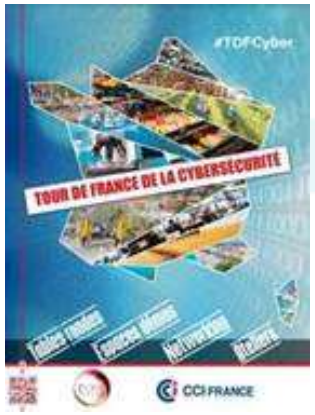
CONSTRUISONS ENSEMBLE
LA DÉFENSE DE DEMAIN

SECURITY BY DESIGN ET NAVIRES

Démarche cyber DGA

CyberCercle

05 avril 2018



DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES

LA CYBER DANS LES OPÉRATIONS D'ARMEMENT

OPÉRATIONS D'ARMEMENT

Déroulement d'une opération d'armement

Etudes amonts

Orientation → Elaboration → Réalisation → Utilisation

- Innovations, dérisquage sur des briques technologiques
- Analyse et évaluation de plusieurs solutions
- Spécification technique, contractualisation
- Réalisation industrielle
- Mise en service opérationnelle

Une perception partagée du besoin et de la solution technique à apporter

RÔLE DE LA DGA EN CYBERDEFENSE

Sécuriser les systèmes fournis aux forces

Fournir aux forces des produits/outils de cyberdéfense

Etre l'expert référent du ministère

Soutenir les opérationnels

DGA

MINISTÈRE DES ARMÉES

ANALYSE DE LA MENACE CYBER

- **Connaître la menace** pour mieux **protéger nos systèmes**

- **Analyse des systèmes**
  - Aspects fonctionnels / métiers
  - Aspects techniques

- **Démonstrateurs**
  - Mise en œuvre de **plateformes**
  - Analyses de **vulnérabilités**
  - Réalisation de **preuves de concept**

➔ Elaboration de spécifications de **sécurisation :**
Protection & détection

APPLICATION DE LA DÉMARCHE AU DOMAINE NAVAL

ETUDES AMONT MALDIVES

Menaces AnaLyses et Détection d'Intrusion sur les naVirES

Etude et proposition de mise en œuvre de capacités
de Lutte Informatique Défensive
à bord des navires.

