MODélisation de SECurité pour l'AERONautique

Guillaume Mockly (Trialog), Gabriel Pedroza (CEA-LIST)
guillaume.mockly@trialog.com gabriel.pedroza@cea.fr

Méthodologie

Le processus MODSECAERO

1 ***Système et périmètre de sécurité***
- Paramétrage pour l'analyse (critères de sécurité, échelles)
- Vues fonctionnelle, composants (biens), sous-composants, ports et connecteurs
- Technologie du composant
- Mesures de protection existantes
- Définition du périmètre d'analyse

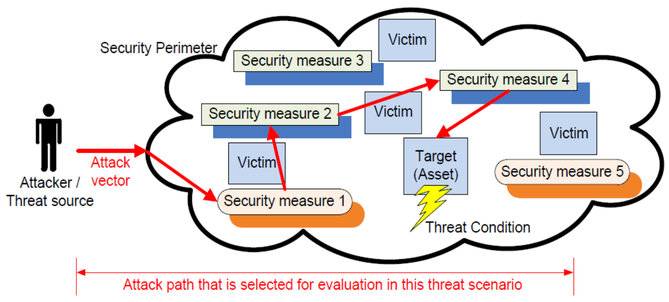
2 ***Instanciation des bases de connaissance***
- Vulnérabilités des composants à appliquer selon leur technologie
- Patterns d'attaques à appliquer selon les vulnérabilités et la technologie des composants
- Support pour la sélection des vulnérabilités et patterns d'attaque à appliquer

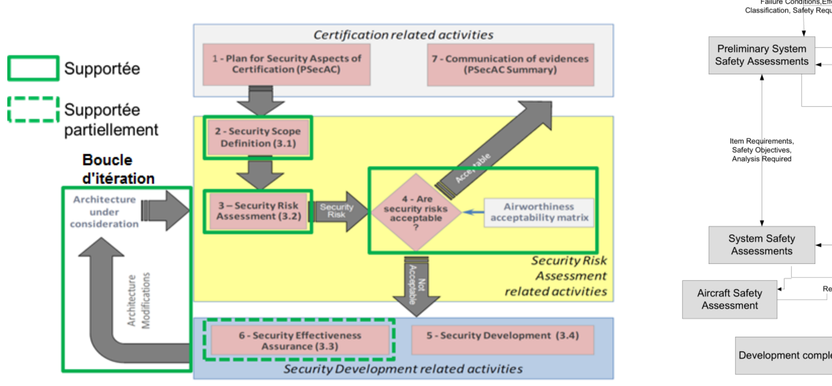
3 ***Scénarios d'attaque***
- Identification des composants critiques cible d'attaques «Threat Conditions»
- Spécification de profil d'attaquant (coût, ressources, connaissances, etc.)
- Application de patterns d'attaques sur un périmètre de sécurité
- Support pour la propagation d'attaques

4 ***Evaluation et traitement des risques***
- Cotation de probabilité/difficulté chemins d'attaque
- Vues propagations d'attaques et défaillances
- Cotation des risques et acceptabilité
- Traitement / réduction des risques par mesures de protection

Contexte normatif

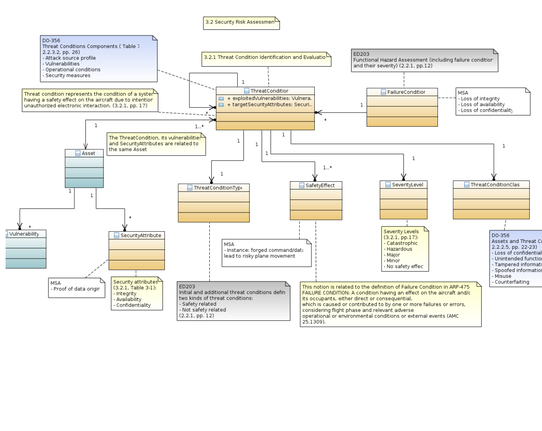
Les normes ED-202A et ED-203
- Spécifient une terminologie commune pour l'analyse des système aéronautiques.
- Décrivent les interactions avec les analyses de sûreté
- Décrivent un processus permettant la certification du système.

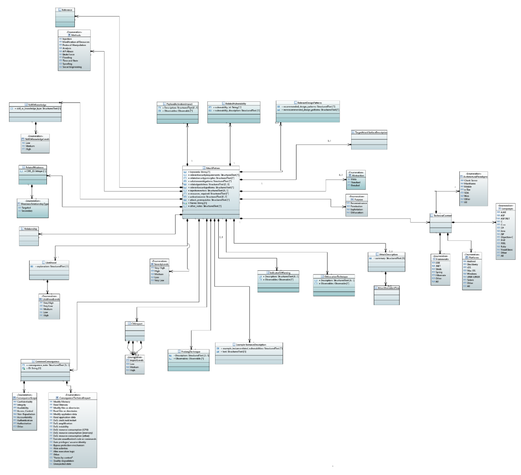




Métamodèle pour l'analyse de risque

La méthodologie de ModSecAero s'appuie sur:
- Un métamodèle traduisant les concept des normes
- Un second métamodèle décrivant les bases de connaissances de faiblesses et de patrons d'attaque

