUE 1 — DÉCRIRE UN HUMAIN PAR DES FACTEURS

FACTEURS DIRECTS — LA PERSONNE

Compétence • Expérience • Robustesse • Stabilité émotionnelle • Confiance •
Conscienciosité • Fiabilité • Niveau informationnel • Coopération organisationnelle

FACTEURS INDIRECTS — SON CONTEXTE

Communication • Management • Exigence de la tâche • Politique de sécurité • Culture •
Ressources • Position

Deux types d'échelle, issus des sciences humaines et sociales :

- **Ordinale** : un entier de 1 à 5 (ex. compétence = 3)
- **Catégorielle** : un adjectif (ex. stabilité émotionnelle $\in$ {stable, peu émotif, anxieux, lunatique})

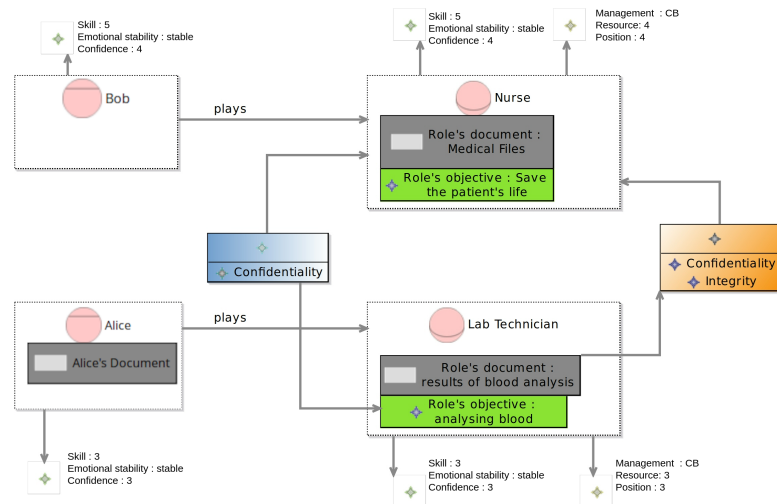
P. Perrotin, N. Belloir, S. Sadou, D. Hairion, A. Beugnard, « HoS-ML : Socio-Technical System ADL Dedicated to Human Vulnerability Identification », ICECCS 2022.

BRIQUE 2 — LE RÔLE ATTENDU, L'ACTEUR RÉEL, ET L'ÉCART

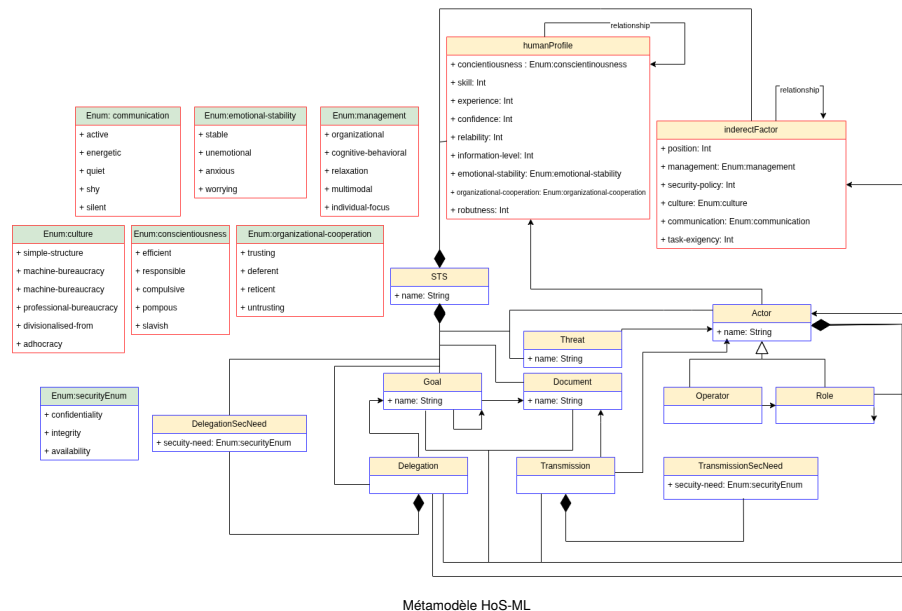
- L'architecte décrit un **rôle** : le profil attendu à un poste (« opérateur bâbord », « chef de quart »)
- Il décrit ensuite un **acteur** qui tient ce rôle : Alice, Bob. ...
- La vulnérabilité naît du **delta** entre les deux

POURQUOI C'EST IMPORTANT

On ne juge pas une personne dans l'absolu : on mesure un **écart à un poste donné**.



