Journée Thématique “Validation de architectures de Système via les modèles MBSE-MBSA”

“ Approche MBSA à la DGA ”

http://afis.community/jt-afis-validation-architectures-systeme-par-utilisation-des-modeles-mbse-mbsa/

Christophe FRAZZA
Expert modélisation dysfonctionnelle

CONSTRUISONS ENSEMBLE
LA DÉFENSE DE DEMAIN

Modélisation dysfonctionnelle (MBSA*)

des analyses de sécurité dirigées par les modèles

Christophe FRAZZA
DGA TA
christophe.frazza@intradef.gouv.fr

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES

***MBSA: Model Based Safety Assessment**

SOMMAIRE

- Objectifs
- Approche DGA
  - Documents d'entrée
  - Principes de la modélisation
  - Simulation / Validation
  - Résultats
- Plus-values illustrées
- Perspectives

DIVISION SIE (SYSTÈMES INFORMATIQUES EMBARQUÉS)

- Mission
  - Expertise en vue de la Certification et de la Qualification des systèmes et logiciels critiques
- Activités
  - Validation des architectures (ARP 4754 & 4761)
    - Fonctionnelles (FHA)
    - Organiques (PSSA / SSA)
    - Zonales (ZHA, PRA)
  - Expertise des logiciels et composants complexes (DO-178 & DO-254)
    - Audits dépendants du DAL (Development Assurance Level)
  - Qualification des équipements aux environnements (DO-160)
    - Niveau d'agression dépendant du DAL ou « Safe path »

DGA

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMÉES

OBJECTIFS

Problématique

- Des types d'aéronefs variés et complexes
  - Avions de transport, avions de chasse, hélicoptères, drones, ...
- Des tonnes de documentation
  - Plus de 20 systèmes par aéronefs
  - 1000 à 1500 pages d'analyses par système
    - 1 avion = 25 000 pages d'analyses de sécurité
- Des délais courts, des équipes réduites
  - « C'était pour hier,
    mais pour demain ça ira... »

DGA

MINISTÈRE DES ARMÉES

OBJECTIFS

- Vérifier la bonne allocation de DAL* (ARP 4754 A)
- Déterminer les causes communes - CCA
  - Modes communs - CMA (alimentation, développement...)
  - Analyse zonale - ZSA (feu, fuite …)
  - Risques particuliers - PRA (foudre, choc à l'oiseau…)
- Orienter l'ingénierie de nos essais
- Supporter les enquêtes après accident

→ Utiliser des modèles pour supporter nos expertises

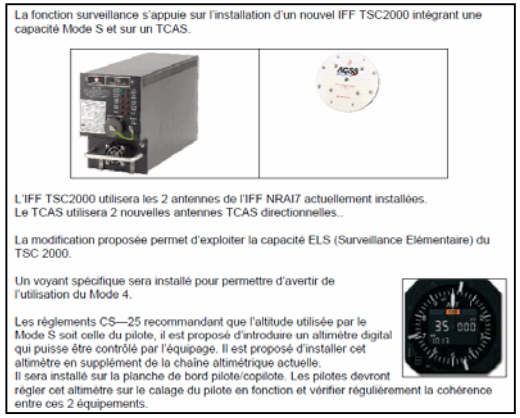
* DAL Development Assurance level

SOMMAIRE

- Objectifs
- Approche DGA
  - Documents d'entrée
  - Principes de la modélisation
  - Simulation / Validation
  - Résultats
- Plus-values illustrées
- Perspectives

DOCUMENTS D'ENTRÉE

Descriptif fonctionnel



La fonction surveillance s'appuie sur l'installation d'un nouvel IFF TSC2000 intégrant une capacité Mode S et sur un TCAS.

L'IFF TSC2000 utilisera les 2 antennes de l'IFF NRAI7 actuellement installées.
Le TCAS utilisera 2 nouvelles antennes TCAS directionnelles..

La modification proposée permet d'exploiter la capacité ELS (Surveillance Elémentaire) du TSC 2000.

Un voyant spécifique sera installé pour permettre d'avertir de l'utilisation du Mode 4.

Les réglements CS—25 recommandant que l'altitude utilisée par le Mode S soit celle du pilote, il est proposé d'introduire un altimètre digital qui puisse être contrôlé par l'équipage. Il est proposé d'installer cet altimètre en supplément de la chaîne altimétrique actuelle.
Il sera installé sur la planche de bord pilote/copilote. Les pilotes devront régler cet altimètre sur le calage du pilote en fonction et vérifier régulièrement la cohérence entre ces 2 équipements.

Analyses de sécurité (type FHA)

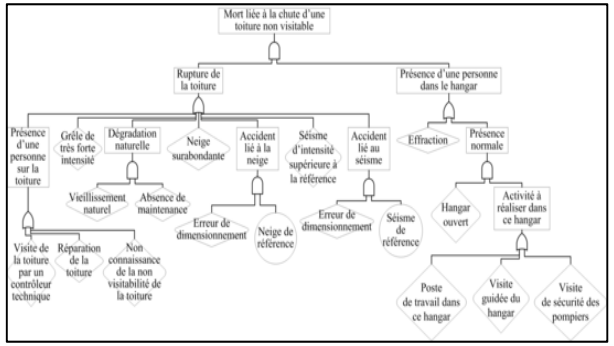
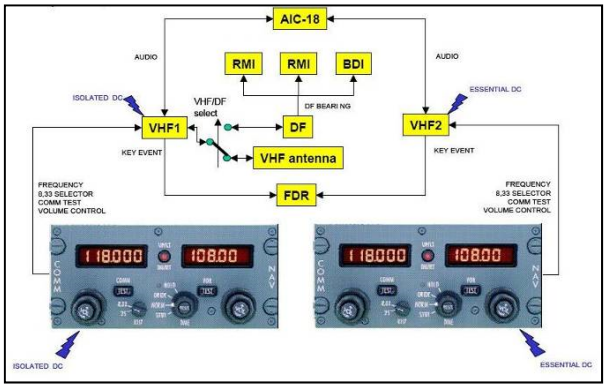
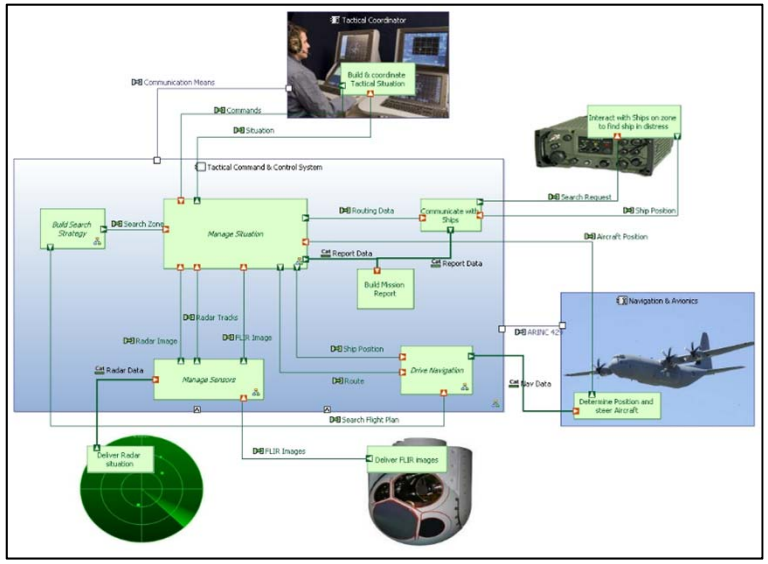


Schéma d'architecture

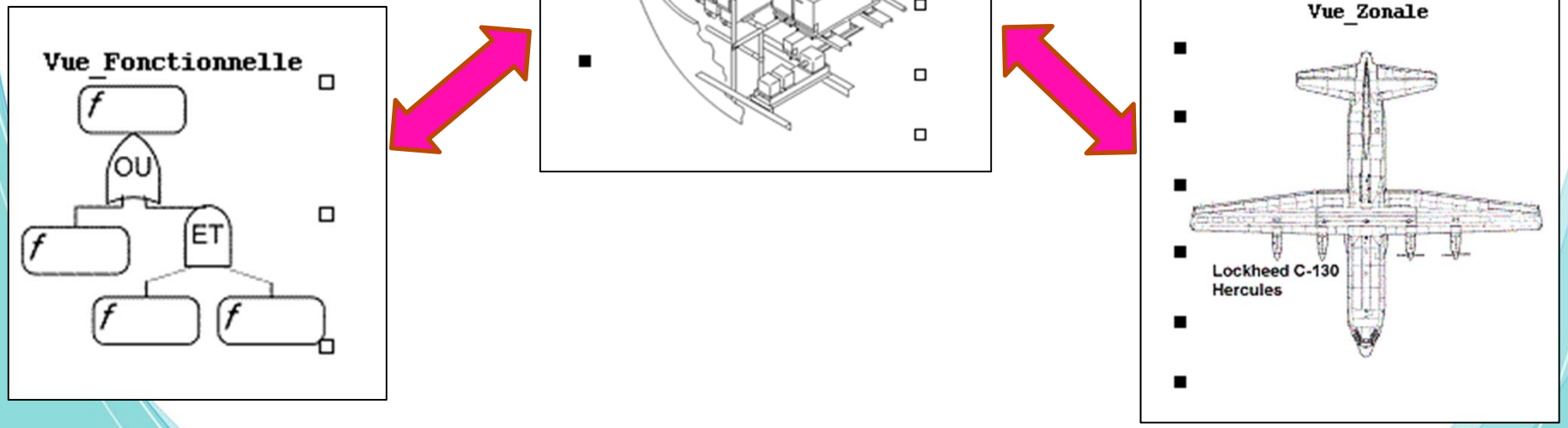


Modèle d'Ingénierie Système (MBSE)

