IEC 61508 Functional safety – Préparation de l'édition 3

La cybersécurité dans l'IEC 61508

Bertrand Ricque
TC65/SC65A

Sommaire

Etat des lieux

Contexte et enjeux

Discussions en cours et perspectives

Etat des lieux

Contenu de l'édition 2

La security fait partie du périmètre de la norme :

k) requires malevolent and unauthorised actions to be considered during hazard and risk analysis. The scope of the analysis includes all relevant safety lifecycle phases;

La norme demande que l'analyse de risques s'y intéresse :

The hazards, hazardous events and hazardous situations of the EUC and the EUC control system shall be determined under all reasonably foreseeable circumstances (including fault conditions, reasonably foreseeable misuse and malevolent or unauthorised action). This shall include all relevant human factor issues, and shall give particular attention to abnormal or infrequent modes of operation of the EUC. If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out

Pourquoi faire évoluer le contenu

15 commentaires nationaux de 7 pays demandent :

- Des clarifications
- Plus d'exigences
- Des orientations vers des « solutions » (pas forcément techniques)

Un précédent problématique

IEC TR 63069

- Développé par le TC65 / WG20
- Recherche d'un « pontage » entre safety et security
- Des problèmes de ciblage
- Des limites à l'expertise des participants

C'est un recul du point de vue de l'IEC 61508

Contexte et enjeux

Que se passe-t-il dans l'industrie ? (du point de vue de la safety)

La cyber est une vieille menace nouvellement prise en compte

- Documentée dès 1980
- Structurée en 2004 (LAAS - Laprie et al.)

La structure des systèmes évolue

- Exemple : aéronef, voiture électrique

Le contenu fonctionnel des systèmes évolue

- Autonomie
- Contrôlabilité

Les référentiels de safety deviennent inopérants

Deux options majeures pour la normalisation

- Augmenter la portée des textes existants → complexité accrue des normes
- Cantonner les textes existants à ce qu'il savent faire et rédiger des textes spécifiques pour les nouveaux problèmes → complexité accrue de l'utilisation conjointe de textes et cohérence d'ensemble des textes

Impact safety

Les éléments précédents (la cyber n'en est que le plus simple et le plus visible) ont un impact direct sur l'évaluation des risques

Tout impact sur l'évaluation des risques a un impact potentiel sur les contraintes (safety) pesant sur les systèmes, en termes de :

- Solution technique
- Coût de l'ingénierie
- Conformité aux normes existantes

Cet impact est variable en fonction des pratiques des secteurs

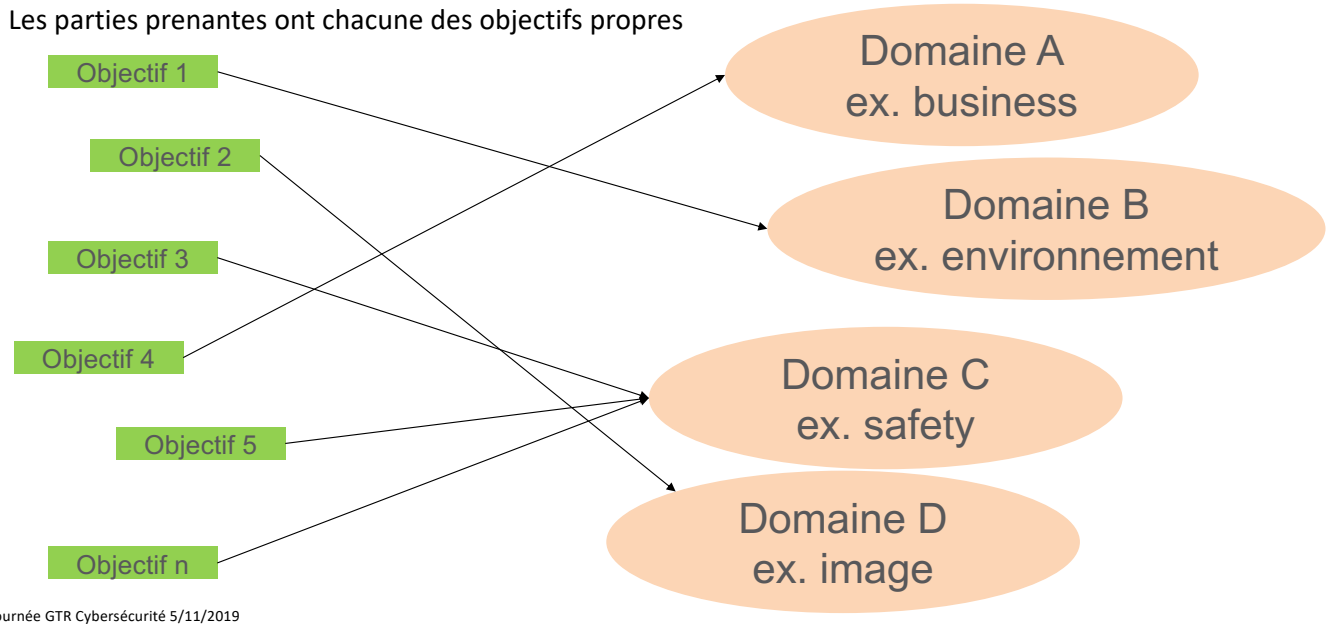
L'absence de référentiel global d'ingénierie dans beaucoup de secteurs complique la donne :

