

CONSTRUISONS **ENSEMBLE**
LA DÉFENSE DE DEMAIN

Modélisation dysfonctionnelle

des analyses de sécurité
dirigées par les modèles

Christophe FRAZZA
DGA TA/SIE



SOMMAIRE

- Définition et objectifs
- Principe
 - Modélisation
 - Simulation / Validation
 - Intégration multi systèmes
 - Analyses
- Plus-values illustrées
- Perspectives

DÉFINITION ET OBJECTIFS

Division SIE (Systèmes Informatiques Embarqués)

■ Mission

- Expertise en vue de la Certification et de la Qualification des systèmes et logiciels critiques

■ Activités

- 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 »
- Validation des analyses de sécurité (ARP 4754 & 4761)
 - Fonctionnelles (FHA)
 - Organiques (PSSA / SSA)
 - Zonales (ZHA)

DÉFINITION ET OBJECTIFS

■ Définition

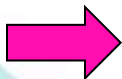
Modélisation dysfonctionnelle ou MBSA
(Model Based Safety Assessment)

=

Analyse de sécurité dirigée par les modèles

■ Objectifs principaux

- Vérifier la bonne allocation des DAL* (ARP 4754 A)
- Vérifier l'absence de modes communs
- Vérifier l'analyse zonale : feu, agression HIRF,...
- Orienter l'ingénierie de nos essais : « Safe path »
- Supporter les enquêtes après accident



Utiliser des modèles pour supporter nos expertises



SOMMAIRE

- Définition et objectifs
- Principe
 - Modélisation
 - Simulation / Validation
 - Intégration multi systèmes
 - Analyses
- Plus-values illustrées
- Perspectives

PRINCIPE

- Modélisation
- Simulation / Validation
- Intégration
- Analyses

Schéma d'architecture

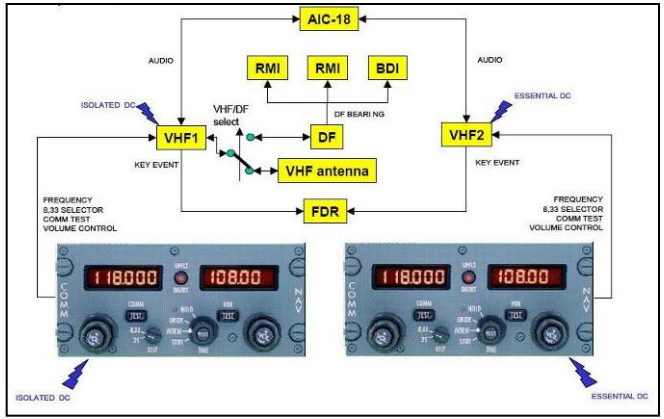
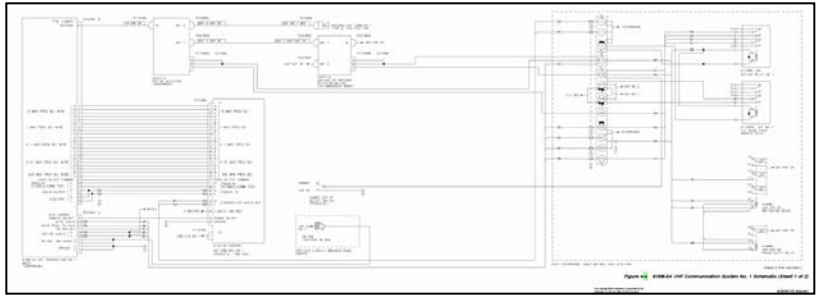


Schéma de câblage



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 NRA17 actuellement installées. Le TCAS utilisera 2 nouvelles antennes TCAS directionnelles.

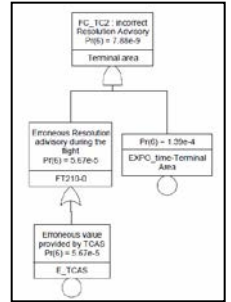
La modification proposée permet d'exploiter la capacité ELS (Surveillance Élémentaire) du TSC 2000.

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

Les règlements 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.