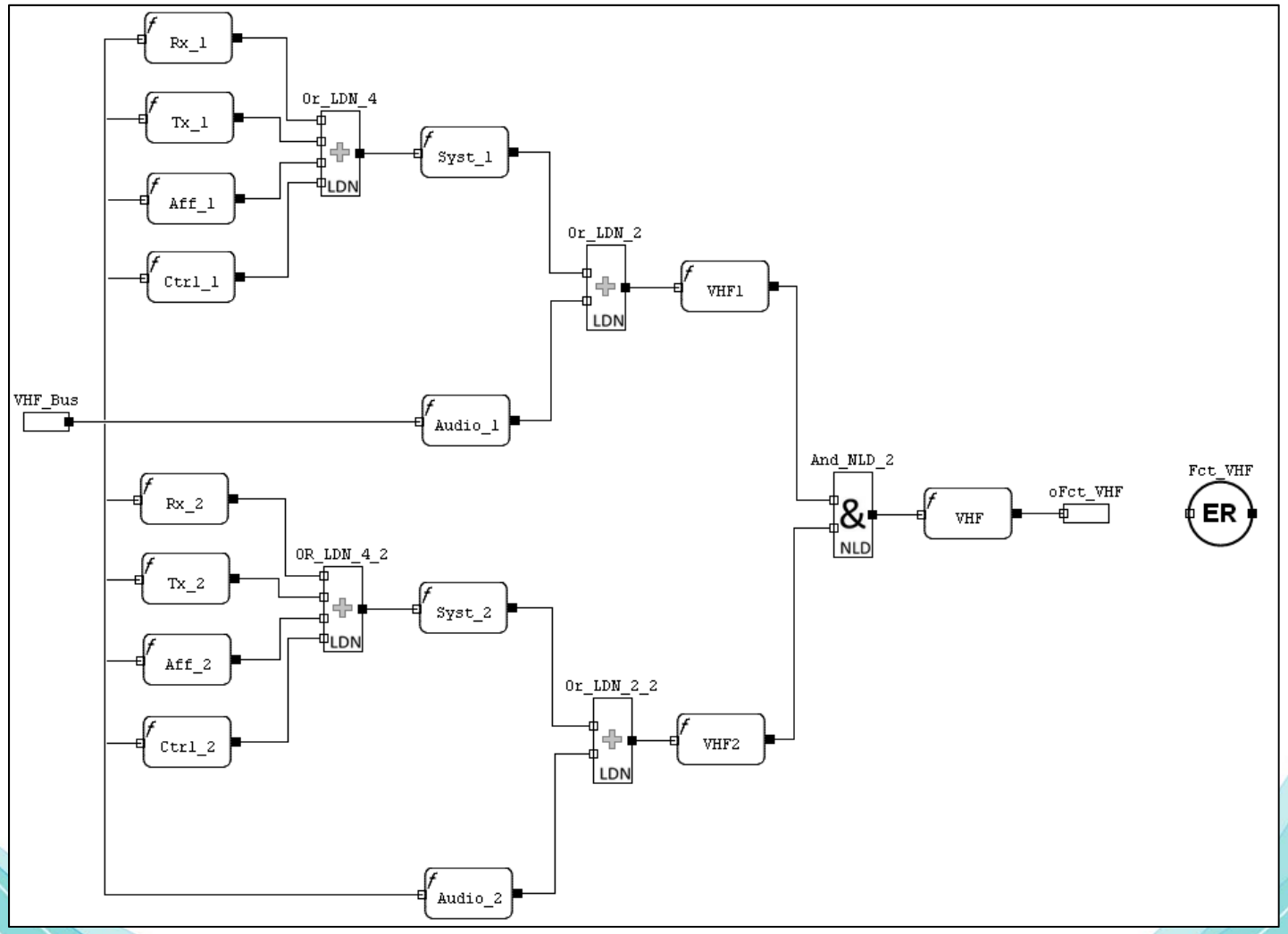


PRINCIPES

Vues du modèle = méta-modèle

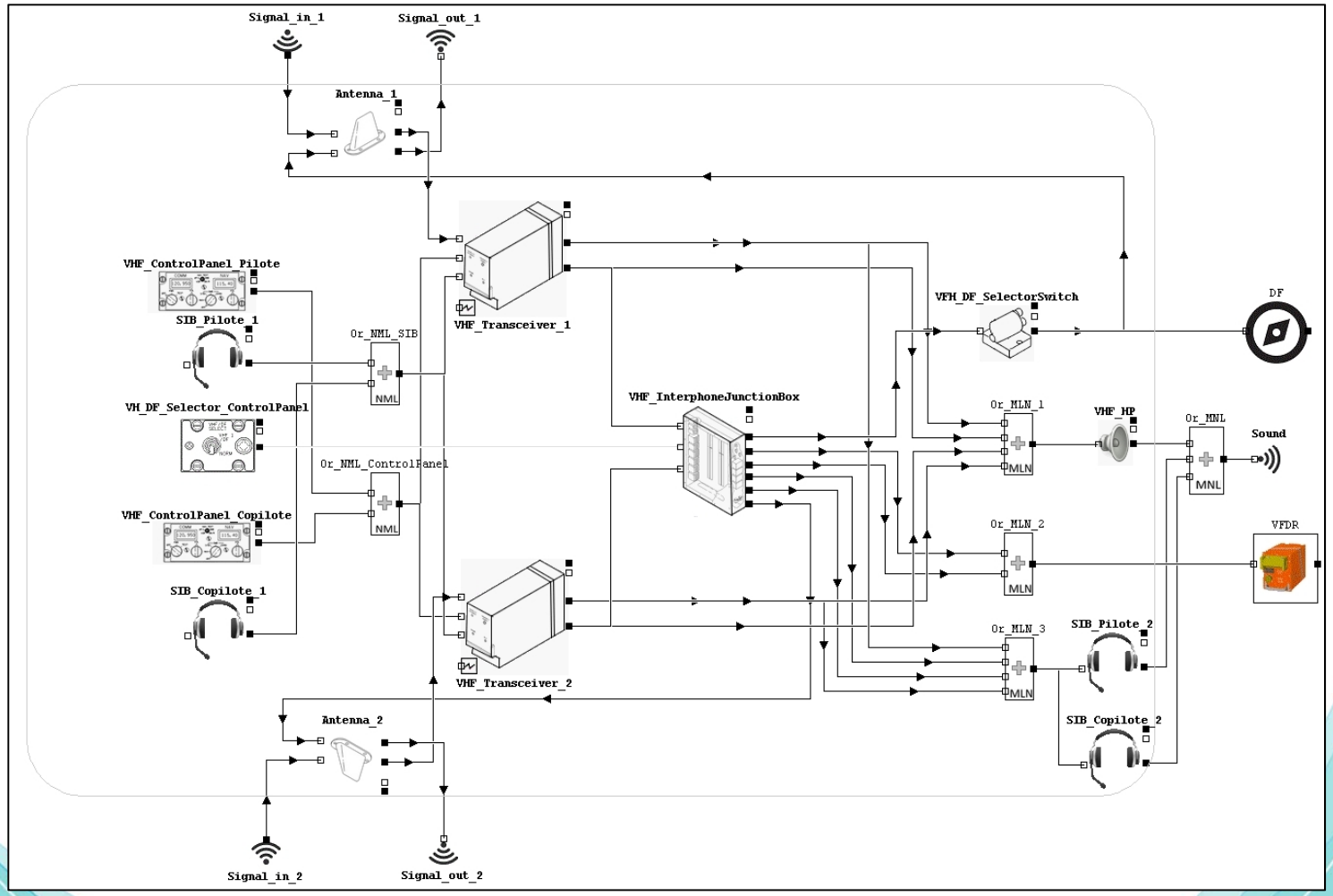


PRINCIPES
Vue fonctionnelle



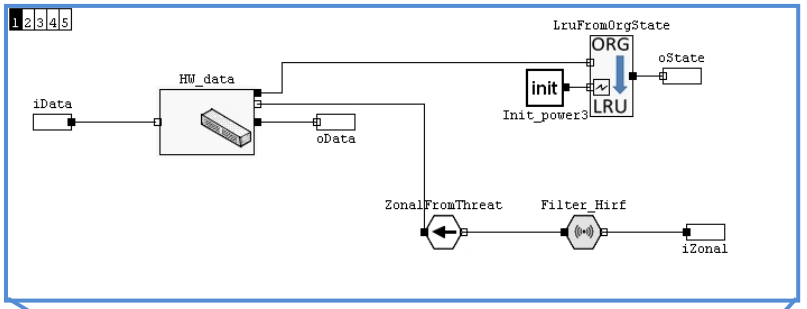
PRINCIPES

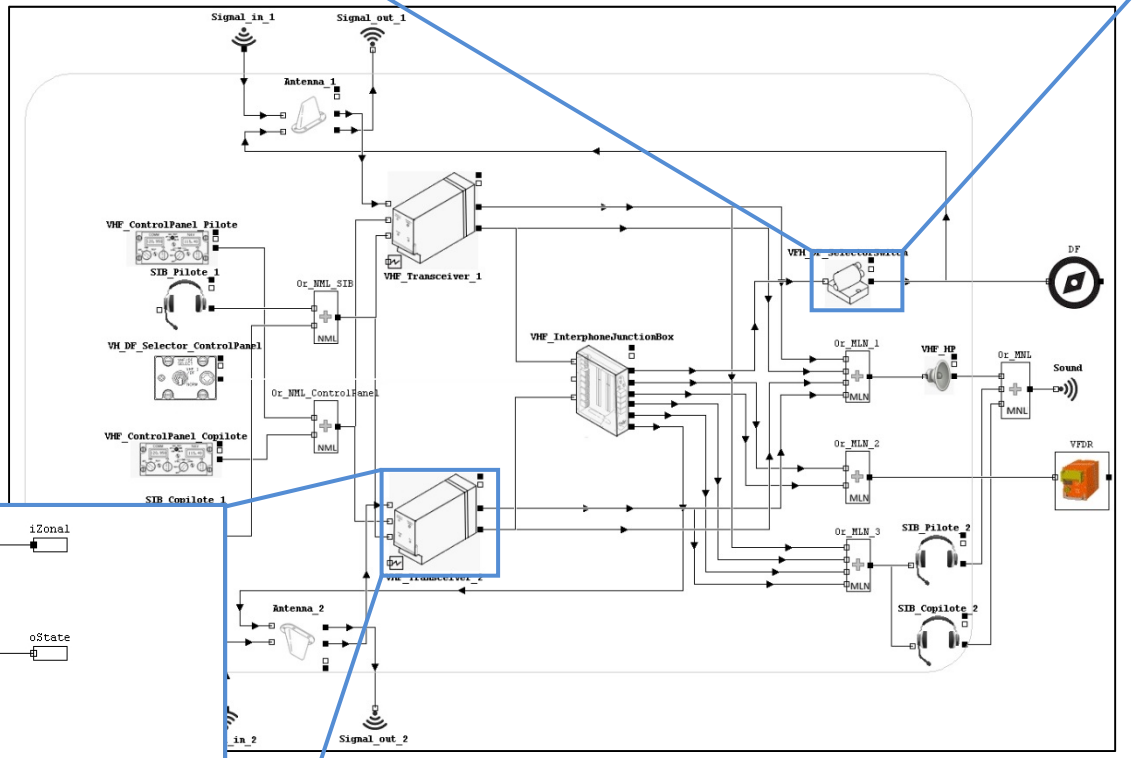
Vue organique

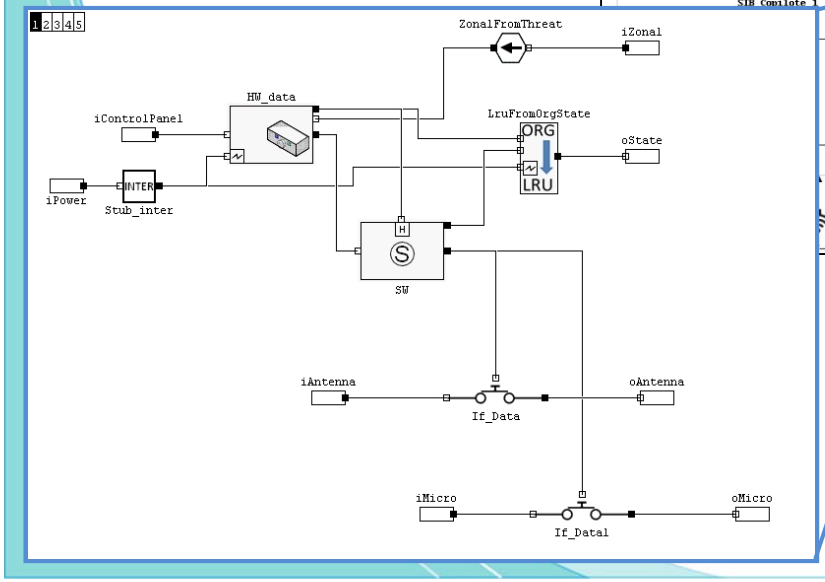


PRINCIPES

Vue organique

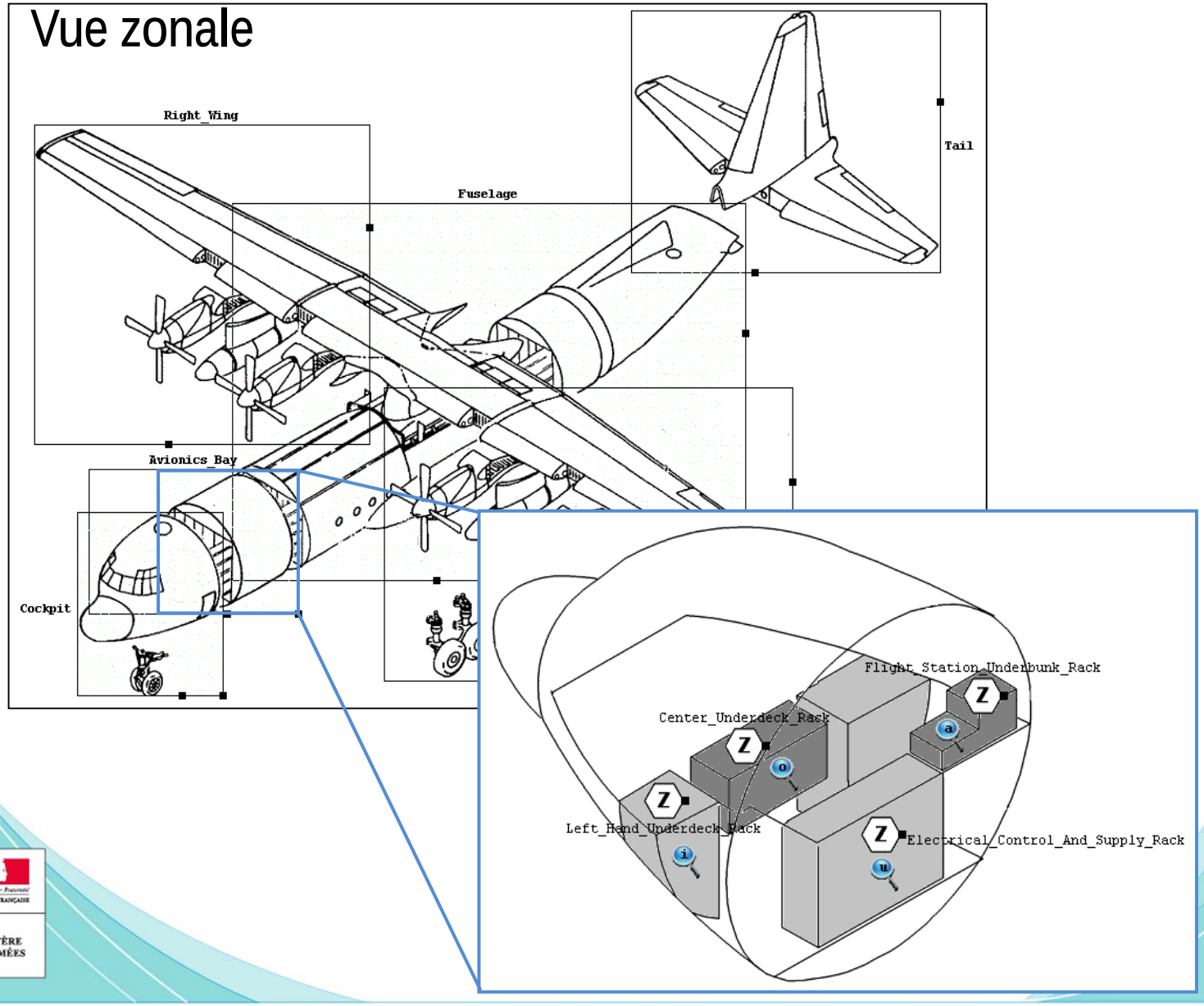




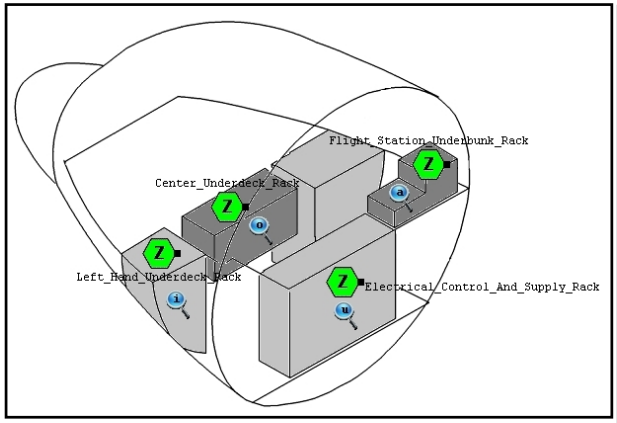


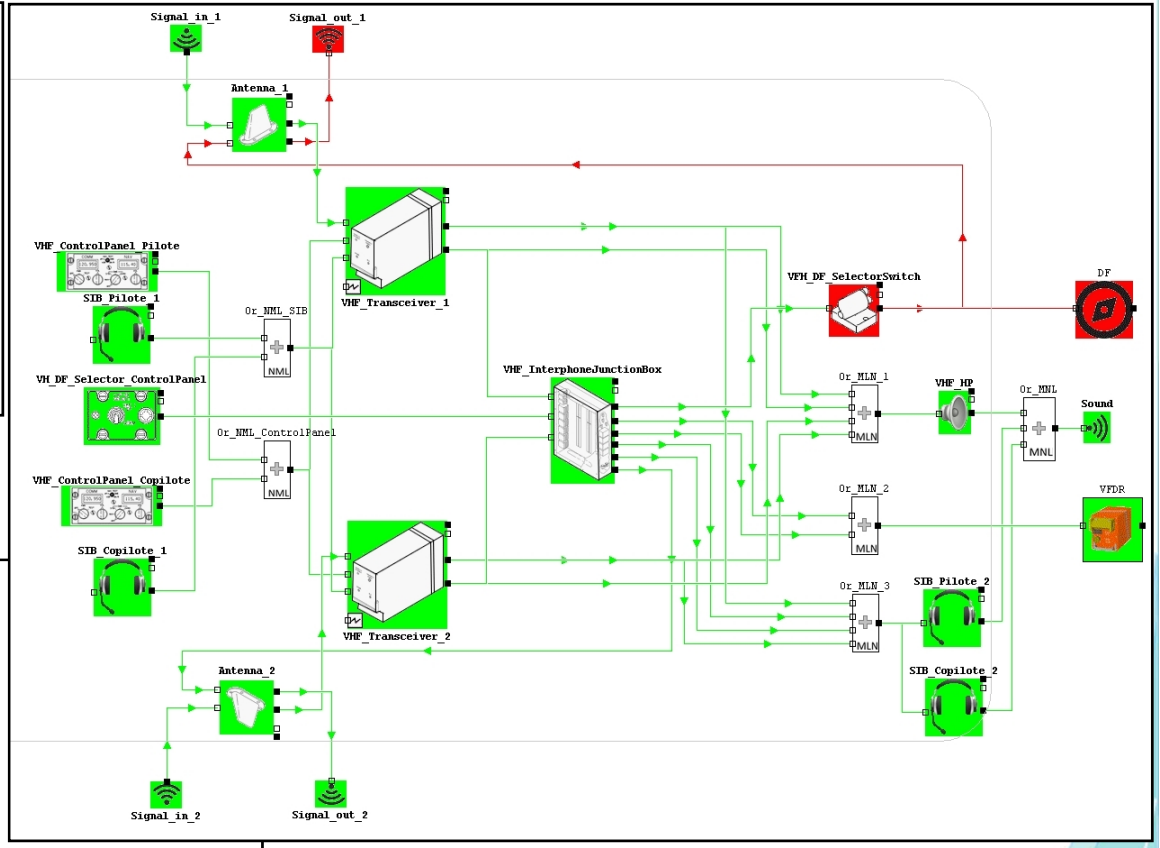
PRINCIPES

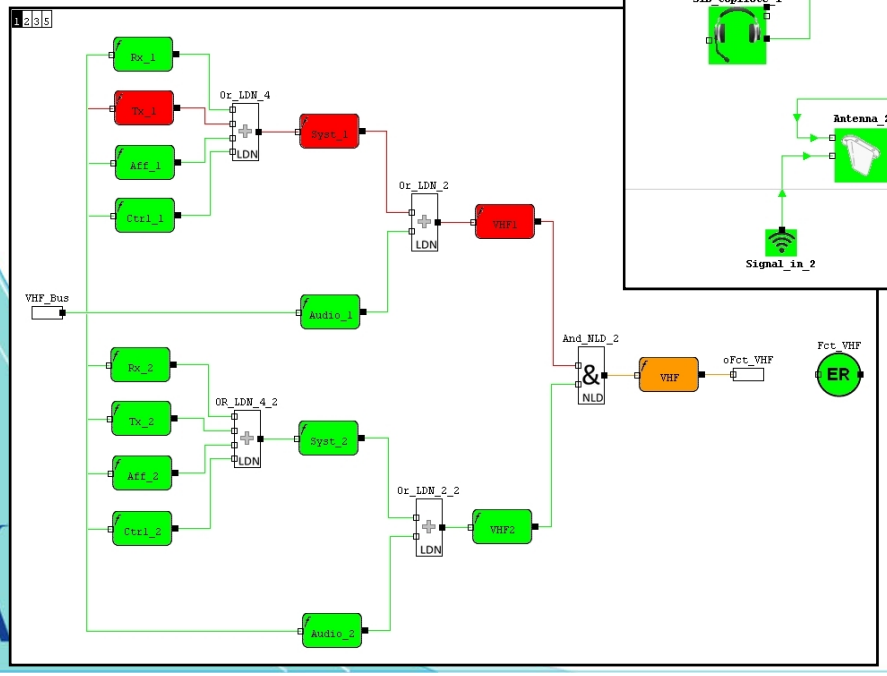
Vue zonale



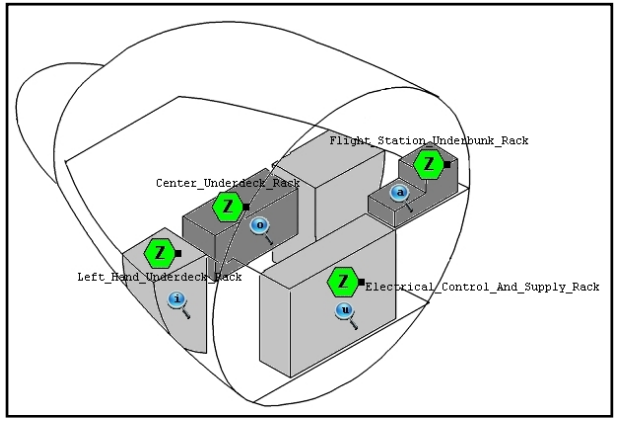
SIMULATION-VALIDATION

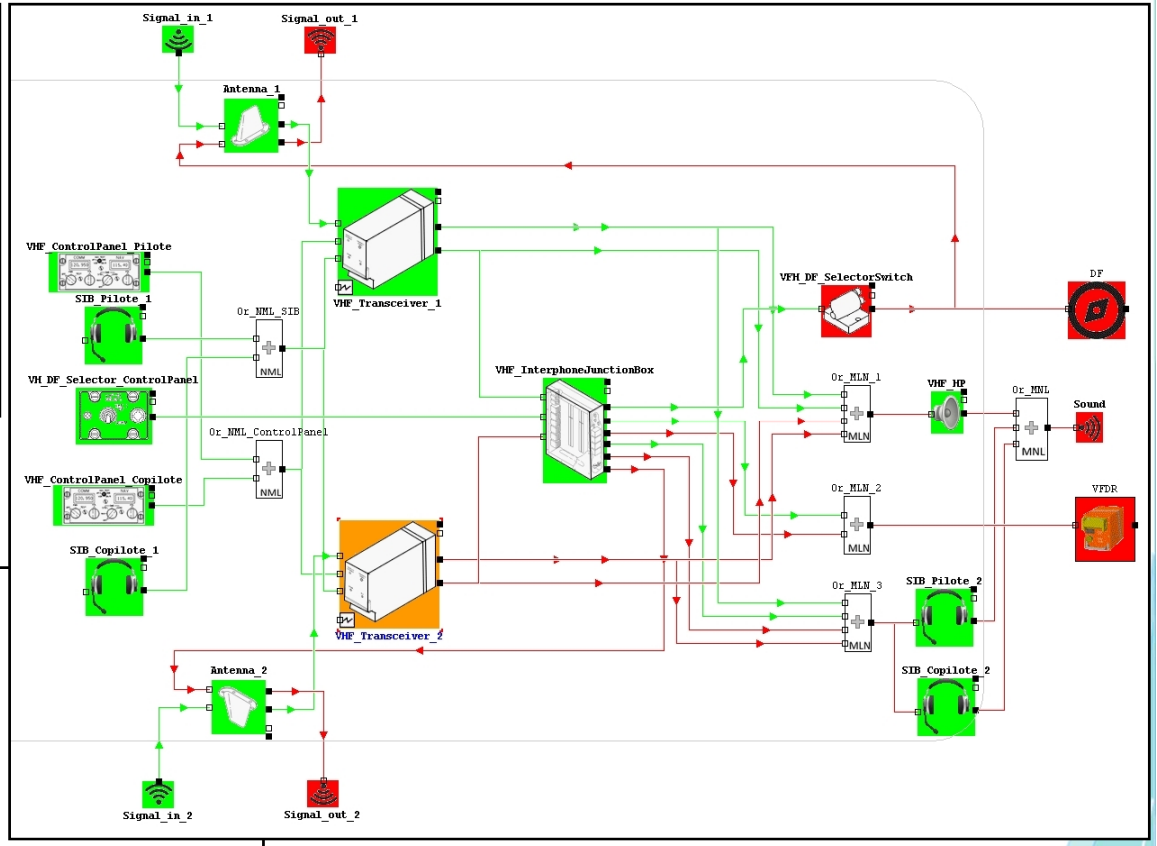


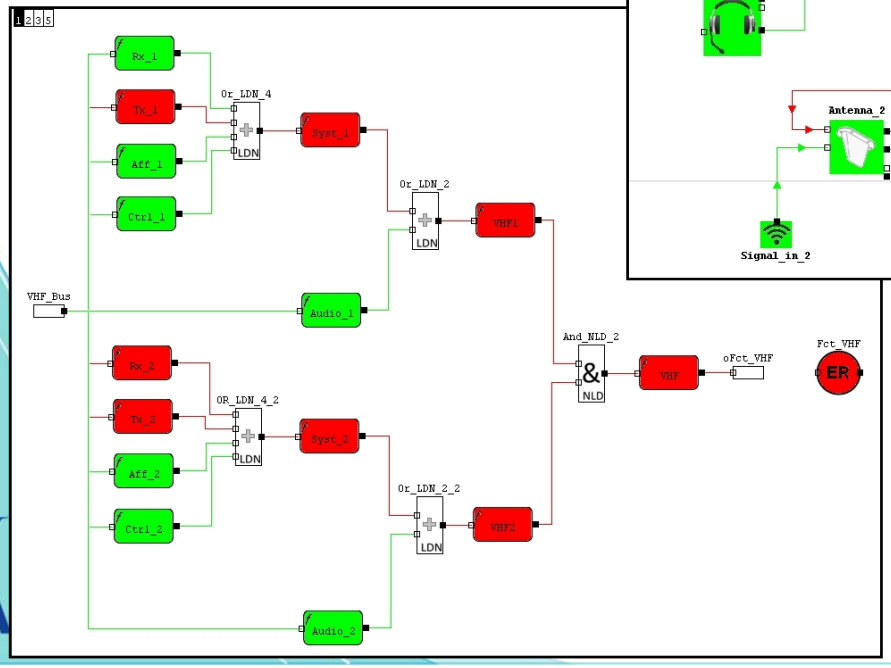




SIMULATION-VALIDATION

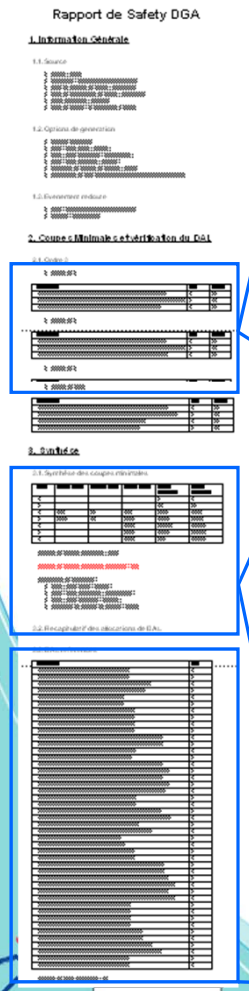






RÉSULTATS

Combinaison exhaustive des évènements ➡ coupes


Rapport de Safety DGA

1. Information Générale

2. Coupes Minimales et vérification du DAL

3. Synthèse

- Coupe n° 57

Evénement	DAL	Check
SysCOM.Organic.RxCOM_VHF.synchro_SW_eMisleading_TransceiverVHF	B	OK
SysCOM.Organic.RxCOM_UHF.Transceiver_UHF.SW.eFailure	C	OK