2 Axes

- Analyse de la menace
- Stratégie défensive

3 Phases

- Etudes
- Démonstrateur
- Propositions

NAVAL GROUP

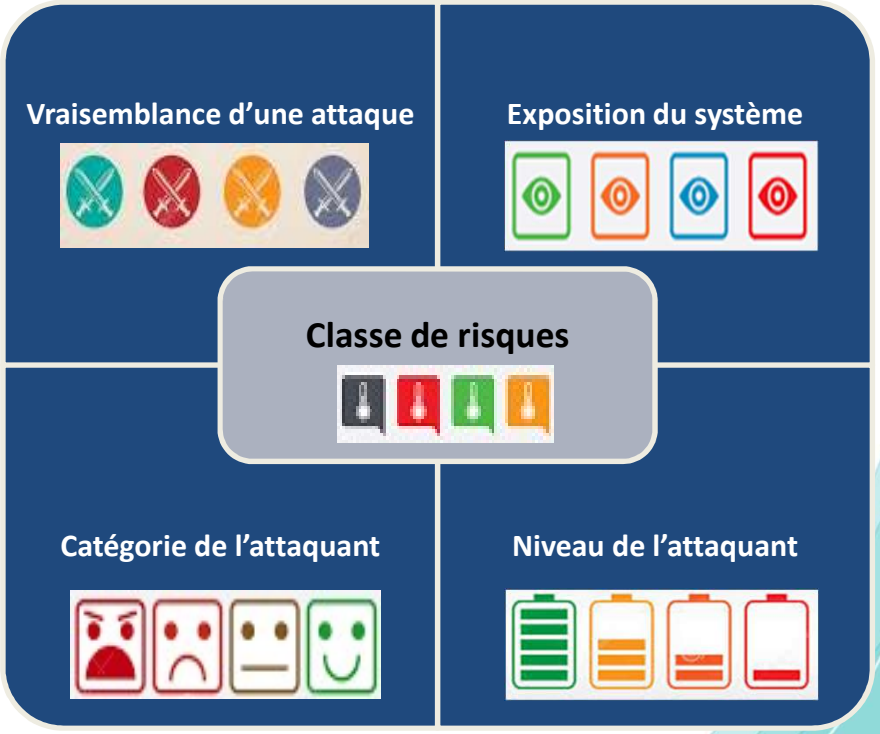
THALES

DGA

MINISTÈRE DES ARMÉES

FONCTIONS DU NAVIRE

- Identification des fonctions du navire
- Définition des classes de risques cyber
- Association des classes de risques aux fonctions du navire



SOUS-SYSTÈMES NAVIRE

Système de communication

AIS

VDR

Radar

ECDIS

Système de navigation

GPS

Système bureautique

Infrastructure réseau

Système Plateforme

Système de combat

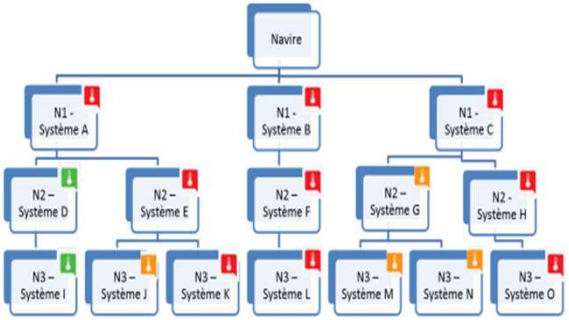
Automates et systèmes industriels

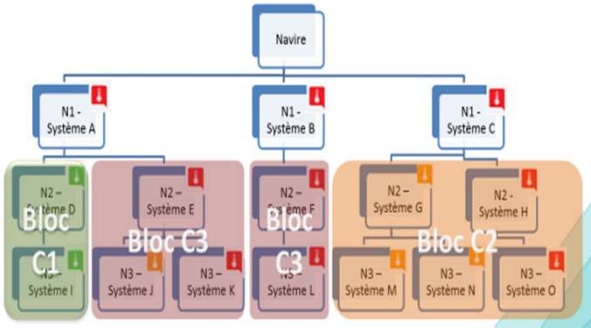
CLASSES DE RISQUES CYBER

Etape 1
Etablir le niveau de criticité des systèmes porteurs des fonctions du navire

Etape 2
Construire la matrice des échanges entre systèmes et Identifier les systèmes en interfaces

Etape 3
Identifier des blocs de systèmes et allouer à chaque bloc une classe de cyber-sécurité