- les **rôles** et les **acteurs** qui les jouent
- leurs **facteurs**
- les **objectifs** délégués
- les **documents** transmis
- les **besoins de sécurité** (C/I/D) portés par chaque lien



BRIQUE 4 — DU MODÈLE AU CHIFFRE : UN RÉSEAU BAYÉSIEN

Le problème

Un facteur bas ne suffit pas à créer une vulnérabilité. C'est une **combinaison** de facteurs qui la crée.

La réponse

- Un réseau bayésien encode ces dépendances
- Les tables de probabilités sont dérivées d'études SHS
- En sortie : un **niveau de vulnérabilité de 1 à 5** et sa probabilité



BRIQUE 5 — UNE VULNÉRABILITÉ HUMAINE SE PROPAGE

Un opérateur vulnérable contamine ceux avec qui il travaille. Trois canaux, lus directement sur l'architecture :

Canal de propagation	Origine	Condition
Délégation d'objectif	Architecture	impact > 3 et vulnérabilité > 3
Transmission de document	Architecture	impact > 2 et vulnérabilité > 2
Relation personnelle	Profils des acteurs	idem + stress non maîtrisé

LE POINT INTÉRESSANT

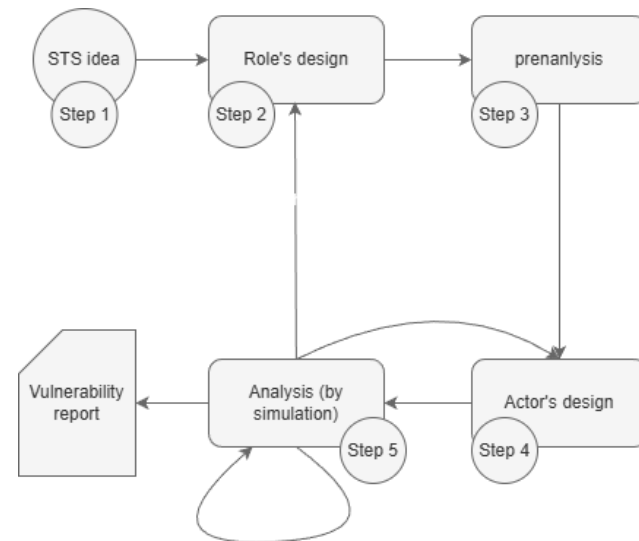
Le troisième canal **n'existe pas dans l'organigramme**. C'est le réseau informel : contagion du stress, confiance, proximité. Il double l'architecture officielle.

P. Perrotin *et al.*, « Using the architecture of Socio-Technical Systems to analyse its vulnerability », SOSE 2022.

UNE MÉTHODE OUTILLÉE, UTILISABLE PAR UN ARCHITECTE

- 1 Idée du SoSTS
- 2 **Conception des rôles** — le poste attendu
- 3 **Pré-analyse** — le rôle est-il déjà vulnérable ?
- 4 **Conception des acteurs** — qui arme le poste
- 5 **Analyse par simulation** — itération jusqu'à un domaine de couverture acceptable

En sortie : un **rapport de vulnérabilité**, pas une note individuelle.