SysCOM.Organic.RxCOM_HF.synchro_SW_eFailure_TransceiverHF	B	OK

- Coupe n° 58

Evénement	DAL	Check
SysCOM.Organic.RxCOM_VHF.synchro_SW_eMisleading_TransceiverVHF	B	FAIL
SysCOM.Organic.RxCOM_UHF.Transceiver_UHF.SW.eFailure	C	FAIL
SysCOM.Organic.RxCOM_HF.synchro_SW_eMisleading_TransceiverHF	C	FAIL

option-1 [un DAL niveau A et les autres de niveau C minimum] ou option-2 [deux DAL niveau B et les autres de niveau C minimum]

3.1. Synthèse des coupes minimales

Ordre	Coupe (Filtre)	Erronée (DAL)	Cumul (Filtre)	Coupe (Complet)	Cumul (Complet)
1				4	4
2				36	40
3	176	36	176	2718	2758
4	2264	88	2440	31648	34406
5			2440	185184	219590
6			2440	23008	242598
7			2440	892	243490

Nombre de coupes minimales : 2440

Nombre de coupes minimales erronnées : 124

Paramètres de génération :

- Filtre : Filtre Zonal (.Zonal.)
- Filtre : Filtre Electrique (.RxElectric.)
- Filtre : Filtre Bouchon (.STUB)
- Limitation du nombre de coupes : 10000

3.3. DAL référencés

Evénement	DAL
SysCOM.Organic.RxCOM_HF.Antenne_HF_1.HW	A
SysCOM.Organic.RxCOM_HF.Antenne_HF_2.HW	B
SysCOM.Organic.RxCOM_HF.ControlPanel_HF_Copilote.HW	C