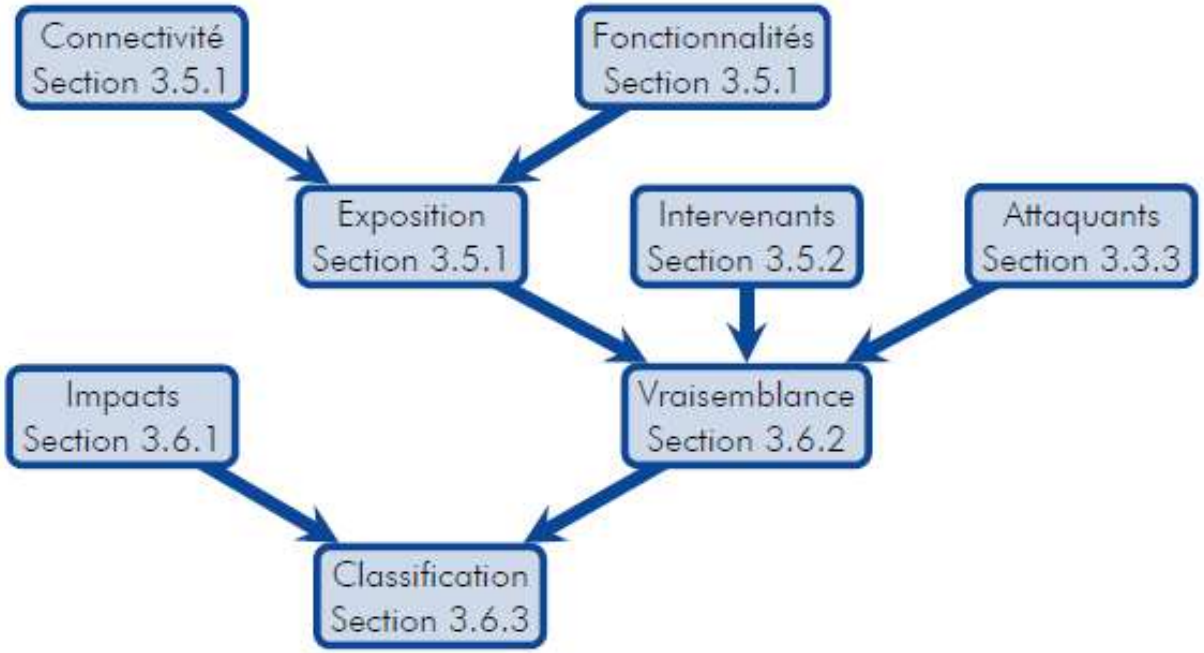




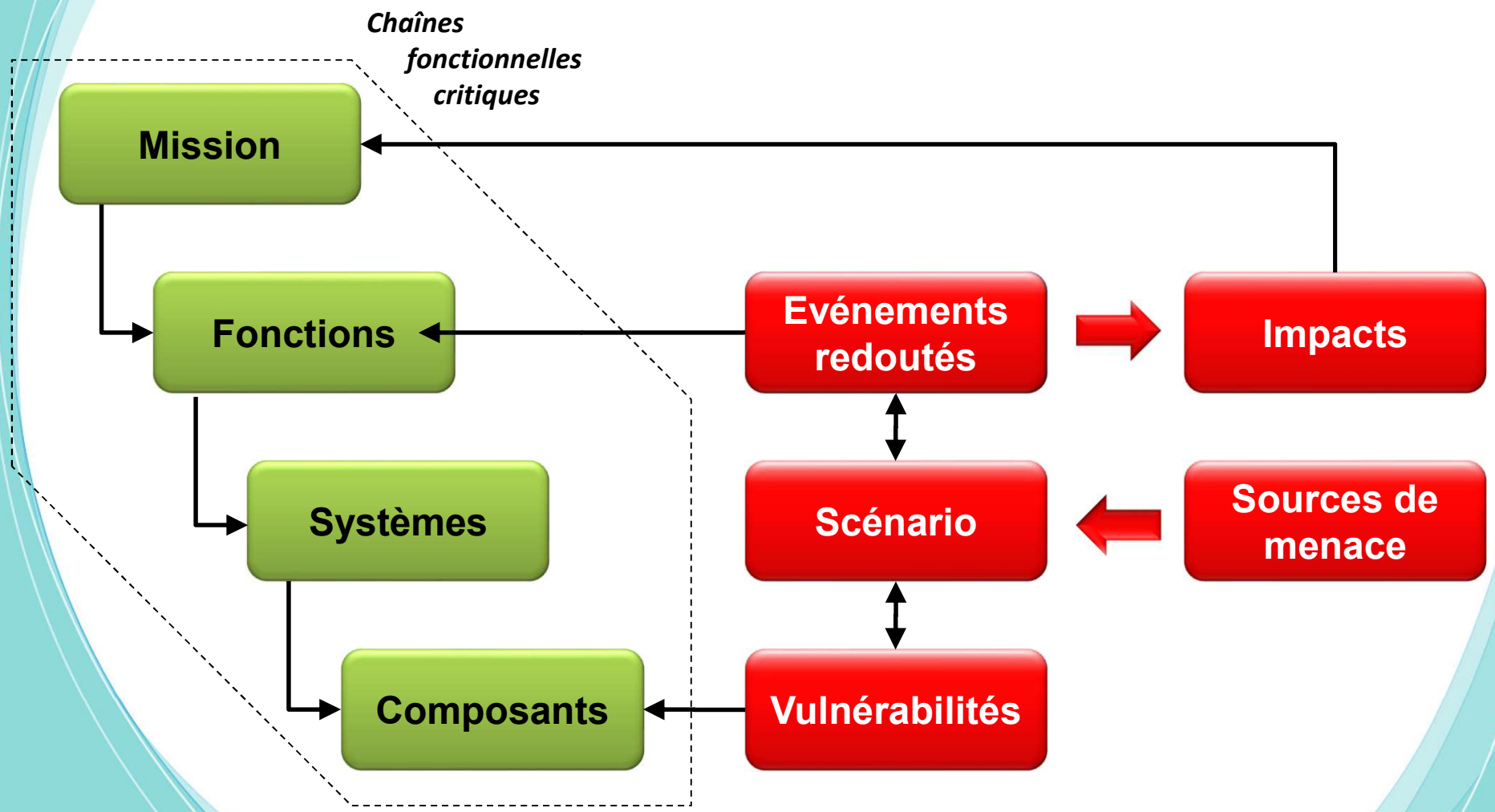
MÉTHODE DE CLASSIFICATION