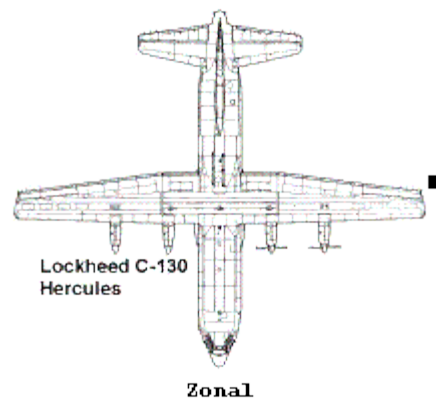
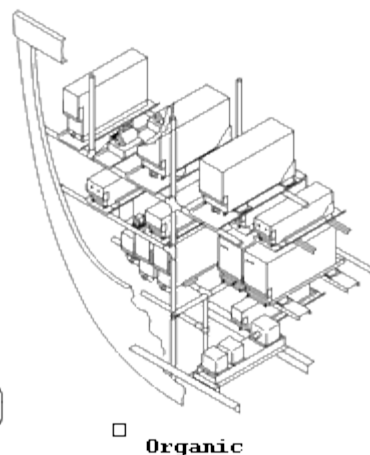
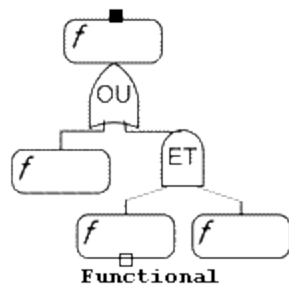
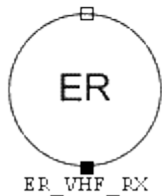
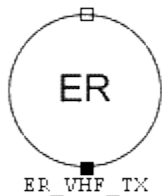
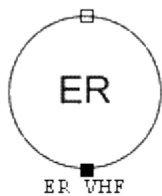
Analyses de sécurité



