Security Problems in operational navy systems, Industrial point of view

STRENGTH at sea

DCNS

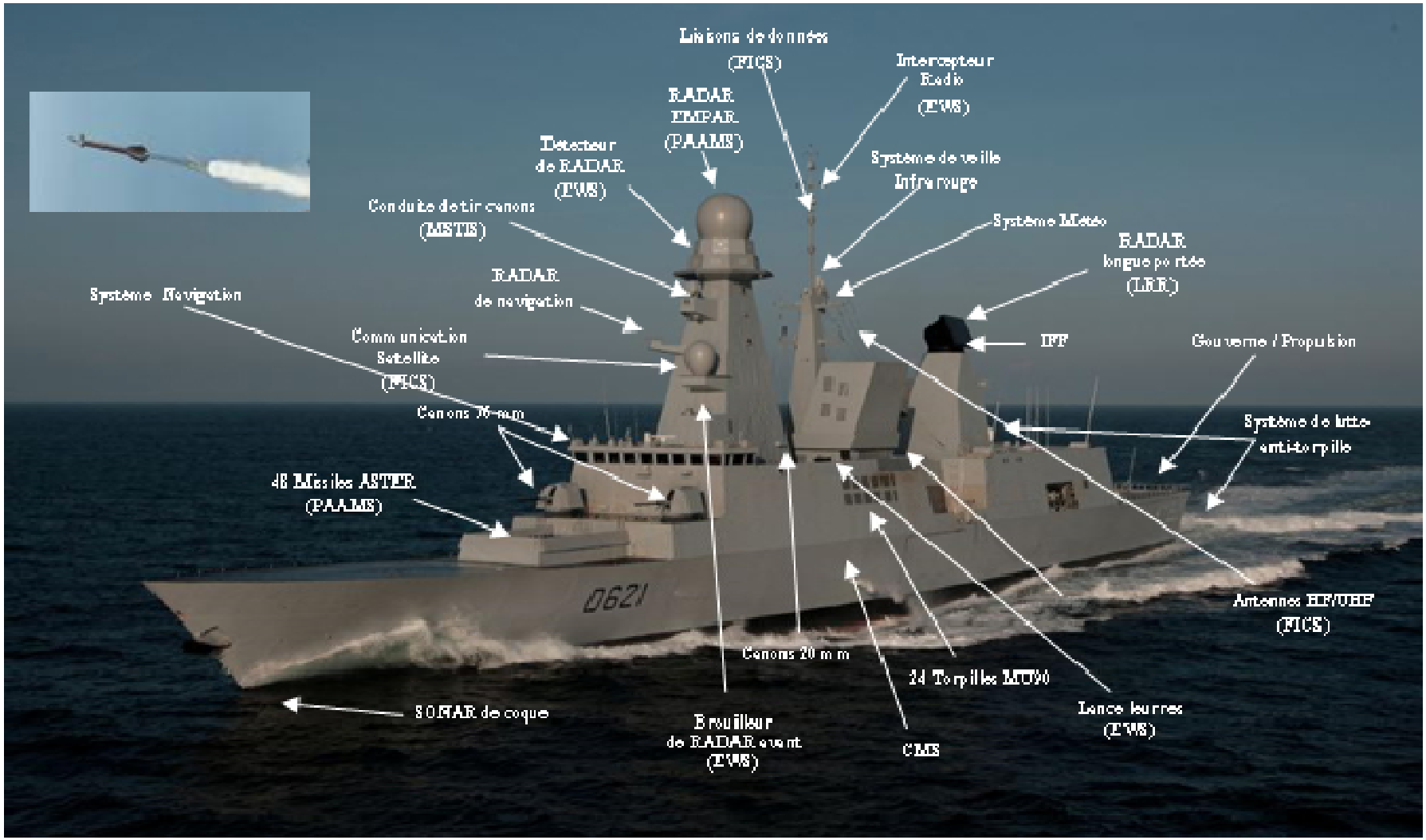
Laurent COMTE, head of security laboratory