Mise en place par l'ANSSI

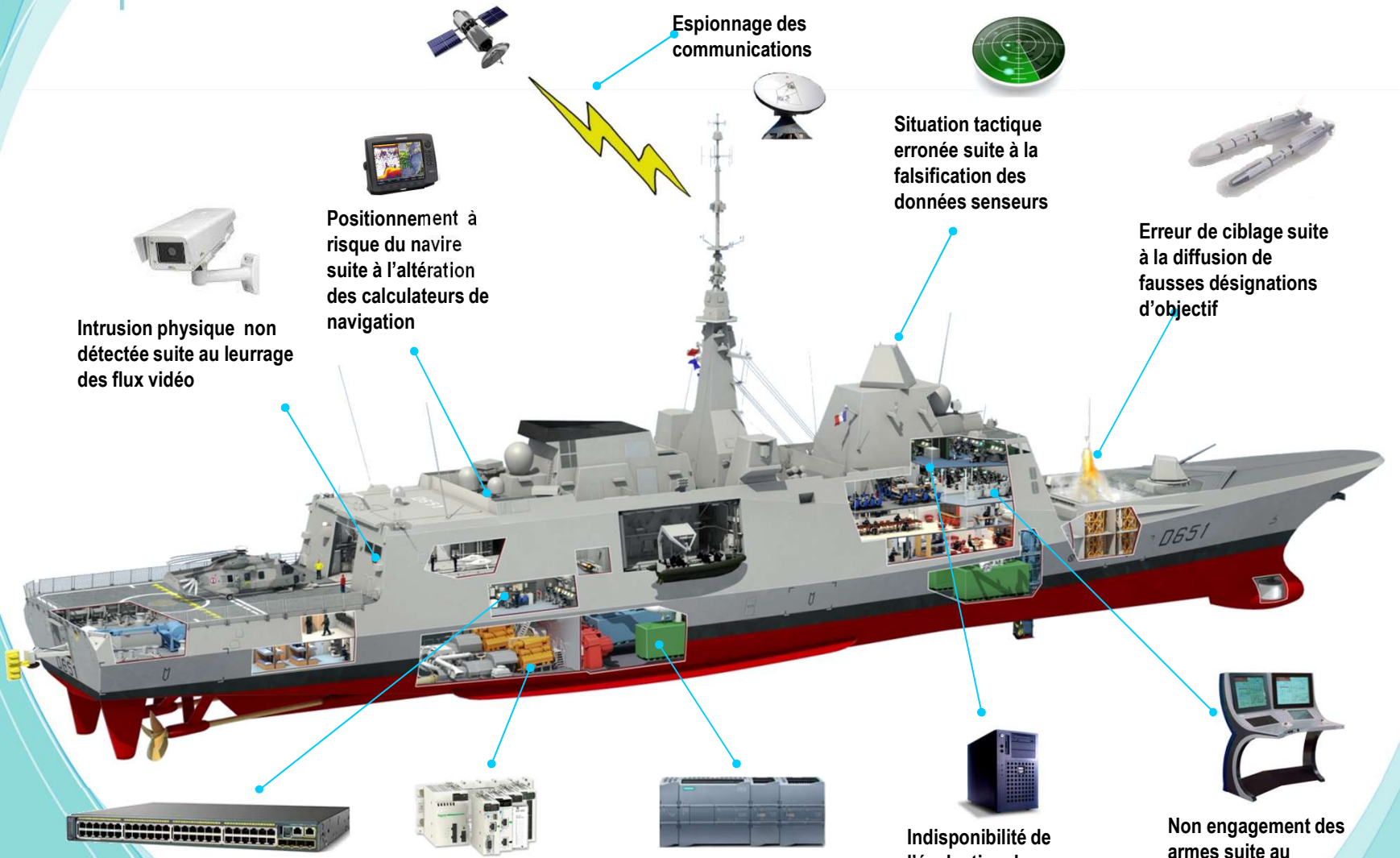
- **Classe 1 : risque et impact faible**
- **Classe 2 : risque et impact significatif**
- **Classe 3 : risque et impact critique**