PRINCIPE

- Modélisation
- Simulation / Validation
- Intégration
- Analyses

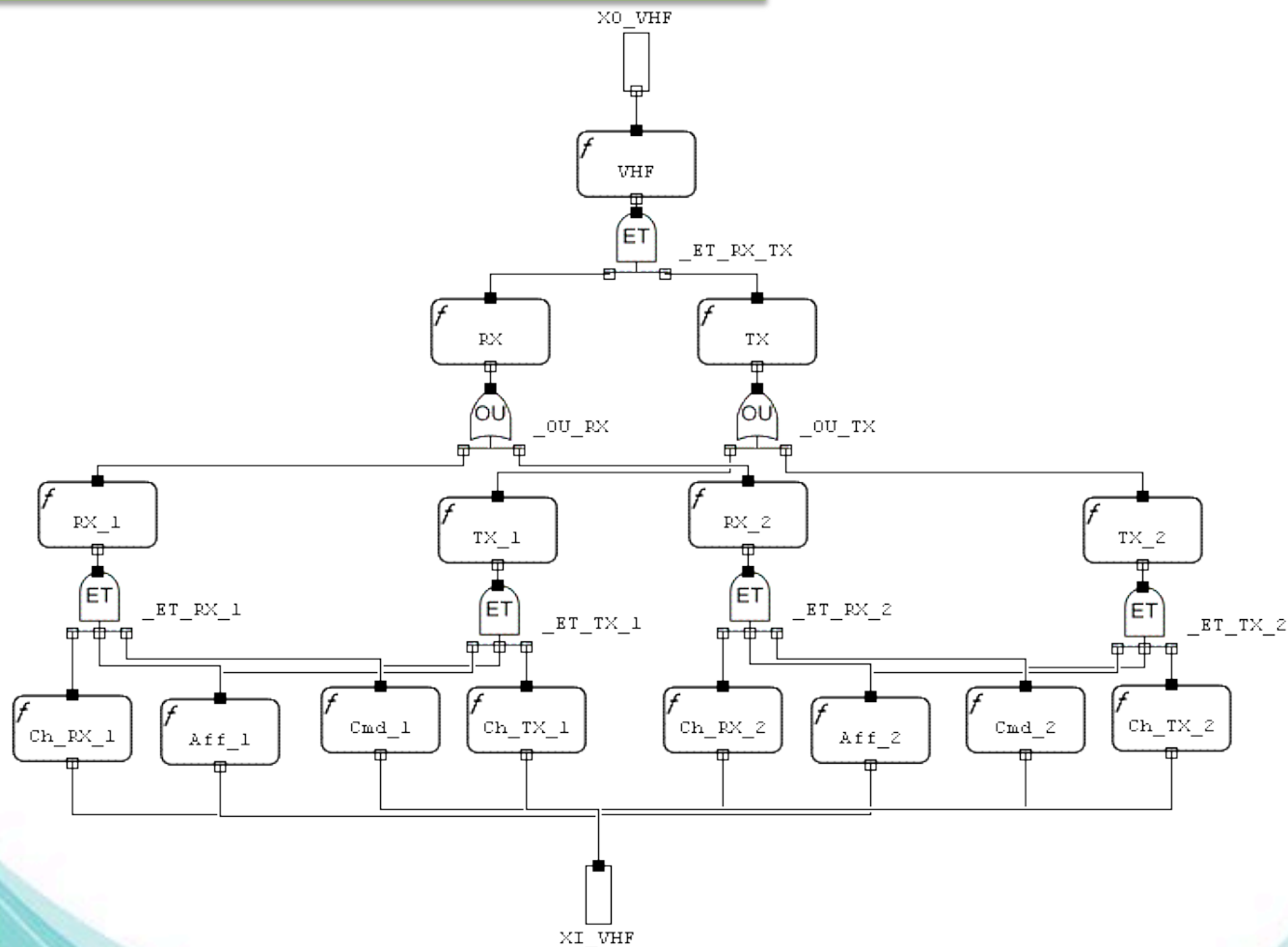
Méta modèle



PRINCIPE

- Modélisation
- Simulation / Validation