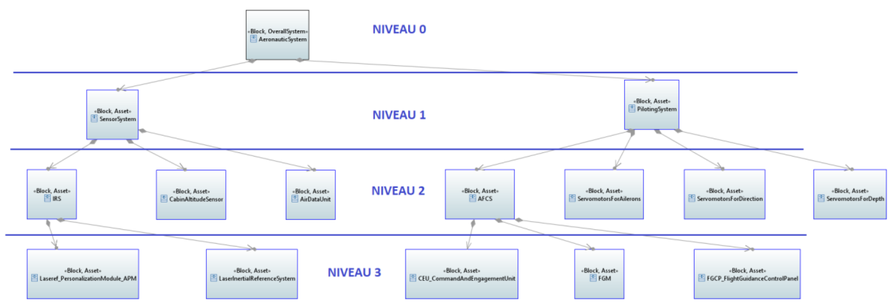


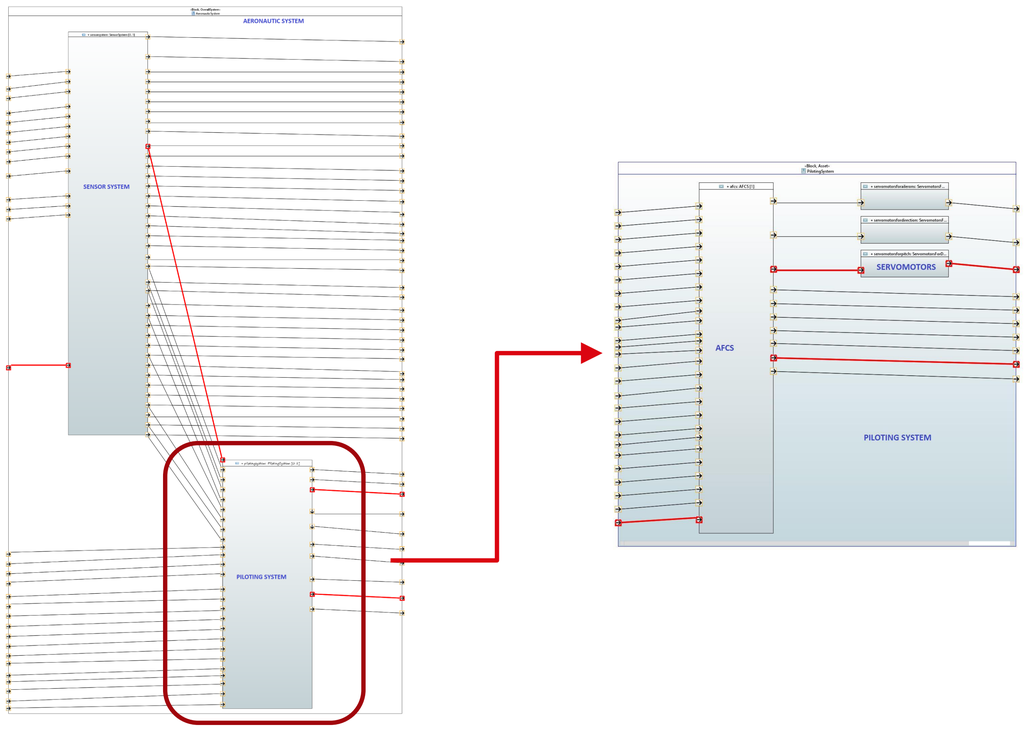


Cas d'étude: attaque d'un système de contrôle de vol

Modélisation du système

Le système considéré est un système de contrôle de vol automatique qui comprend:
- Une centrale inertielle qui calcule les paramètres de vol
- Un automate qui agit sur les surfaces de contrôle pour corriger la trajectoire





Scénario d'attaque

Objectif: Obtenir une modification de la trajectoire de l'appareil.
Vecteur d'attaque considéré: Modification des données issues des capteurs.
Les élément des bases de connaissances ci-dessous sont utilisés

Attribute	Value
Pattern ID	624
Name	Fault Injection
Description summary	The adversary uses disruptive signals or events (e.g. electromagnetic pulses, laser pulses, clock glitches, etc.) to cause faulty behavior in electronic devices.
Attacker prerequisites	Physical access to the system:: The adversary must be cognizant of where fault injection vulnerabilities exist in the system in order to leverage them for exploitation.
Resources required	The relevant sensors and tools to detect and analyze fault/side-channel data from a system. A tool capable of injecting fault/side-channel data into a system or application.
Criticality	Typical severity: high. Typical likelihood: low.
Solutions and mitigations	Implement robust physical security countermeasures and monitoring.

Attribute	Value
Weakness ID	790
Name	Improper Filtering of Special Elements.
Description	The software receives data from an upstream component, but does not filter or incorrectly filters special elements before sending it to a downstream component.
Modes of introduction	:::PHASE:Implementation:DESCRIPTION:::
Common consequences	::SCOPE:Integrity:TECHNICAL IMPACT:Unexpected State::

Arbre d'attaque

Généré à partir de:
- Description du système
- Eléments du scénario

Cet arbre présente l'attaque à différent niveaux de raffinements