Une approche de l'analyse des risques des systèmes de contrôle industriels combinant sûreté et sécurité : le cyber Noeud-Papillon

François Masse, Houssein Abdo, Jean-Marie Flaus

Une approche de l'analyse des risques des systèmes de contrôle industriels combinant sûreté et sécurité : le cyber Nœud-Papillon

Contributeur
François MASSE
/
Collaborateurs
Houssein ABDO
et
Jean-Marie FLAUS
(laboratoire G-SCOP, Institut national polytechnique de Grenoble)

La numérisation croissante des systèmes de contrôle, notamment dans l'industrie chimique, crée de nouvelles vulnérabilités qui peuvent être exploitées par des attaquants pour provoquer des phénomènes dangereux pour les personnes ou l'environnement. La prise en compte de ces menaces dans l'analyse des risques est donc un élément important d'une évaluation globale des risques. Cependant, la plupart du temps, la sûreté et la sécurité sont évaluées séparément et les conséquences physiques des cyberattaques sont peu étudiées. Une méthode d'analyse intégrant la cybersécurité dans l'évaluation des scénarios d'accidents industriels a donc été proposée. Au cours de la phase d'analyse détaillée des risques, cette approche combine le modèle de nœud papillon (NP), couramment utilisée pour l'analyse des risques des installations classées, et l'analyse par arbre d'attaque (AT), récemment introduite pour l'analyse de sécurité des systèmes de contrôle informatique. L'utilisation combinée de nœuds papillon et d'arbres d'attaque permet d'effectuer une étude qualitative exhaustive des scénarios de cybersécurité et des scénarios accidentels, ainsi qu'une évaluation de la probabilité de réalisation de ces scénarios.

Formalisme du modèle

L'analyse détaillée des risques fait suite à une première phase d'analyse préliminaire des risques au cours de laquelle les principaux scénarios d'accidents sont identifiés. Lors de l'analyse détaillée des risques, on cherche à décrire ces scénarios de manière complète et à les quantifier en probabilité et gravité. Pour cela, on utilise le plus souvent le formalisme des diagrammes de nœuds papillon. L'approche proposée vise à compléter l'analyse détaillée des risques en y intégrant les évènements initiateurs de scénarios et les défaillances de mesures de maîtrise des risques susceptibles d'être provoqués par une cyberattaque.

Pour intégrer les cyberattaques aux nœuds papillon, nous proposons une méthode, dite ATBT *(Attack Tree Bow Tie)* **(Figure 1)**, combinant les nœuds papillon et des arbres d'attaques permettant d'identifier des causes malveillantes aux scénarios décrits dans les analyses de risques accidentels. Un modèle de nœud papillon décrit le scénario accidentel puis, pour chaque évènement élémentaire de ce modèle lié à une défaillance d'un élément du système de contrôle industriel (dérive de capteur, fermeture de vanne…), un arbre d'attaque est développé. Celui-ci représente les différentes séquences d'actions que réaliserait un attaquant (ou agresseur) pour parvenir au déclenchement de l'évènement analysé. Cette représentation permet de lier les risques relatifs à la sécurité (malveillance) et les risques relatifs à la sûreté (accidentels).

Les évènements accidentels sont décrits par :

- S_e, le scénario représentant l'évènement indésirable e, ses causes et ses conséquences de nature aléatoire (défaillances d'équipements, agressions de l'environnement, erreurs opératoires…) ;
- P_e, la probabilité d'occurrence de S_e ;
- X_s, la gravité des conséquences de S_e.

L'ensemble de ces scénarios est intégré dans des nœuds papillon dans le cadre de l'analyse des risques physiques.

Les arbres d'attaques représentent les différentes vulnérabilités potentiellement exploitées par un attaquant/agresseur pour produire l'effet recherché sur le système physique (c'est-à-dire les différents systèmes informatiques à corrompre pour manœuvrer une vanne par exemple). Il n'apparaît pas pertinent de caractériser les attaques par une probabilité d'occurrence, les risques liés à la sécurité sont donc décrits par :

- tv représentant une menace ou attaque t (threat) exploitant une vulnérabilité v (description du scénario d'attaque) ;
- P_{tv} la vraisemblance que la menace t exploite la vulnérabilité v, estimée à partir de la complexité de réalisation de l'attaque ;
- X_{tv}, la gravité des conséquences si t exploite la vulnérabilité v.

Les arbres d'attaques sont ensuite connectés aux nœuds papillon pour les évènements initiateurs, les évènements intermédiaires ou les barrières pouvant être causés par une action malveillante.