- Intégration
- Analyses

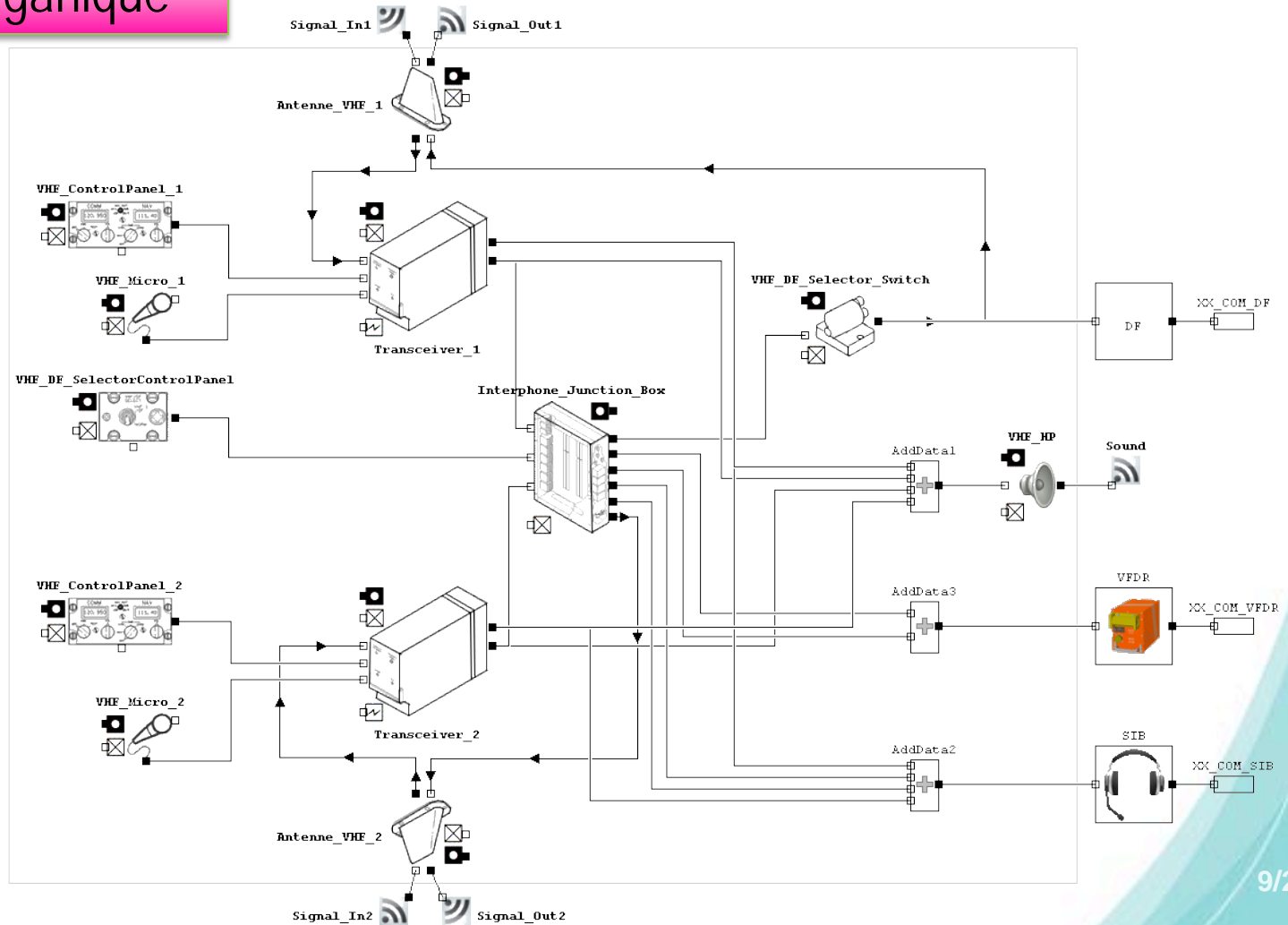
Vue fonctionnelle hiérarchique



PRINCIPE

- Modélisation
- Simulation / Validation
- Intégration
- Analyses