SysCOM.Organic.RxCOM_HF.ControlPanel_HF_Pilote.HW	A
SysCOM.Organic.RxCOM_HF.CouplerHF1.HW	B
SysCOM.Organic.RxCOM_HF.CouplerHF2.HW	C
SysCOM.Organic.RxCOM_HF.HF_Transceiver_1.HW	A
SysCOM.Organic.RxCOM_HF.HF_Transceiver_1.SW	B
SysCOM.Organic.RxCOM_HF.HF_Transceiver_2.HW	C
SysCOM.Organic.RxCOM_HF.HF_Transceiver_2.SW	A
SysCOM.Organic.RxCOM_HF.InterphoneJunctionBox_HF.RelayHF1	B
SysCOM.Organic.RxCOM_HF.InterphoneJunctionBox_HF.RelayHF2	C
SysCOM.Organic.RxCOM_HF.Micro_HF_Copilote.HW	A
SysCOM.Organic.RxCOM_HF.Micro_HF_Pilote.HW	B
SysCOM.Organic.RxCOM_HF.synchro_HW_eFailure_TransceiverHF	C
SysCOM.Organic.RxCOM_HF.synchro_HW_eMisleading_TransceiverHF	A
SysCOM.Organic.RxCOM_HF.synchro_SW_eFailure_TransceiverHF	B
SysCOM.Organic.RxCOM_HF.synchro_SW_eMisleading_TransceiverHF	C
SysCOM.Organic.RxCOM_UHF.Interphone_Junction_Box_UHF.Relay	A
SysCOM.Organic.RxCOM_UHF.Transceiver_UHF.HW	B
SysCOM.Organic.RxCOM_UHF.Transceiver_UHF.SW	C
SysCOM.Organic.RxCOM_UHF.UHF_Antenna_Selector_Switch.HW	A
SysCOM.Organic.RxCOM_UHF.UHF_Antenna_SelectorControlPanel.HW	B