Exploitation du modèle

L'exploitation du modèle ATBT consiste à identifier les combinaisons d'évènements aléatoires et d'actions malveillantes menant à un évènement indésirable, et à évaluer le risque global selon les paramètres suivants :

- $S_{(tv,e)}$, la description du scénario pouvant résulter d'une combinaison d'incidents et d'actes malveillants ;
- $P_{(se,sa)}$ qui est la vraisemblance de l'occurrence du scénario $S_{(tv,e)}$ avec *se*, la vraisemblance liée à la réalisation des actes malveillants, et *sa*, la probabilité d'occurrence des évènements aléatoires (défaillances, agressions de l'environnement...) ;
- $X_{(tv,e)}$, la gravité des conséquences de $S_{(tv,e)}$.

La possibilité d'occurrence des différents scénarios est donc cotée selon un vecteur à deux dimensions : la probabilité (accidents) et la vraisemblance (réalisation d'une attaque). Chaque scénario est évalué indépendamment, trois types de scénarios sont possibles :

- des scénarios purement incidentels caractérisés uniquement par une probabilité ;
- des scénarios purement malveillants caractérisés par une vraisemblance ;
- des scénarios dus à l'occurrence simultanée d'attaques et d'évènements incidentels caractérisés par une probabilité et une vraisemblance : la vraisemblance caractérise l'attaque du système de commande et la probabilité caractérise l'occurrence de conséquences pour les personnes sachant que l'attaque a été réalisée.

Cette approche met en évidence les séquences malveillantes et permet donc d'identifier soit les systèmes de contrôle à sécuriser pour diminuer la vraisemblance soit les barrières de sécurité d'autres technologies, non vulnérables aux cyberattaques (exemple, soupape), permettant de réduire la probabilité de réussite de l'attaque.

Conclusion

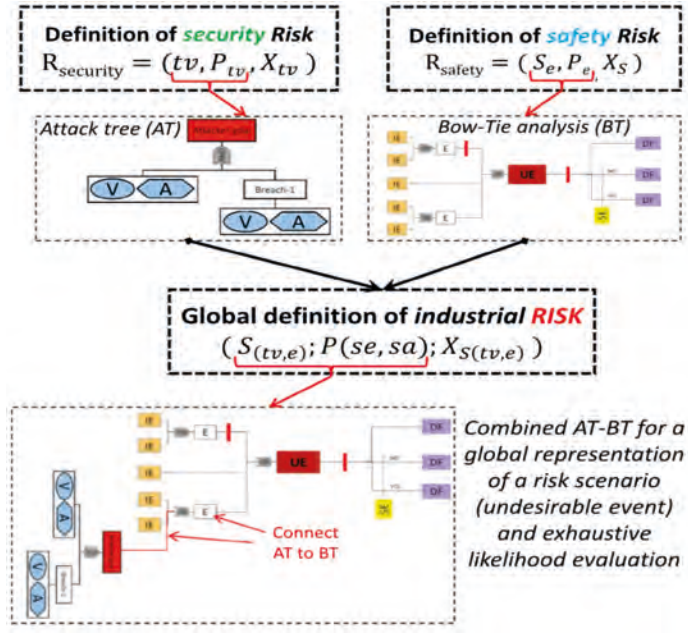
L'approche proposée vise à intégrer les causes malveillantes à l'analyse des scénarios étudiés lors de l'analyse des risques accidentels. Les travaux actuels de l'Ineris portent sur l'évaluation de nouveaux scénarios ou phénomènes dangereux propres aux cyberattaques et qui ne sont donc pas encore pris en compte dans l'analyse des risques accidentels.

ABSTRACT /

The increasing importance of digital technology in chemical process industry creates new vulnerabilities that can be exploited to provoke dangerous phenomenon fore people or environment. However, nowadays, safety and security are assessed separately and possible physical consequences of cyberattacks are not evaluated It is therefore necessary to integrate the consideration of cybersecurity in the global analysis of risks to human health and the environment. In this paper, a new method is proposed by considering safety and security for a probability evaluation during industrial risk analysis. This approach combines Bow-Tie Analysis (BT), commonly used for safety analysis and the Attack Tree Analysis (AT), recently introduced for security analysis of computer control systems.

The combined use of BT and AT provides an exhaustive qualitative investigation of security and safety scenarios, and a qualitative evaluation of the likelihood of these scenarios. The definition of ATBT combined model is presented.

Figure 1 / Présentation générale du modèle ATBT [1].



Référence

[1] Abdo H. ; Kaouk M. ; Flaus J.-M. ; Masse F.
A safety / security risk analysis approach of Industrial Control Systems :
A cyber bowtie - combining new version of attack tree with bowtie analysis.
Computers & Security, 2017, 72: p. 175-195