September 21, 2011

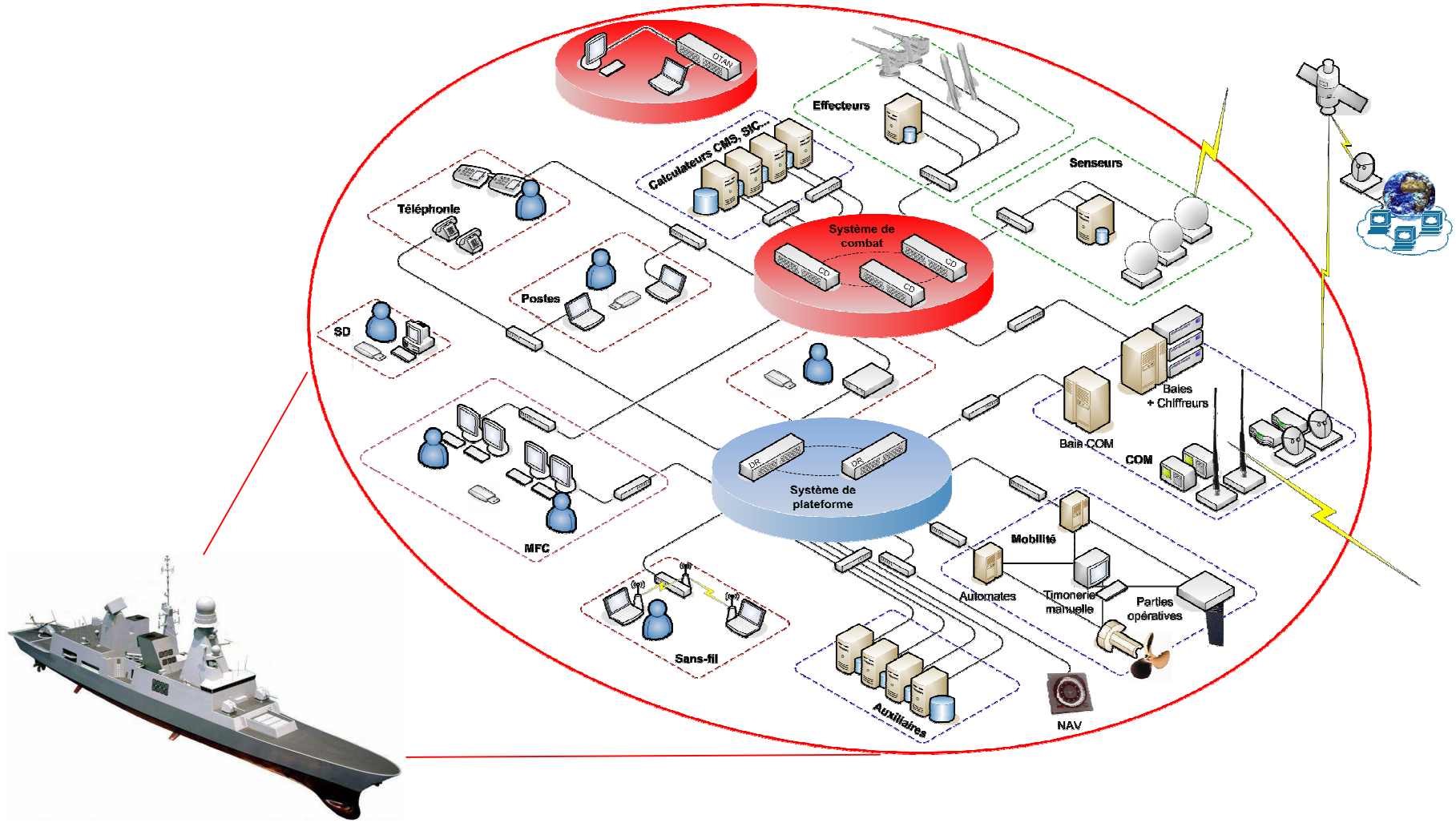
CONTENT

1. Introduction and Context
2. Risk approach
3. Methodology
4. Solutions
