Cyber Security Risk Assessment Process for Military Systems

(STO-TR-IST-151)

Executive Summary

Military platforms are more computerized, networked and processor-driven than ever. The consequence is an increased exposure to cyber attacks and thus, an amplified risk. However, the continuous and stable operation of these platforms is critical to the success of military missions and public safety.

Perfect cyber security does not exist. Cyber security must be continuously managed through iterative risk assessments. Many cyber security risk management frameworks and processes exist for traditional IT systems. However, this is far from being the case when it comes to military platforms and systems. This document presents a cyber security risk assessment process tailored to military systems. This process was developed by the team members of the NATO IST-151 Research Task Group (RTG) activity entitled "Cyber Security of Military Systems". The process can be applied to both traditional IT and firmware-based embedded systems, which are everywhere in military platforms and systems.

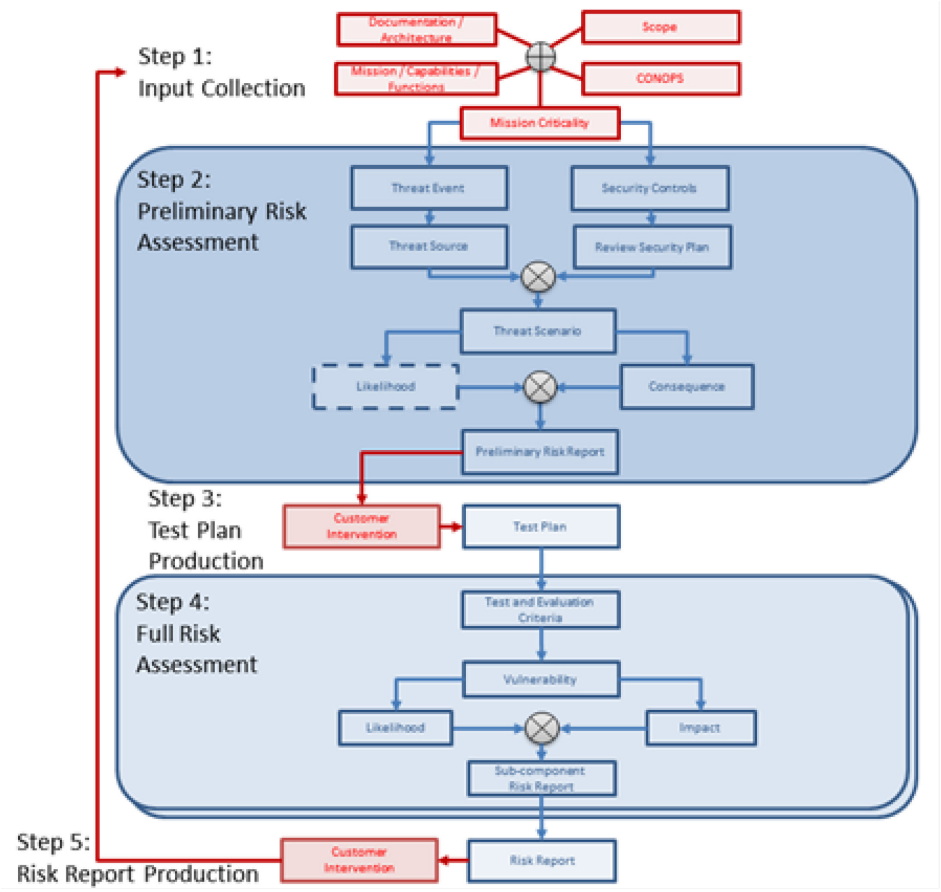

Figure i: The Five Main Steps of the Assessment Process.

Processus d'évaluation des risques de cybersécurité pour les systèmes militaires

(STO-TR-IST-151)

Synthèse

Jamais les plateformes militaires n'ont été plus informatisées, mises en réseau et alimentées par des processeurs. Il en résulte une exposition accrue aux cyberattaques, et ainsi, une amplification du risque. Or la continuité et la stabilité de fonctionnement de ces plateformes revêtent une importance critique pour le succès des missions militaires et pour la sécurité publique.

La cybersécurité n'est jamais parfaite : elle doit être gérée en permanence au moyen d'évaluations itératives du risque. Nombreux sont les cadres et processus de gestion des risques de cybersécurité régissant les systèmes TI traditionnels. Tel n'est pas le cas, en revanche, pour les plateformes et systèmes militaires. Ce document présente justement un processus d'évaluation des risques de cybersécurité adapté aux systèmes militaires. Le processus concerné a été élaboré par les membres de l'équipe de l'activité « Cybersécurité des systèmes militaires » du Groupe de recherche (RTG) IST-151 de l'OTAN. Il s'applique à la fois aux systèmes intégrés TI traditionnels et à ceux équipés d'un micrologiciel, qui sont omniprésents dans les plateformes et systèmes militaires.