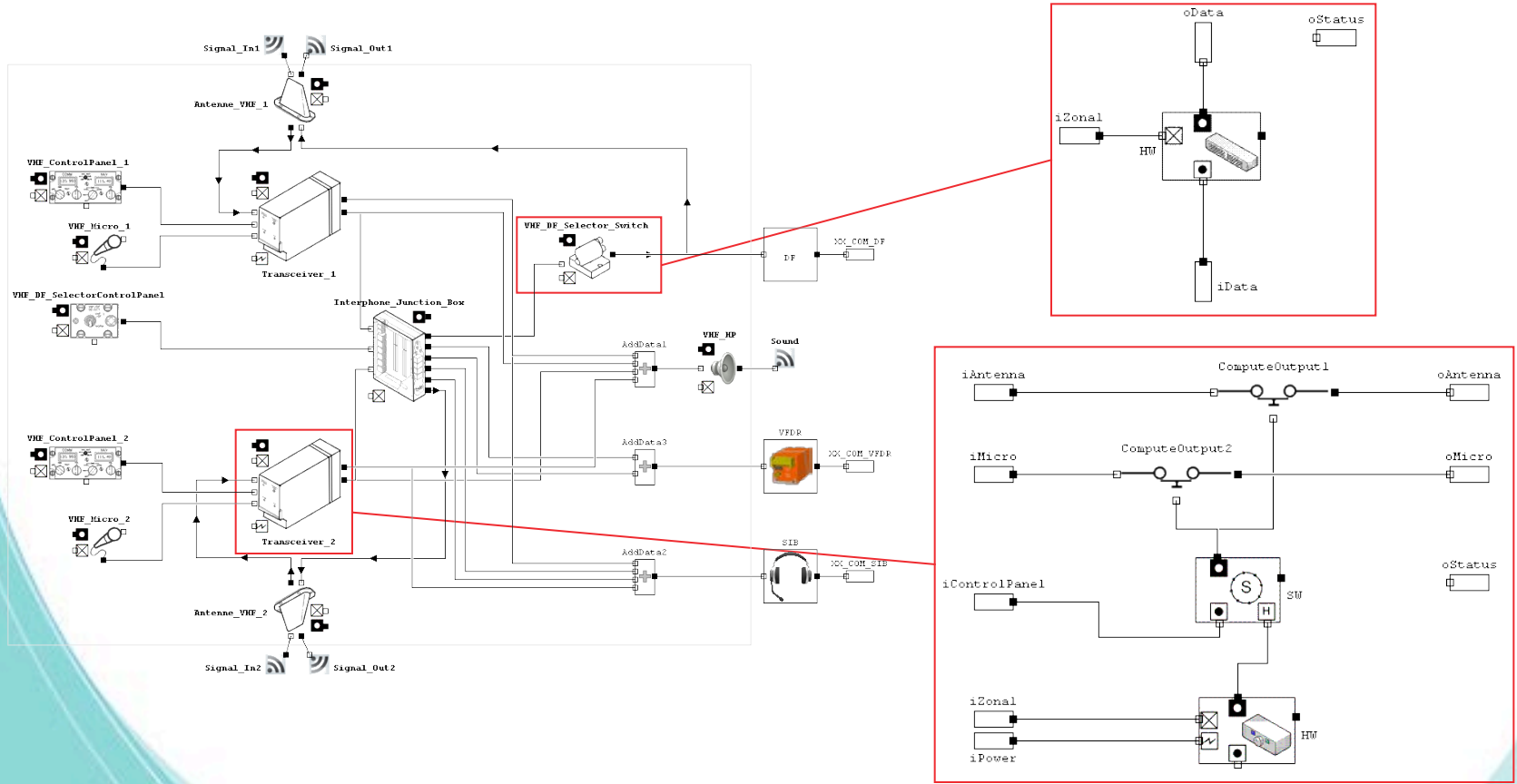
Vue organique



PRINCIPE

- Modélisation
- Simulation / Validation
- Intégration
- Analyses

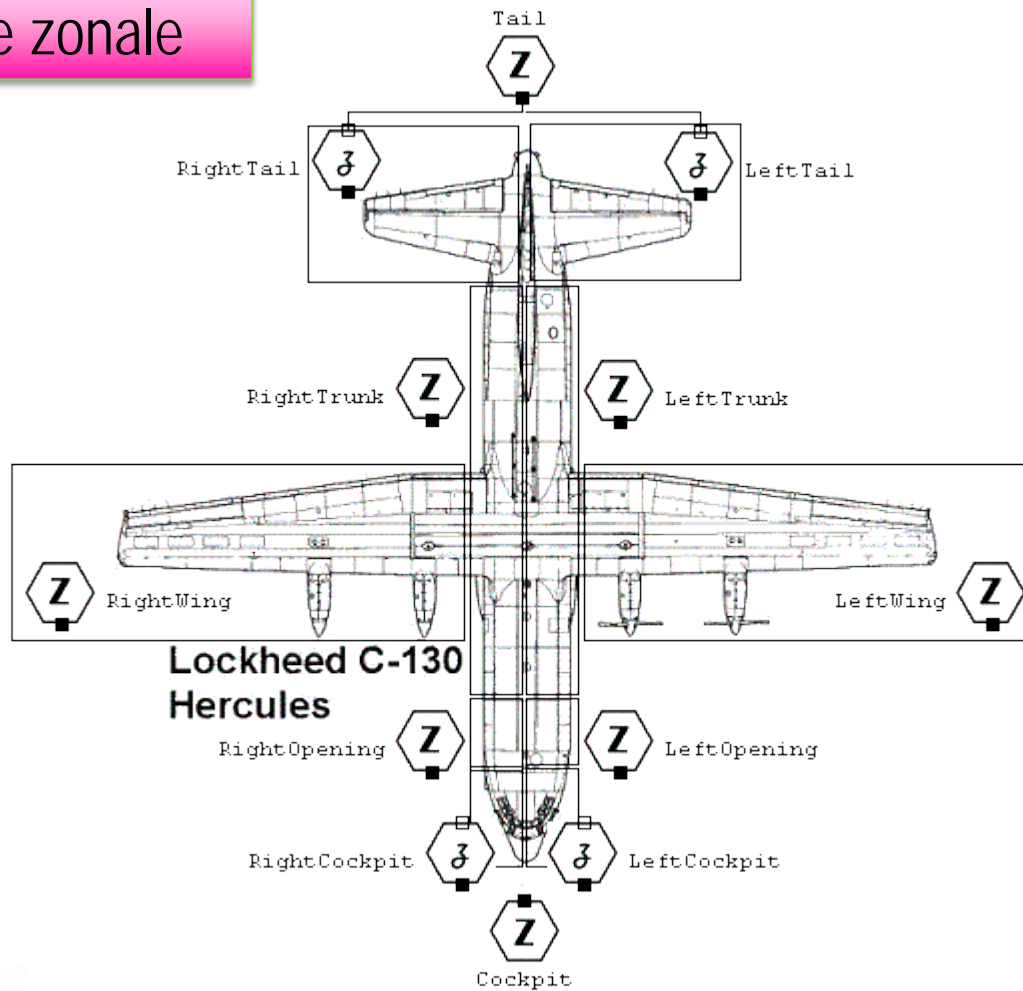