5. Conclusion

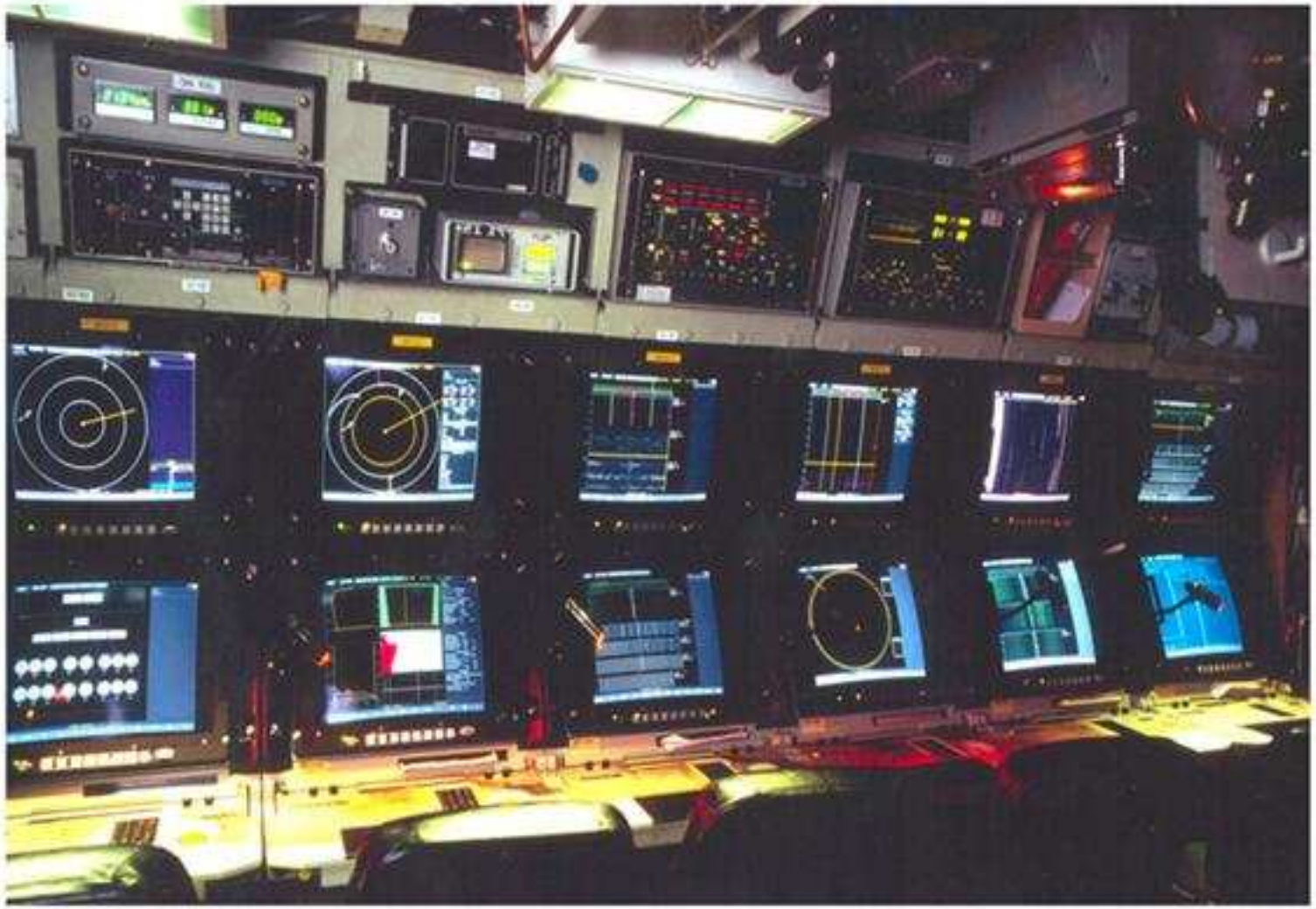
Context : Warship Information System
Combat System & Ship Management System