SysCOM.Organic.RxCOM_UHF.UHF_ControlPanel.HW	C
SysCOM.Organic.RxCOM_UHF.UHF_DF_Selector_Switch.HW	A
SysCOM.Organic.RxCOM_UHF.UHF_HP.HW	B
SysCOM.Organic.RxCOM_UHF.UHF_Micro.HW	C
SysCOM.Organic.RxCOM_VHF.Antenne_VHF_1.HW	A
SysCOM.Organic.RxCOM_VHF.Antenne_VHF_2.HW	B
SysCOM.Organic.RxCOM_VHF.Interphone_Junction_Box.RelayVHF1	C
SysCOM.Organic.RxCOM_VHF.Interphone_Junction_Box.RelayVHF2	A
SysCOM.Organic.RxCOM_VHF.synchro_HW_eFailure_TransceiverVHF	B
SysCOM.Organic.RxCOM_VHF.synchro_HW_eMisleading_TransceiverVHF	C
SysCOM.Organic.RxCOM_VHF.synchro_SW_eFailure_TransceiverVHF	A
SysCOM.Organic.RxCOM_VHF.synchro_SW_eMisleading_TransceiverVHF	B
SysCOM.Organic.RxCOM_VHF.Transceiver_1.HW	C
SysCOM.Organic.RxCOM_VHF.Transceiver_1.SW	A
SysCOM.Organic.RxCOM_VHF.Transceiver_2.HW	B
SysCOM.Organic.RxCOM_VHF.Transceiver_2.SW	C
SysCOM.Organic.RxCOM_VHF.VHF_ControlPanel_1.HW	A
SysCOM.Organic.RxCOM_VHF.VHF_ControlPanel_2.HW	B
SysCOM.Organic.RxCOM_VHF.VHF_DF_Selector_Switch.HW	C
SysCOM.Organic.RxCOM_VHF.VHF_DF_SelectorControlPanel.HW	A
SysCOM.Organic.RxCOM_VHF.VHF_Micro_1.HW	B
SysCOM.Organic.RxCOM_VHF.VHF_Micro_2.HW	C