ANALYSE DE LA MENACE CYBER



EVÉNEMENTS REDOUTÉS



Dégradation des communications internes suite à une saturation réseau

Manœuvre incontrôlée du navire suite au piégeage des logiciels automates

"Blackout" énergie suite à la diffusion de commandes malveillantes

Indisponibilité de l'évaluation des menaces suite à une intrusion des calculateurs tactiques

Non engagement des armes suite au dysfonctionnement des consoles (bombes logiques)

160 évènements redoutés identifiés et analysés

ELABORATION DE SCÉNARIOS

6 types de bâtiments étudiés	BPC, Frégates Multi-missions, Frégates de Défense Aérienne, Porte Avion, SNLE, SNA
5 sous systèmes étudiés	Communications, Réseaux, Navigation, Plateforme, Système de combat
160 événements redoutés analysés	Hiérarchisation en par rapport aux chaînes fonctionnelles critiques
47 scénarios d'attaque étudiés	Scénarios d'attaques caractérisés
10 scénarios d'attaque détaillés	Description détaillée des étapes des scénarios d'attaque
5 scénarios d'attaque implémentés	Implémentation sur le démonstrateur
2 scénarios d'attaque en démo	Restitution aux autorités / sensibilisation / communication

DÉMONSTRATEUR REPRÉSENTATIF

Démonstrateur navire

Scénarios

Système de Combat

Système de navigation

Système Réseau

Système de communications

Système de plate-forme

Preuves de concept

MISE EN PLACE DE SOLUTIONS DE DÉTECTION

Analyse de la Menace

Analyse fonctionnelle Navire Armé

Analyse technique Navire Armé

Evènements redoutés

Analyse de la menace

Stratégie Défensive

Architecture de détection

Impacts opérationnels

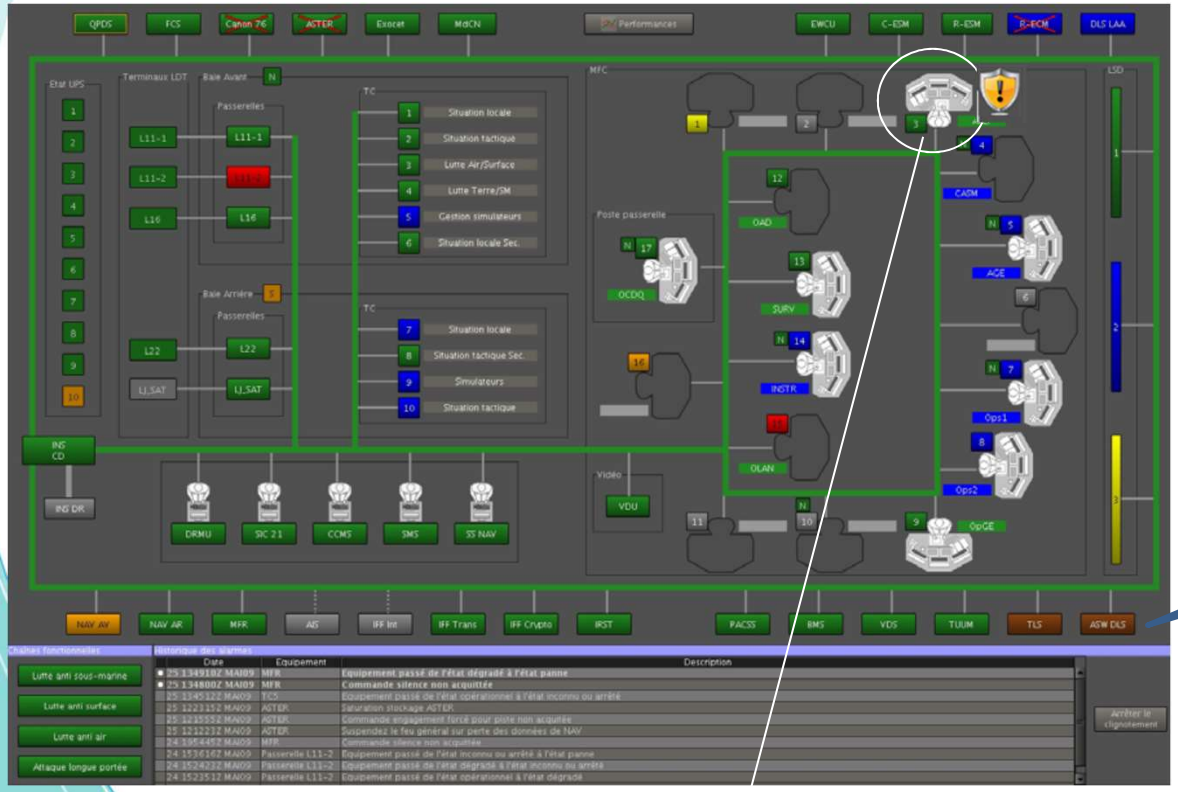
Solution de détection

Besoins de détection

Scénario d'attaque

INDICATEURS « CYBER »