Context : Warship Information System
Combat System & Ship Management System



Context : Warship Information System
Central Operation Room



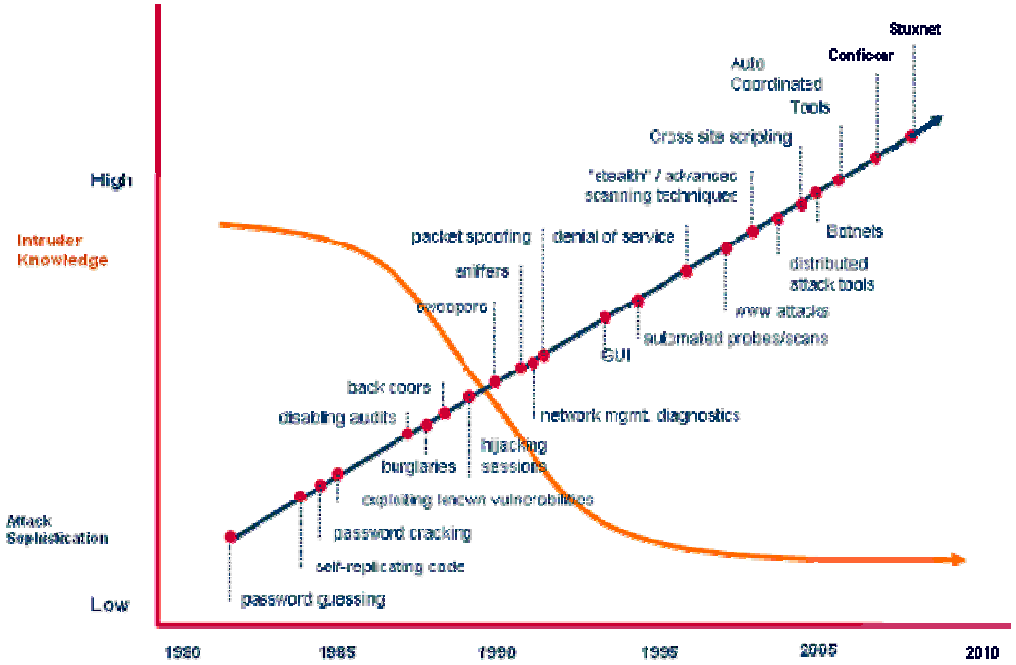
Warship Information System Security : Why Based on Civil Technology

- **Duality Civil / Military**
  - Hardware : PC based equipment
  - Operating Systems : Linux, Windows
  - Application level : web technology, Java
  - Network protocols : TCP/IP, HTTP
  - Network equipments : switch, router
- **Advantages :**
  - Cost reduction
  - Maturity of the Technology
  - Performances

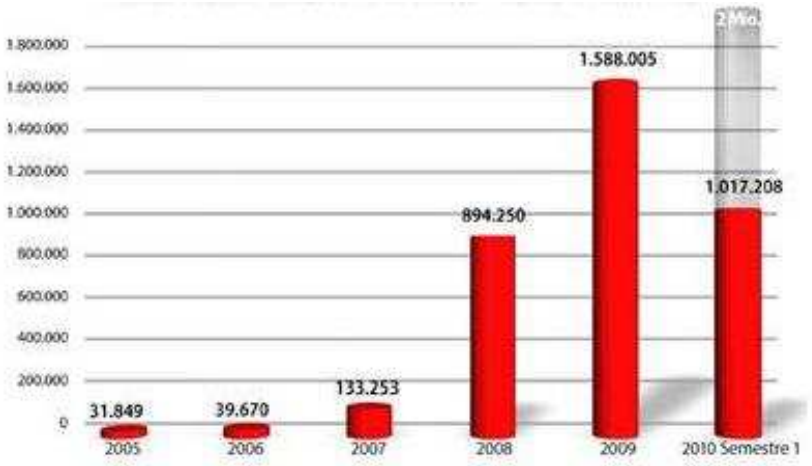
Warship Information System Security : Why Based on Civil Technology