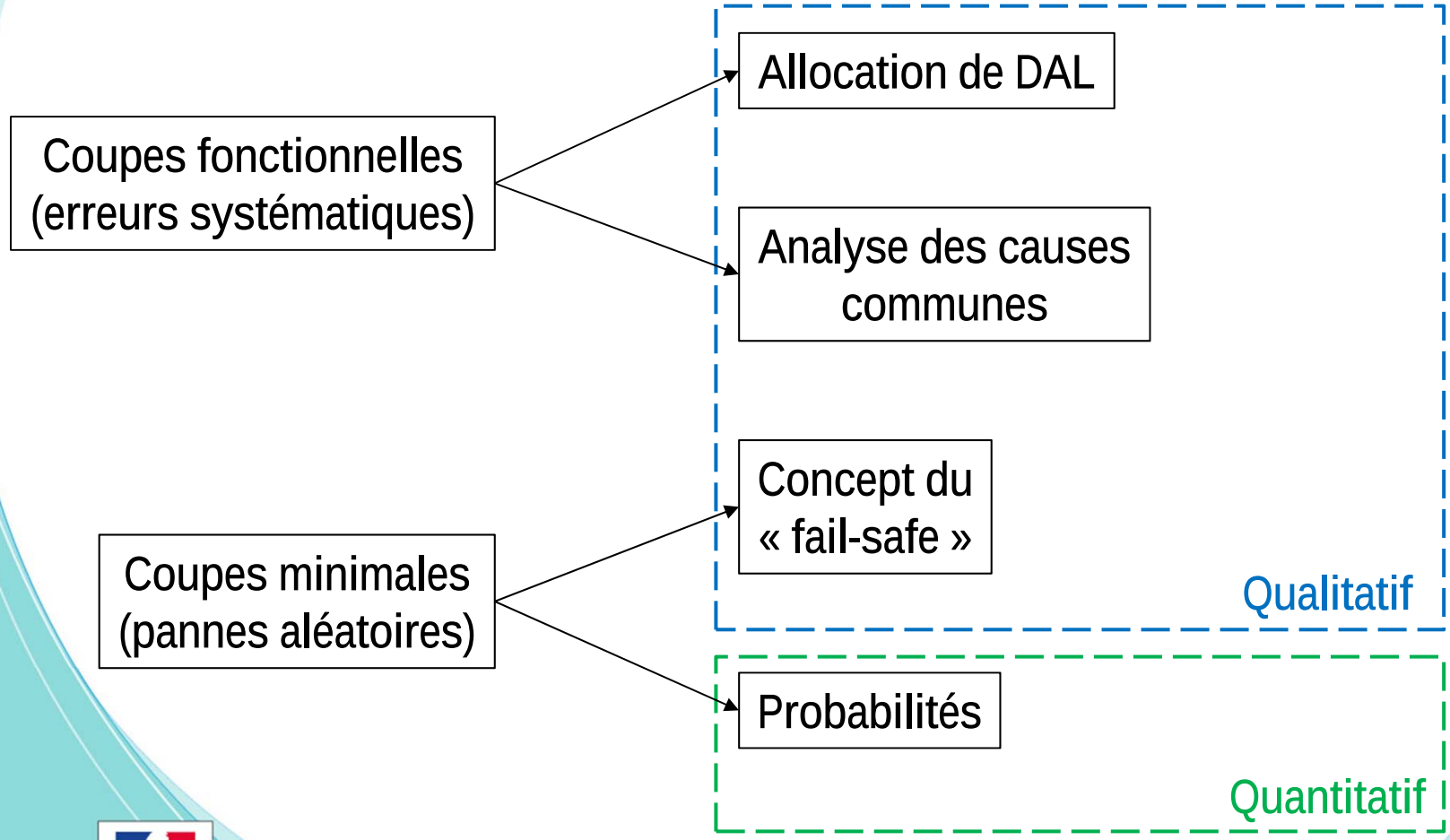
Nombre de DAL référencés : 45

DGA

MINISTÈRE DES ARMÉES

RÉSULTATS

Analyses



SOMMAIRE

- Objectifs
- Approche DGA
  - Documents d'entrée
  - Principes de la modélisation
  - Simulation / Validation
  - Résultats
- Plus-values illustrées
- Perspectives

PLUS-VALUES ILLUSTRÉES

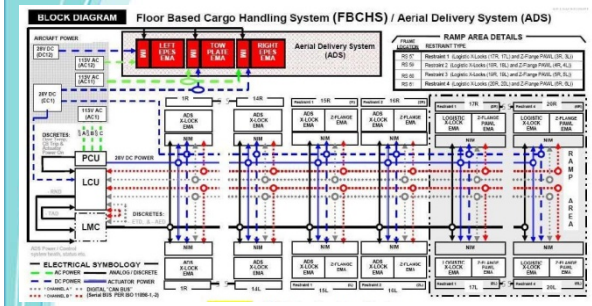
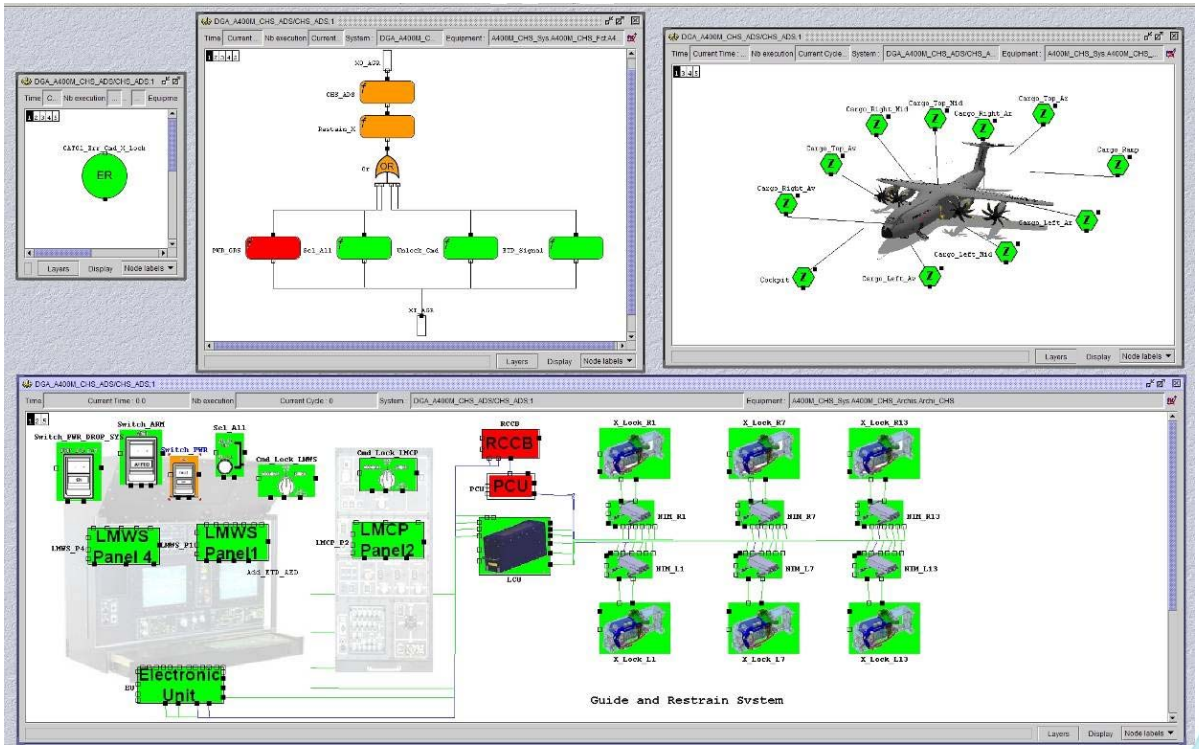