- Pas de cadre de consolidation du problème
- Question des Acceptables Means of Compliance

« Relation » safety – security (1)

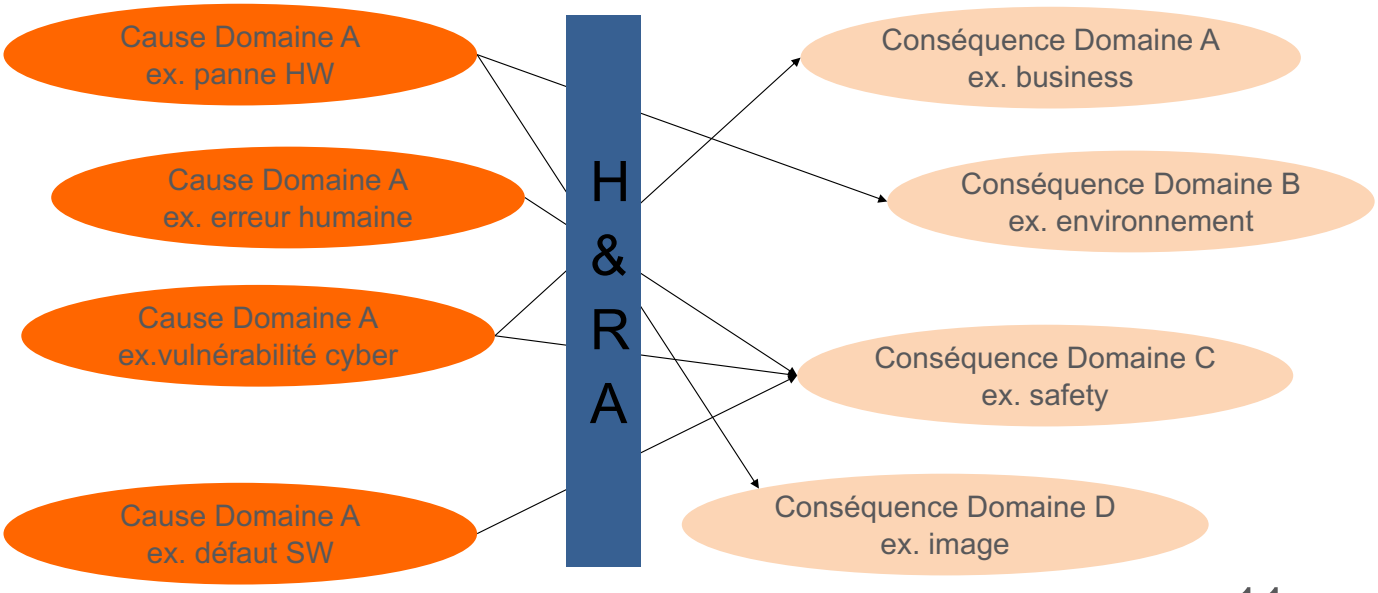
Tout est concentré dans l'analyse des risques et dans ses conséquences