Vue organique



PRINCIPE

- Modélisation
- Simulation / Validation
- Intégration
- Analyses

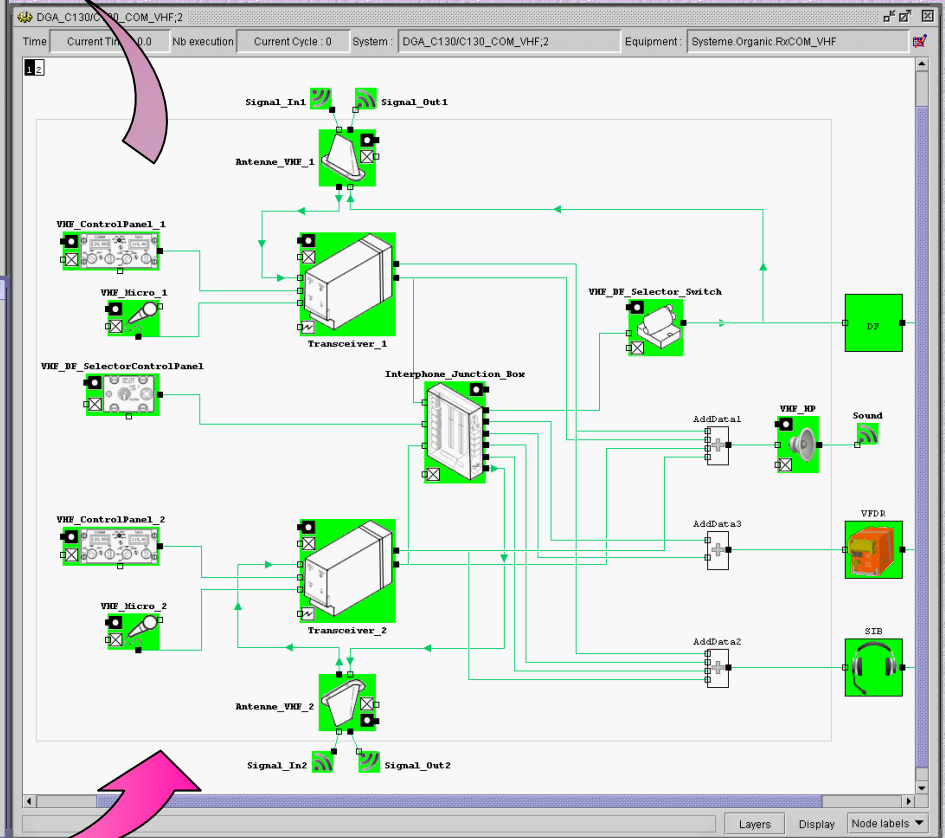
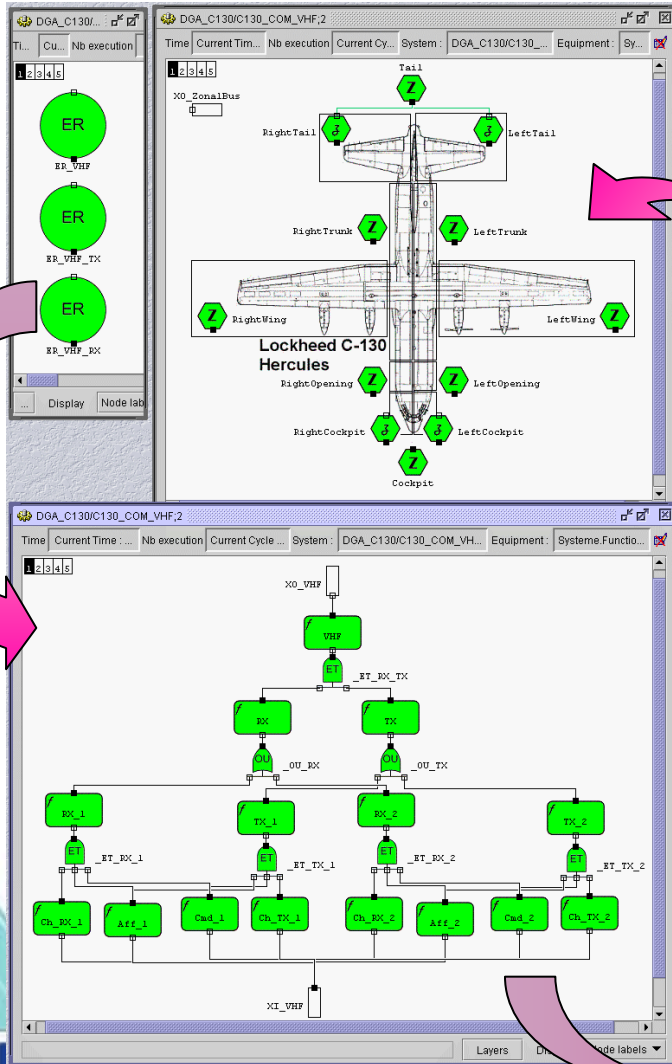
Vue zonale