Schéma fonctionnel

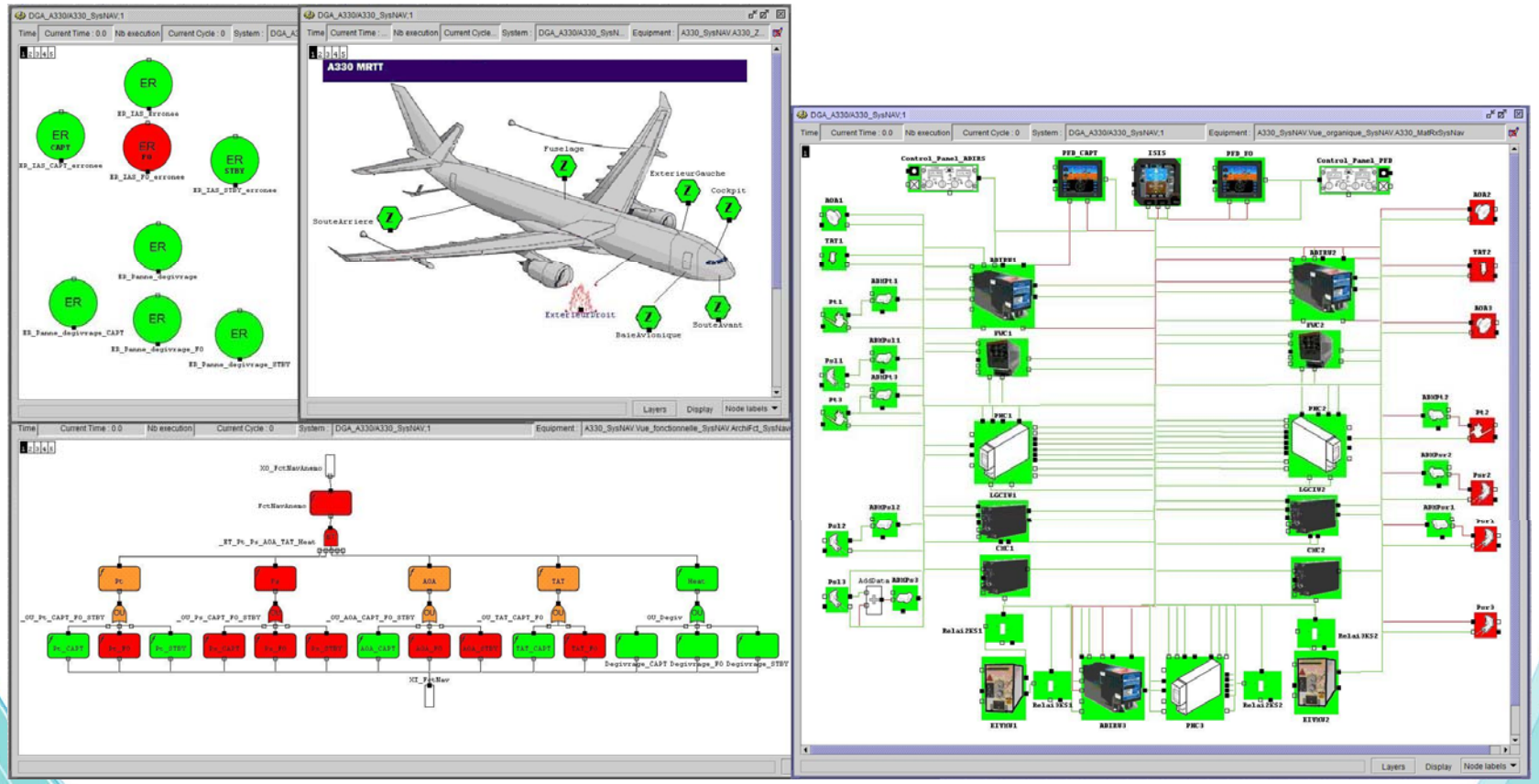
A400M – Cargo Handling System



- Incohérence des niveaux logiciels vs. ARP4754
- Lien vers la qualification environnementale

PLUS-VALUES ILLUSTRÉES

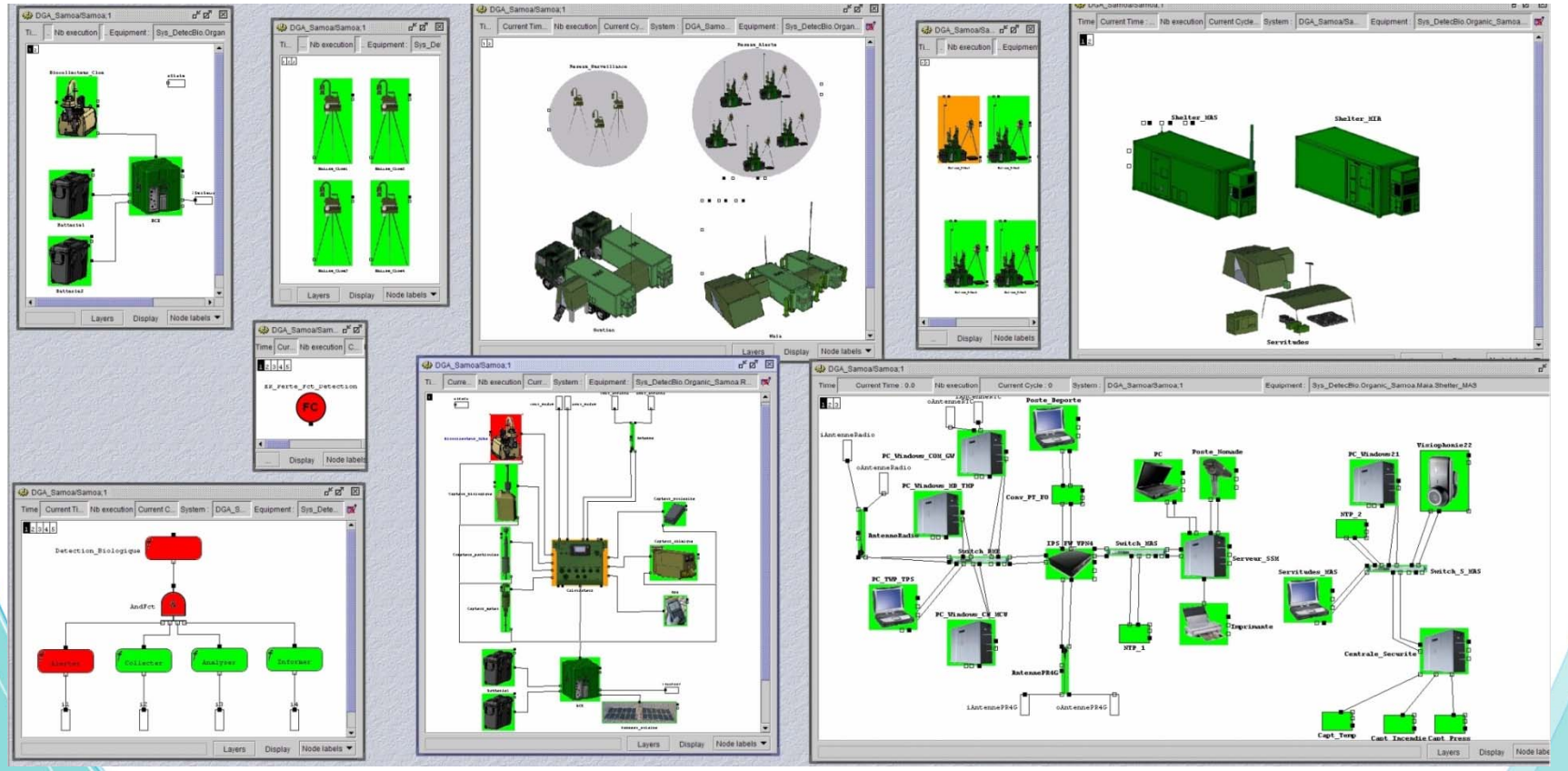
AF447 – Système de réchauffage des sondes



- Compréhension du comportement de l'environnement « sondes Pitot »
- Vérification de l'absence d'un mode commun de panne

PLUS-VALUES ILLUSTRÉES

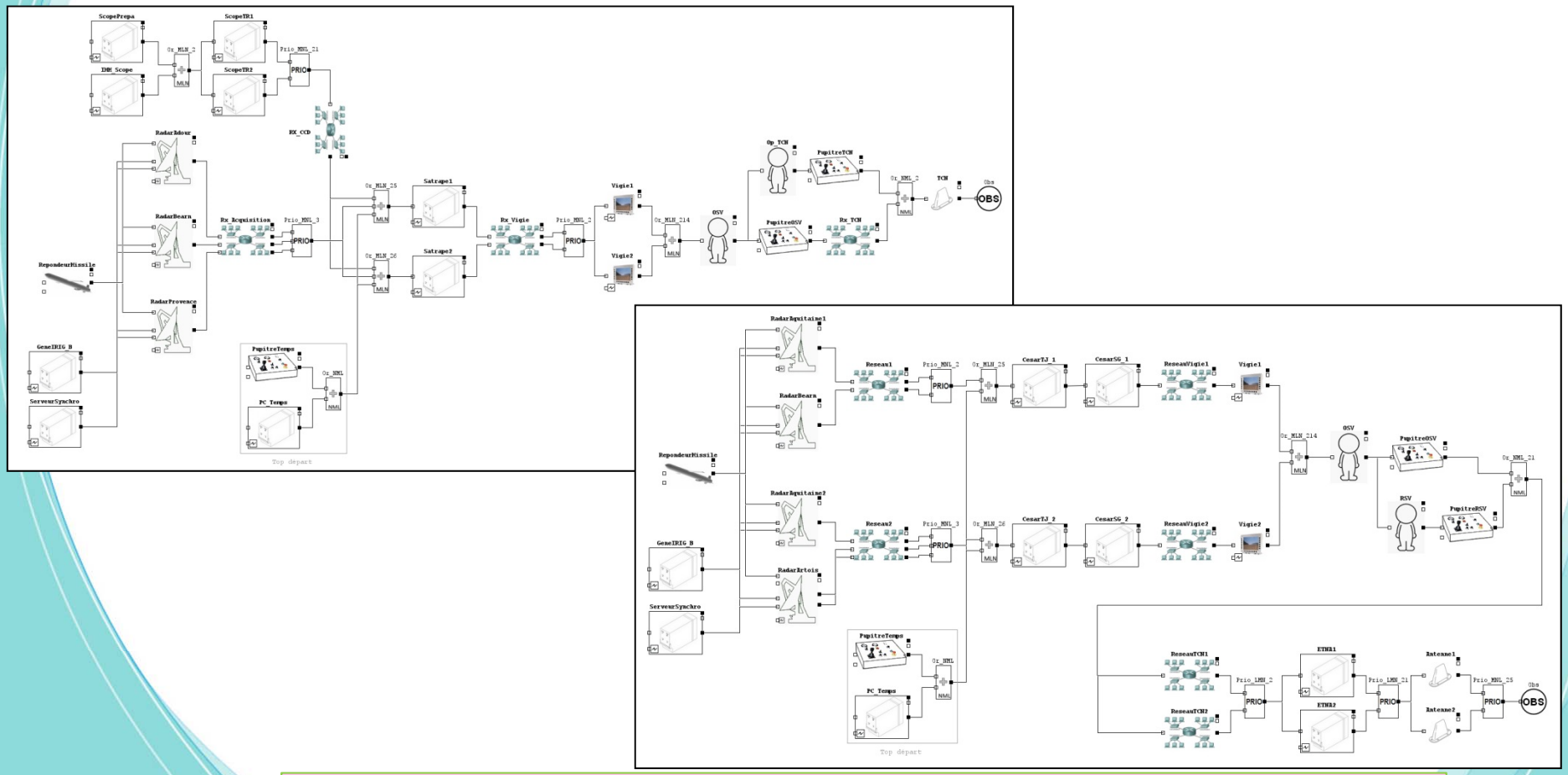
DetecBio (UM NBC)