SOMMAIRE

1. LE VERROU : UN OPÉRATEUR N'EST PAS UNE BOÎTE NOIRE

2. RENDRE L'HUMAIN VISIBLE DANS L'ARCHITECTURE

3. EST-CE QUE ÇA MARCHE ? DEUX CAS D'ÉTUDE

4. DEPUIS LA THÈSE : PASSER À L'ÉCHELLE



PROTOCOLE DE VALIDATION

- Protocole de cas d'étude formalisé (Yin) pour **maîtriser les biais**
- **2 cas d'étude, 2 scénarios** chacun
- Scénarios bâtis sur des **données réelles**, fournies par Naval Group
- **Auditions d'experts** — opérationnels et architectes

LES DEUX CAS

- **Lutte anti-piraterie maritime** — 5 rôles, 12 objectifs
- **Contrôle aérien** en aéroport régional

La question posée aux experts : « ces vulnérabilités sont-elles crédibles chez vous ? »

R. K. Yin, *Case Study Research : Design and Methods*, Sage.



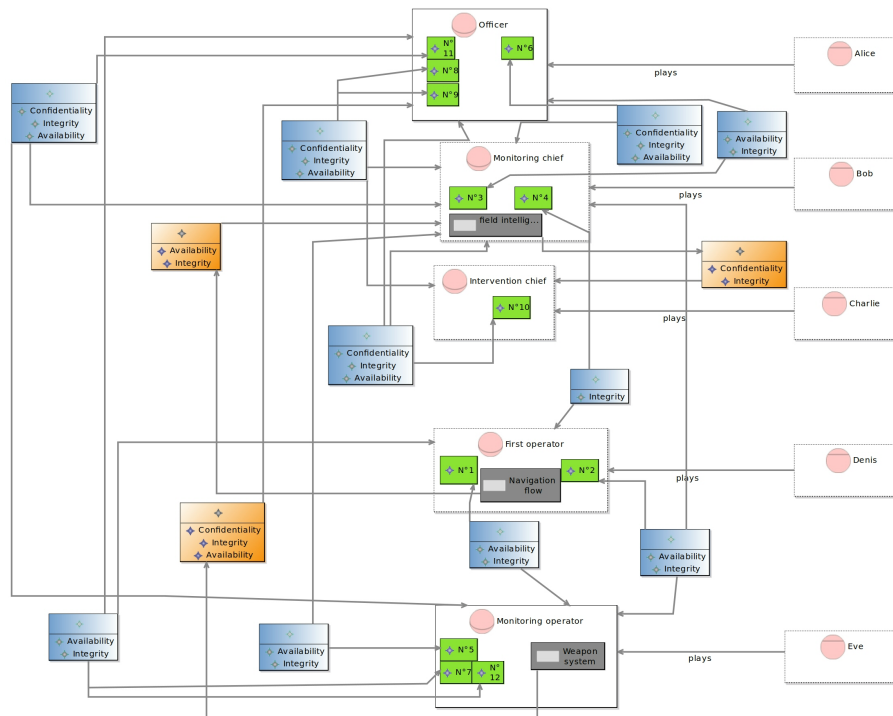
CAS 1 — LA CHAÎNE DE LUTTE ANTI-PIRATERIE

5 rôles

- Officier
- Chef de veille
- Chef d'intervention
- Premier opérateur
- Opérateur de veille

12 objectifs, du marquage d'un navire suspect jusqu'à l'ordre de tir.

Chaque lien porte son besoin de sécurité (C/I/D).





QUATRE SCÉNARIOS, QUATRE MANIÈRES D'ATTAQUER UN ÉQUIPAGE

Cas	Scénario	Résultat simulé
Anti-piraterie	Attaque cybersociale : sextorsion ciblée sur l'opérateur de veille, en moins de 24 h	Vulnérabilité niveau 3 à 60 %
Anti-piraterie	Spoofing AIS : une piste fantôme jouée toutes les heures pendant une semaine	Vulnérabilité niveau 2 à 80 %
Contrôle aérien	MITM sur la VHF	Vulnérabilité niveau 2 à 80 %
Contrôle aérien	Spoofing ADS-B : effet d'accoutumance sur le contrôleur	Vulnérabilité niveau 3 à 80 %

CE QUE MONTRENT CES CHIFFRES

On n'a pas besoin d'attaquer tout le système. **Un seul opérateur, légèrement dégradé, suffit** à empêcher le système d'atteindre son objectif dans les temps — à très faible coût.