PRINCIPE

- Modélisation
- Simulation / Validation
- Intégration
- Analyses

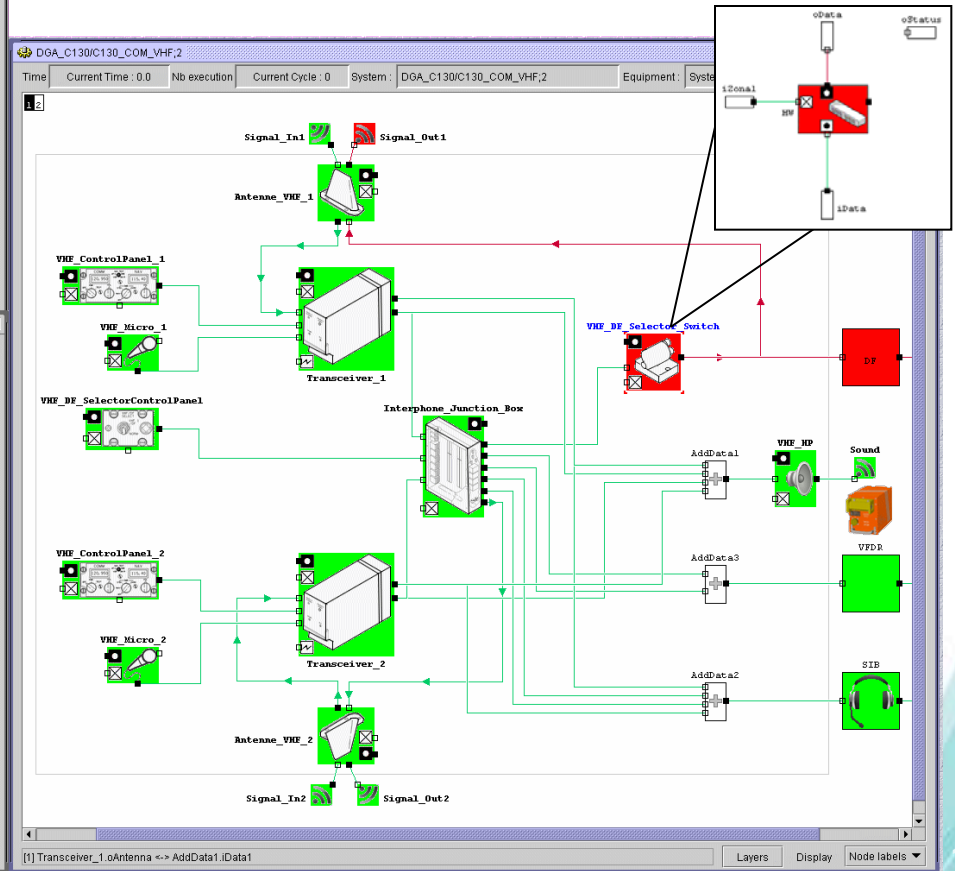
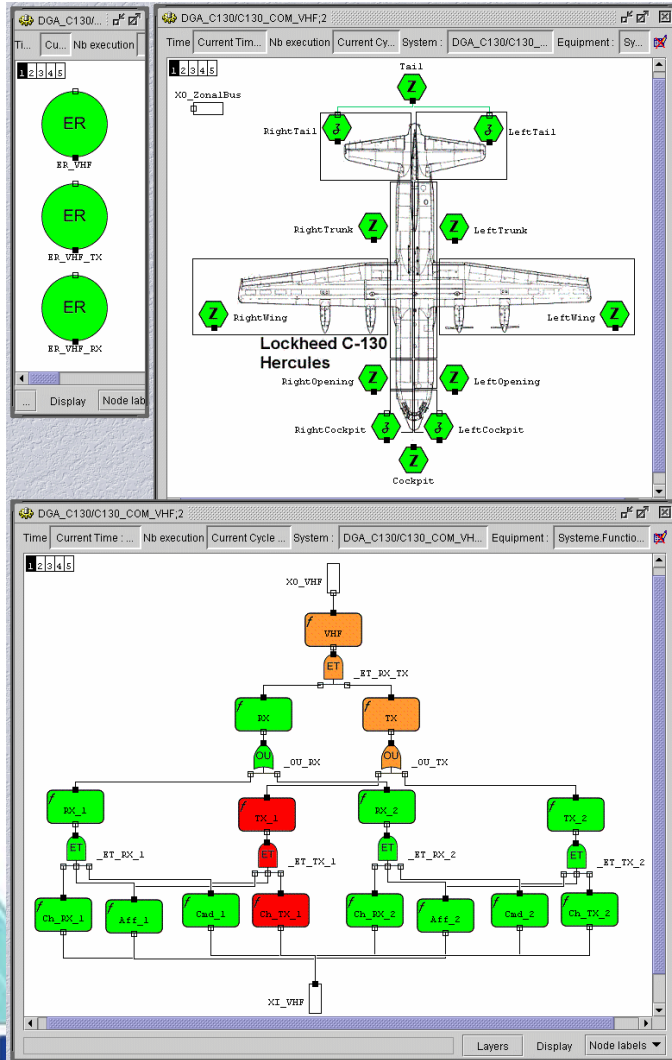
Etat nominal