- Incohérence dans les spécifications / exigences
- Incohérence entre les livrables techniques industriels

PLUS-VALUES ILLUSTRÉES

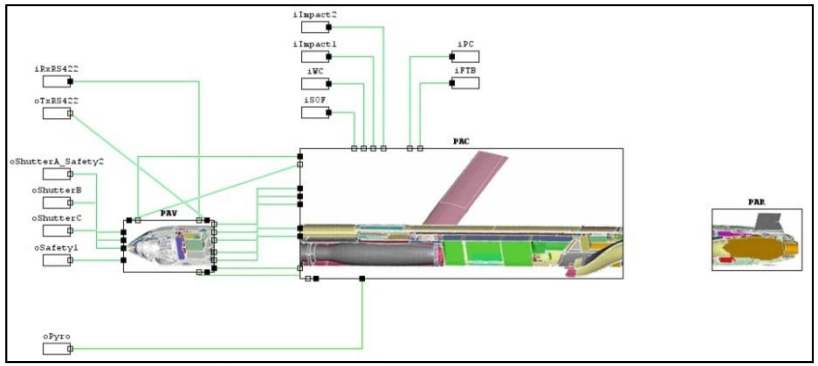
DGA EM – chaîne de sauvegarde

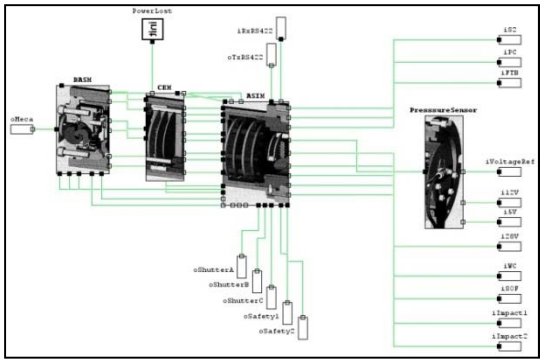


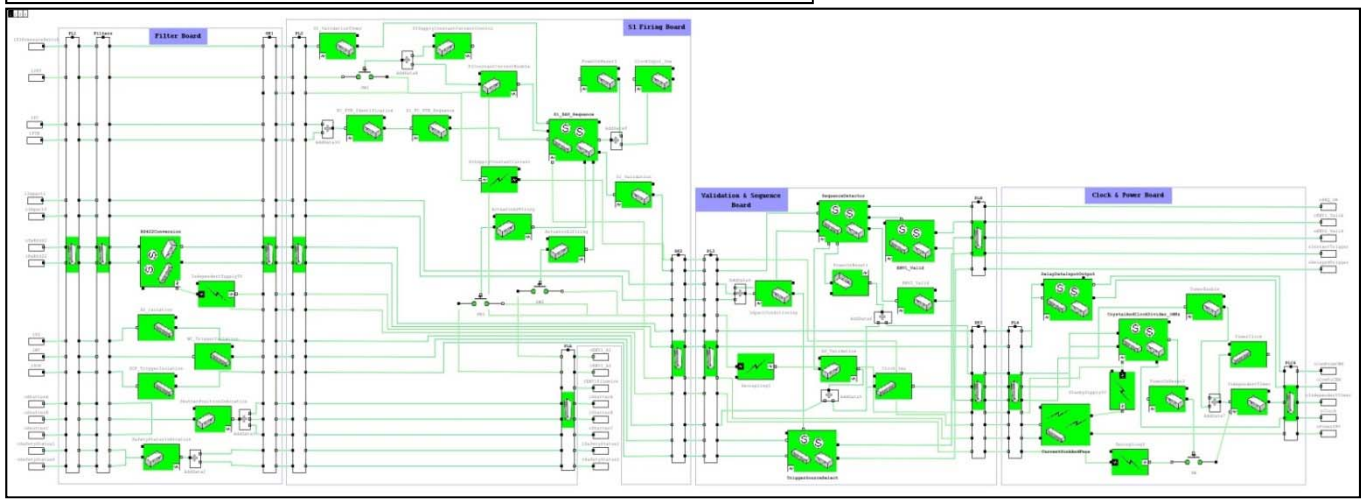
Comparaison des architectures: Ile du Levant vs Biscarrosse

PLUS-VALUES ILLUSTRÉES

MdCN – chaîne de sécurité du missile





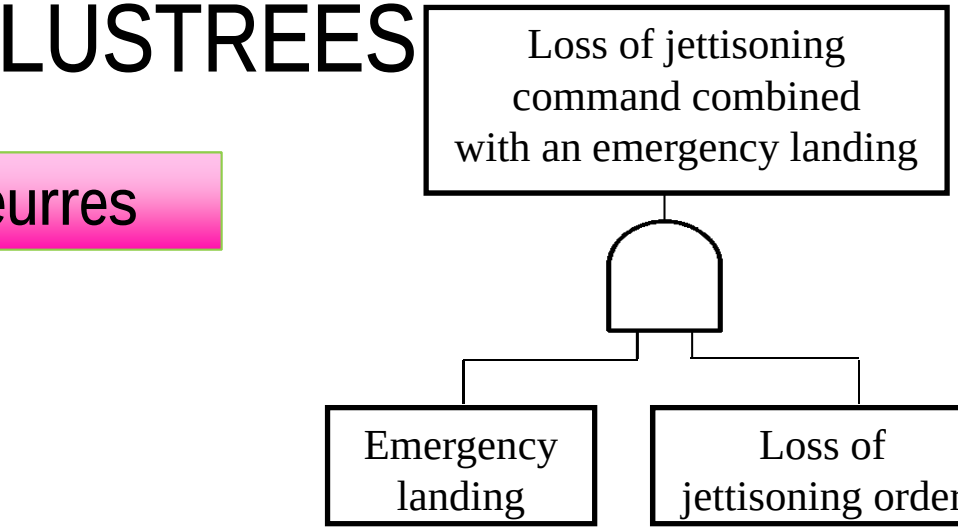


- Gain de temps : 56 lignes sur les 5000 de l'AMDEC
- Vérification de l'absence d'un mode commun de panne

PLUS-VALUES ILLUSTRÉES

Cougar – Système lance-leurres

Orientation des essais HIRF:
- zone à agresser
- fonction à surveiller



PLUS-VALUES ILLUSTRÉES

- Conclusion : objectifs atteints …
  - Vérifier la bonne allocation des DAL ✓ A400M
  - Vérifier l'absence de modes communs ✓ AF 447, MdCN
  - Vérifier l'analyse zonale ✓ Cougar
  - Orienter l'ingénierie de nos essais ✓ A400M, Cougar
  - Supporter les enquêtes après accident ✓ AF 447

- … et dépassés !
  - Compréhension du système AF 447
  - Incohérences documentaires Detec Bio
  - Comparaison d'architectures DGA EM

DGA

MINISTÈRE DES ARMÉES

SOMMAIRE

- Objectifs
- Approche DGA
  - Documents d'entrée
  - Principes de la modélisation
  - Simulation / Validation
  - Résultats
- Plus-values illustrées
- Perspectives

PERSPECTIVES

- Liens entre Ingénierie Système (MBSE*) et Safety (MBSA)
  - Ecosystème Industrie / Recherche : projet S2C de l'IRT
  - En interne (stages)
- Intégration du MBSA dans le processus de certification
  - Formation dispensée à 30 experts de l'EASA
  - Annexe dédiée dans la future ARP 4761 A
- Formations MBSA internes et externes
  - Sensibilisation : pour l'architecte
  - Perfectionnement : pour l'expert Safety

* MBSE Model Based System Engineering

QUESTIONS ?