CE QUE LES EXPERTS ONT DIT — ET CE QUE ÇA NE FAIT PAS

RÉSULTATS DES AUDITIONS

- 3 scénarios sur 4 : vulnérabilités et niveaux jugés **crédibles**
- Le 4^e : vulnérabilité **déjà connue mais non corrigée** chez l'exploitant
- Facteurs dégradés jugés **réalistes**
- Des experts ont identifié des **failles insoupçonnées** dans leur propre spécification

LIMITES ASSUMÉES

- On dit **si** une vulnérabilité existe, pas **quand** elle se déclenchera
- Les systèmes **techniques** ne sont pas encore représentés
- Renseigner les facteurs demande de **l'expertise** — à mitiger par des profils types
- Validation avec des experts **seniors** uniquement



SOMMAIRE

1. LE VERROU : UN OPÉRATEUR N'EST PAS UNE BOÎTE NOIRE

2. RENDRE L'HUMAIN VISIBLE DANS L'ARCHITECTURE

3. EST-CE QUE ÇA MARCHE ? DEUX CAS D'ÉTUDE

4. DEPUIS LA THÈSE : PASSER À L'ÉCHELLE



OÙ J'EN SUIS AUJOURD'HUI

Un article de journal en cours, avec Céline Comte (CNRS), Nicolas Belloir, Salah Sadou et David Hairion :
Analysis of Human Vulnerability in Socio-Technical Systems.

Trois apports par rapport à la thèse :

- Une **réimplémentation open source** du réseau bayésien (bibliothèque `pgmpy`)
- Un **second cas d'étude naval** complet : la lutte anti-piraterie
- Et surtout : une **méthode d'analyse systématique**, qui attaque de front la limite « il faut un expert pour renseigner les facteurs »



L'IDÉE : RENVERSER LA QUESTION

PENDANT LA THÈSE

L'architecte propose un profil. L'outil répond : « *vulnérable, niveau 3, à 60 %* ».

⇒ il faut **deviner** les profils à tester.

DEPUIS

On fixe le **poste** (rôle + contexte). On demande à l'outil : « *énumère **tous** les profils d'opérateur qui peuvent rendre ce poste vulnérable au niveau k* ».

⇒ plus rien à deviner : on **balaie tout l'espace**.

9 facteurs directs $\rightarrow 4^2 \times 5^7 = 1\,250\,000$ profils possibles par poste.



ÉTAPE 1 — DE 1 250 000 PROFILS À 436

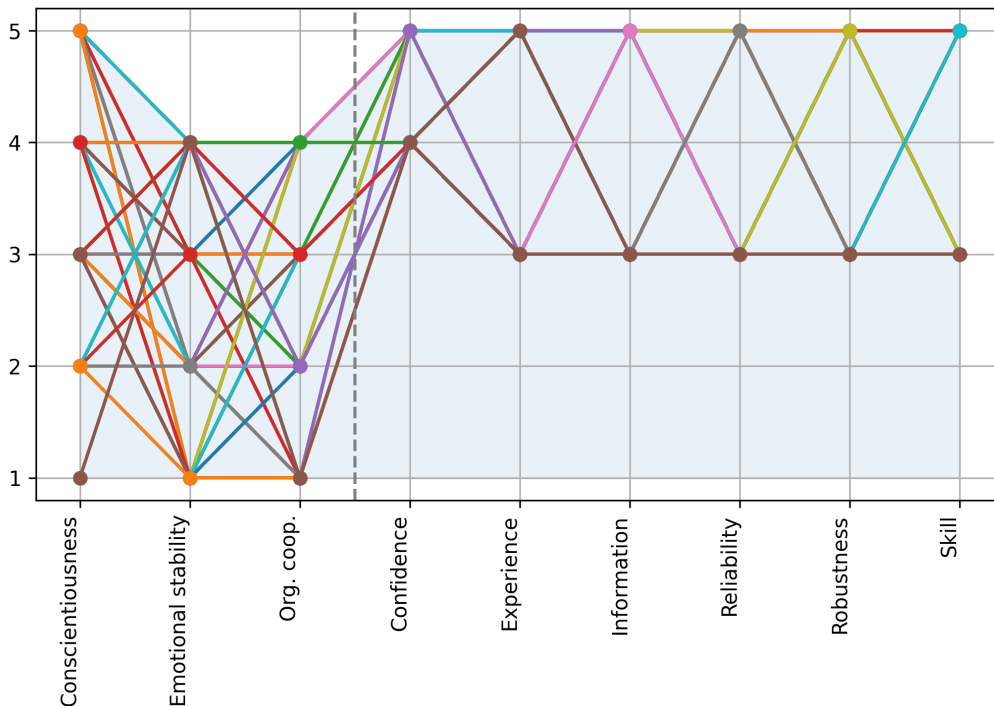
Le principe

Si un profil rend le poste vulnérable, tout profil *moins bon* le rend vulnérable aussi.