Les parties prenantes ont chacune des objectifs propres



« Relation » safety – security (2)

Nature de l'analyse des risques



« Relation » safety – security (3)

Les vulnérabilités cyber sont toujours du côté des causes

La safety est du côté des conséquences

Du point de vue de la safety :

- La cyber n'est qu'un domaine de causes
  - Pas nouveau
  - Mais pris en compte récemment
- Ces causes ont la capacité :
  - De générer de nouvelles conséquences (sur un scénario existant)
  - De modifier la gravité d'une conséquence existante
  - De modifier la fréquence des conséquences existantes

Discussions en cours et perspectives

Travaux du MT61508-1/2 - JTG06

Deux positions s'affrontent

- La séparation totale (d'un point de vue normatif) des deux domaines
  - Portée par une partie du comité national allemand et par les Pays Bas
  - La safety doit partir du principe que la security est assurée et qu'il n'y a pas de menaces cyber concernant la safety
  - Pas de security dans les analyses de risque safety
- La prise en compte de la security par la safety dans la limite des vulnérabilités impactant les conséquences safety
  - Portée par la France et le Royaume Uni, soutenu par les USA et une partie du Japon
  - L'analyse de risque doit identifier les vulnérabilités et documenter les scénarios
  - Les référentiels de safety doivent identifier les exigences applicables en fonction du contexte

Contenu de la position française

Obligation de prendre en compte les vulnérabilités cyber dans les clauses 7.3 and 7.4 dans la limite du périmètre défini par les parties prenantes :

- "le type de menaces de sécurité devant être prise en compte (par exemple perte de confidentialité, d'intégrité, de disponibilité, erreur humaine pouvant mener à des événement dangereux) doit être spécifié de la même manière que les autres causes doivent déjà être spécifiées (7.3.2.5 et périmètre de l'analyse de risques)."
- Dans l'objectif de documenter les scénarios menant aux événements dangereux.

Cette position rejette l'exclusion par la norme des menaces cyber du champ de l'analyse des risques car :

1. cela mène à une sous-estimation du risque et à l'identification de scénarios erronés,
2. cela empêche de savoir si des menaces cyber affectent ou pas la safety,
3. Cela rend impossible l'atteinte des objectifs de la clause 7.4.

Clarification des exigences de l'IEC 61508 applicable à des artefacts cyber **uniquement** quand la security est partie prenante de la démonstration de safety avec 3 approches graduées :

- Les contremesures de cybersécurité sont embarquées des les fonctions de sécurité – Toutes les exigences de l'IEC 61508 s'appliquent.
- Il n'y a pas d'indépendance fonctionnelle entre des éléments spécialisés cyber et les éléments de safety – les éléments technologiques ne s'appliquent pas. Les aspects technologiques des éléments cyber sont conformes aux normes cyber.
- La démonstration de safety repose sur le bon fonctionnement des contre-mesures cyber – seules les exigences du cycle de vie s'appliquent.

Conclusion

Une situation conflictuelle qui reflète :

- Le manque de maturité académique du domaine de la cybersécurité
- La baisse de l'investissement financier et académique dans la safety depuis la fin des années 90 (fin du programme électronucléaire pour la France)
- La véritable difficulté de l'industrie à accepter une augmentation de ses coûts comme contrepartie d'une augmentation de la complexité de ses applications

Des besoins accrus de modélisation des systèmes à un niveau plus élevé que dans le passé

En fonction des secteurs industriels, des lacunes dans l'Ingénierie Système

Un défi pour l'avenir en terme de sécurité des personnes