Interfaces opérationnelles, travaux sur l'ergonomie



Système de combat

Indicateur Lutte Informatique Défensive

PRINCIPAUX RÉSULTATS

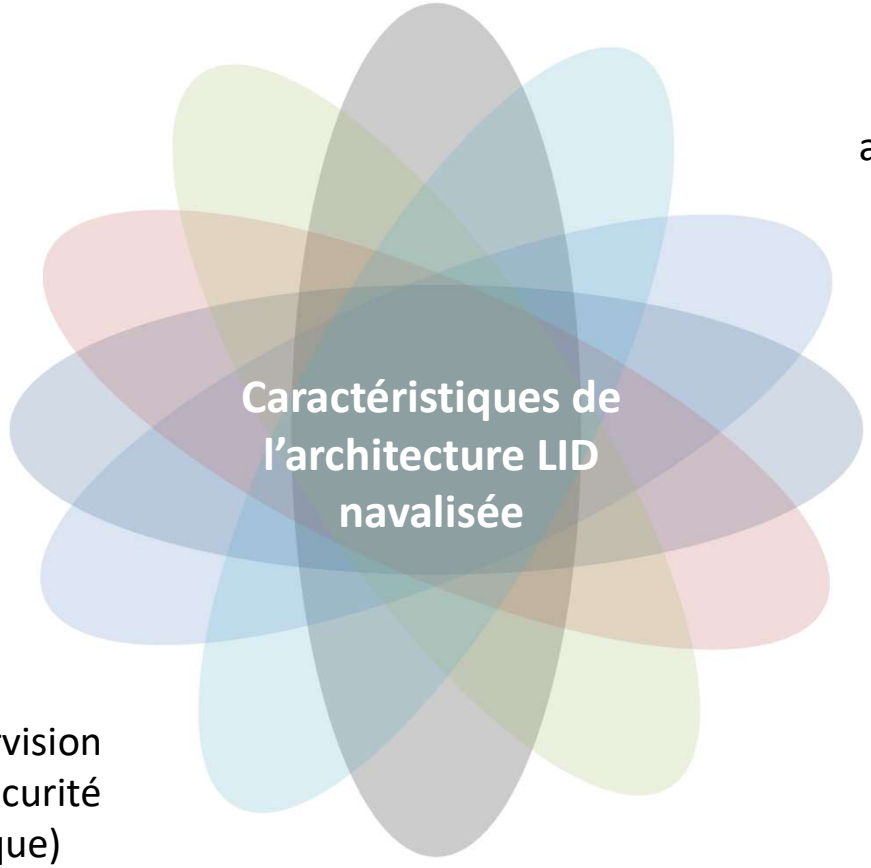
Présence de capteurs

Prise en compte des multiples réseaux bord

Autonomie à bord

Visualisation sous forme d'alertes (similaire aux autres domaines de lutte)

Surveillance globale du navire



Surveillance renforcée des points d'accès au SI du navire

Capacité d'enregistrement pour analyse/investigation à posteriori

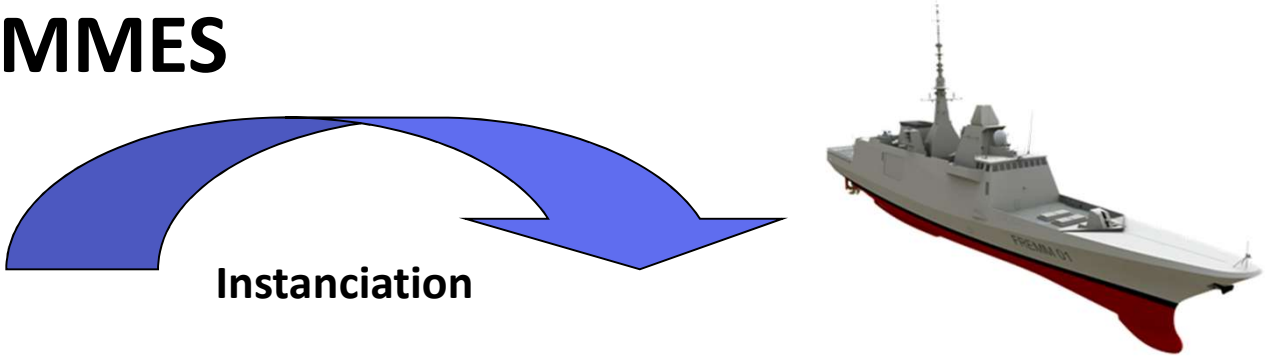
Adaptation aux contraintes du navire (ex: encombrement)

Convergence supervision SI et supervision sécurité (logique + physique)

Respect des standards et privilégier les solutions ouvertes

Architecture modulaire

RÉUTILISATION DE MALDIVES DANS LES PROGRAMMES



Résultats de MALDIVES

- Analyse de la menace
- Stratégie de détection
- Architecture LID de référence
- Besoin de capteurs métiers

Prise en compte de la sécurité cyber dès la phase de conception

Programmes existants : FREMM

- Vérification du maintien des performances
- Déploiement d'une 1er version LID « technique » (périmètre MALDIVES)
- Déploiement de capteurs « métiers »

Nouveaux programmes : FTI, …

- Transformation des résultats de MALDIVES en données d'entrée (spécification/conception)