- **Duality Civil / Military**
  - Hardware : PC based equipment
  - Operating Systems : Linux, Windows
  - Application level : web technology, Java
  - Network protocols : TCP/IP, HTTP
  - Network equipments : switch, router
- **Advantages :**
  - Cost reduction
  - Maturity of the Technology
  - Performances
- **But :**
  - **Well known Vulnerabilities**

Warship Information System Security : Why Increase of security attack



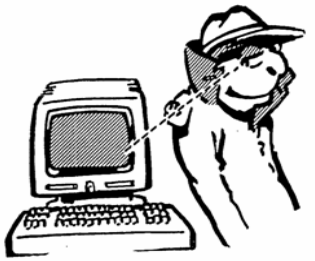
New malware between 2005 and 2010



Warship Information System Security : Why Critcal Impacts

- **Combat system :**
  - **Confidentiality : Communication,**
    - e.g : disclosure of mission data
  - **Integrity : Tactical situation, information database**
    - e.g : corruption of missile target data
  - **Availability : main warfare systems**
    - e.g : shutdown of Air Defence System

Confidentiality



Integrity

Availability

Warship Information System Security : Why Critical Impacts

- **Ship Management System :**
  - **Confidentiality : navigation subsystem**
    - e.g : disclosure of SSBN position
  - **Integrity : auxiliary automate**
    - e.g : corruption of the course
  - **Availability : ship management**
    - e.g : uncontrollability of the ship