On ne garde donc que les **profils maximaux** : les meilleurs profils encore dangereux.

Rôle d'officier, vulnérabilité 5

- 1 250 000 profils balayés
- 436 profils maximaux
- 1 min 28 sur un portable standard

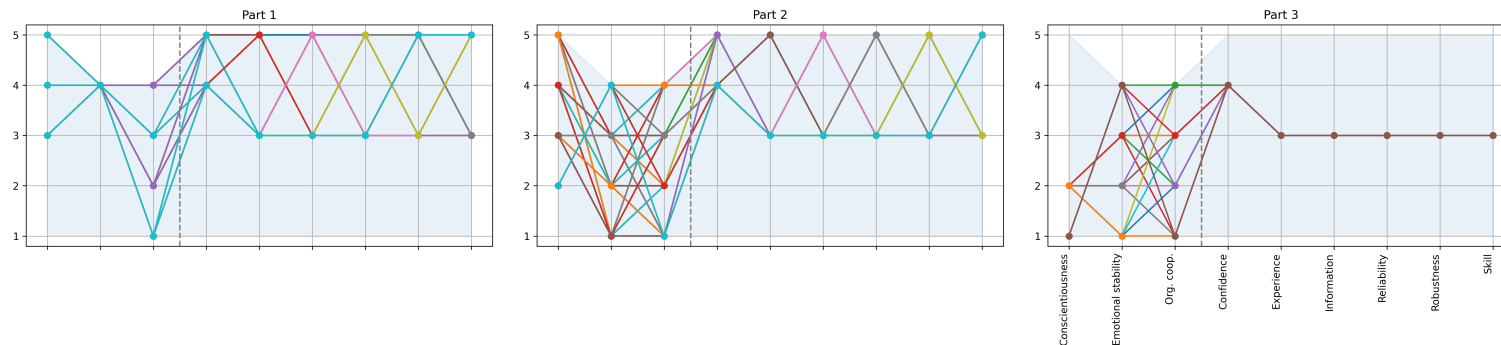


Les 436 profils maximaux menant à une vulnérabilité de niveau 5 (rôle d'officier).



ÉTAPE 2 — DE 436 PROFILS À 3 FAMILLES LISIBLES

436 profils, c'est encore illisible. On les **regroupe** en exploitant la structure du réseau bayésien → **3 familles**, de la plus à la moins dangereuse.



FAMILLE 1 — LA PLUS RISQUÉE

Opérateur *compulsif / suffisant / servile et lunatique* : vulnérabilité maximale **même avec de très bons scores** de compétence, d'expérience et de fiabilité.

FAMILLE 3 — LA MOINS RISQUÉE

Vulnérabilité maximale **uniquement si** tous les facteurs chiffrés sont simultanément très bas.



CE QUE ÇA CHANGE, ET CE QUI VIENT ENSUITE

CE QUE ÇA CHANGE

- On ne teste plus un profil : on **caractérise un poste**
- On obtient un **critère exploitable** pour armer ou former un poste sensible
- L'analyse devient **reproductible** et **outillée**, sans expert en boucle
- Code **open source**

PERSPECTIVES

- **Coupler** vulnérabilité humaine et vulnérabilité technique — et l'**émergence** née de leur combinaison
- Automatiser la **description en langue naturelle** de chaque famille
- Nouveaux types de vulnérabilités : **biais cognitifs, désinformation**
- **Acteurs pivots** : un même acteur sur plusieurs rôles

Merci de votre attention.

Questions ?

Paul Perrotin — `paul.perrotin@univ-ubs.fr`