Availability

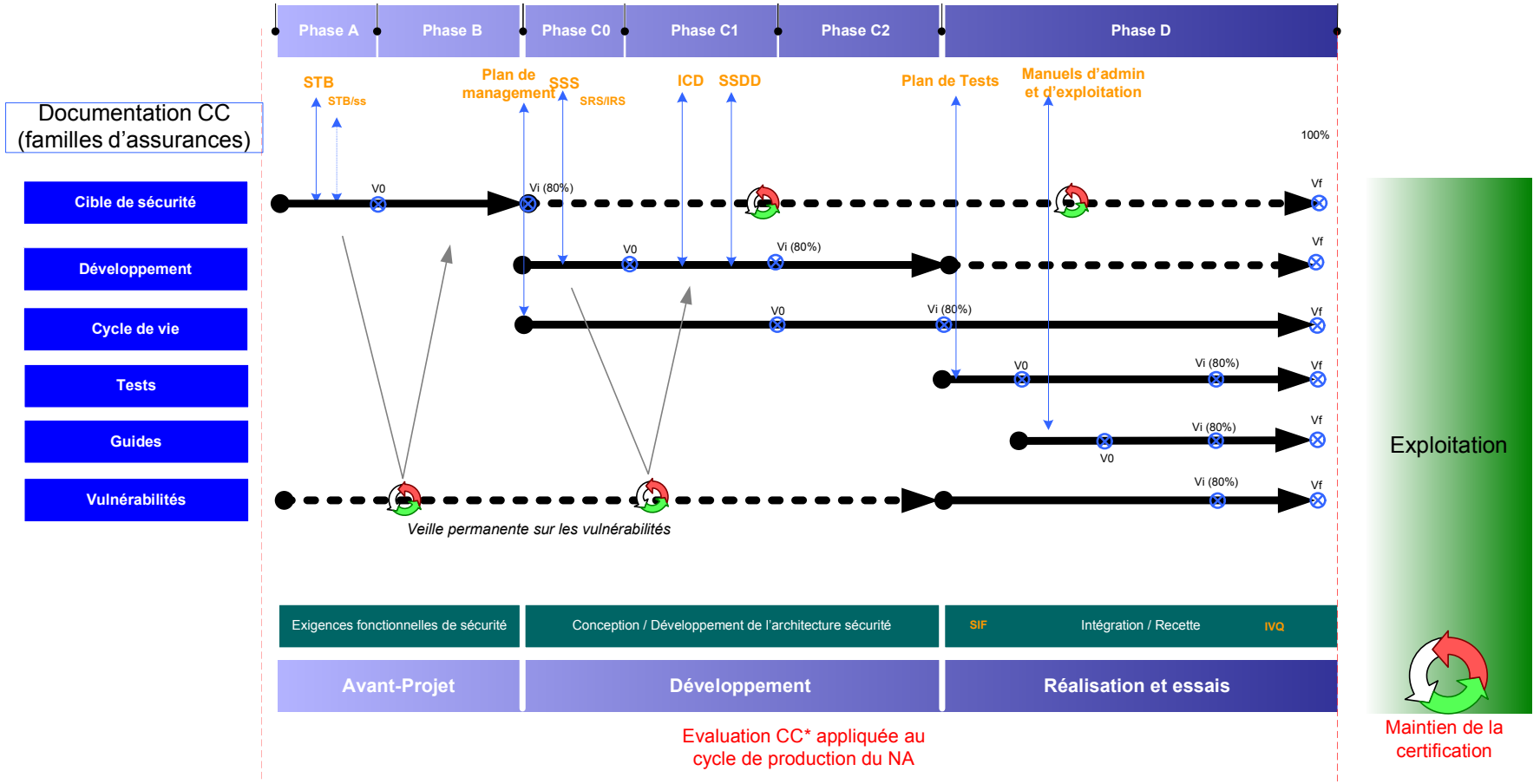
Integrity

Confidentiality

Warship Information System Security : How Security Methodology

- **Methodology depends on National or NATO Security Accreditation Authority**
  - **Accreditation process**
    - Risk analysis (MOD)
    - Security requirements (IND)
    - Security mechanisms development and test (IND)
    - Audit (MOD)
    - Authority acceptation (MOD)
  - **Common Criteria methodology**
    - Global security analysis to give an assurance on the whole information system
      - › e.g : EAL1 at whole warship level
    - A deeper analysis for critical part of the system
      - › e.g : EAL3-5 at subsystem, component or equipment

Warship Information System Security : How Security in Industrial development



Warship Information System Security : How Security Functions

- **Risk analysis lead to security requirements**
  - **Based on Common Criteria Security Functions**

  - **Identification and authentication**
  - **Access Control Policy**
  - **Flux Control Policy**
  - **User Data Protection**
  - **Communication and cryptography**
  - **Security Audit**
  - **Security Management**

Warship Information System Security : What Security mechanisms

- **Architecture**
  - Sensitive level separation
  - Red / Black Architecture
- **GOTS/COTS integration**
  - Cipher
  - Antivirus
  - Firewall
  - IDS/IPS
  - Diode
- **Specific development**
  - Operating System Configuration
  - Software Components

Antivirus

IP Cipher

Firewall

IDS/IPS

Warship Information System Security : What Security mechanisms

- **Physical security**
  - Electronic access control
  - Alarms
  - Video surveillance
  - Intruder detection systems

Protected areas

CCTV

Locks

- **Administration and Organisation of Security**
  - Regulation
  - Security operating procedures
  - Technical policies (ex: password policy)

Safes

InfraRed & hyper-frequency sensors

Motion detectors

- **Personnel security**
  - Security clearance
  - Training

Holograms

Digicode

security seals

Warship Information System Security
Conclusion

- **Warship Information System can be targeted by malware**
  - **System based on civilian technology**
  - **Number of malware increasing**
  - **Human life impact**

Security … Not an option … A MUST

STRENGTH at sea