PRINCIPE

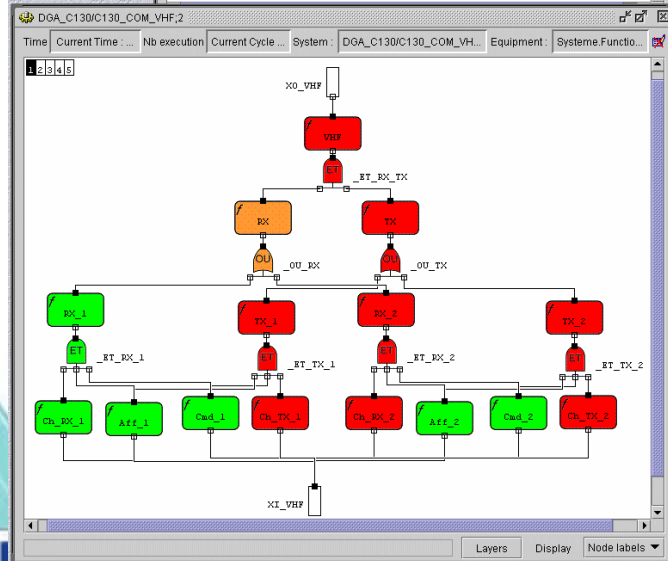
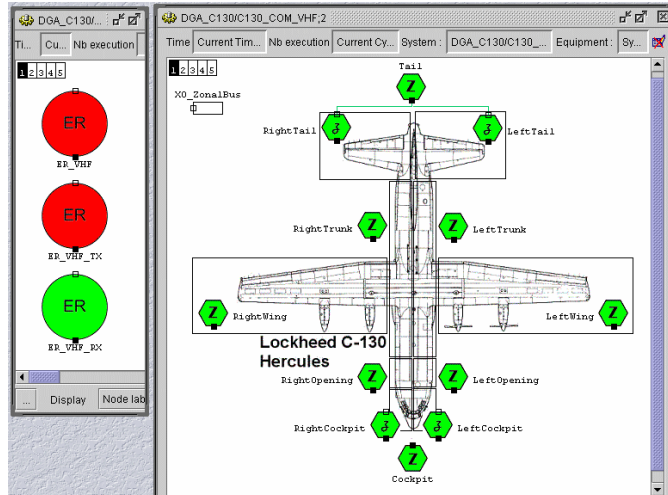
- Modélisation
- Simulation / Validation
- Intégration
- Analyses

Panne HW

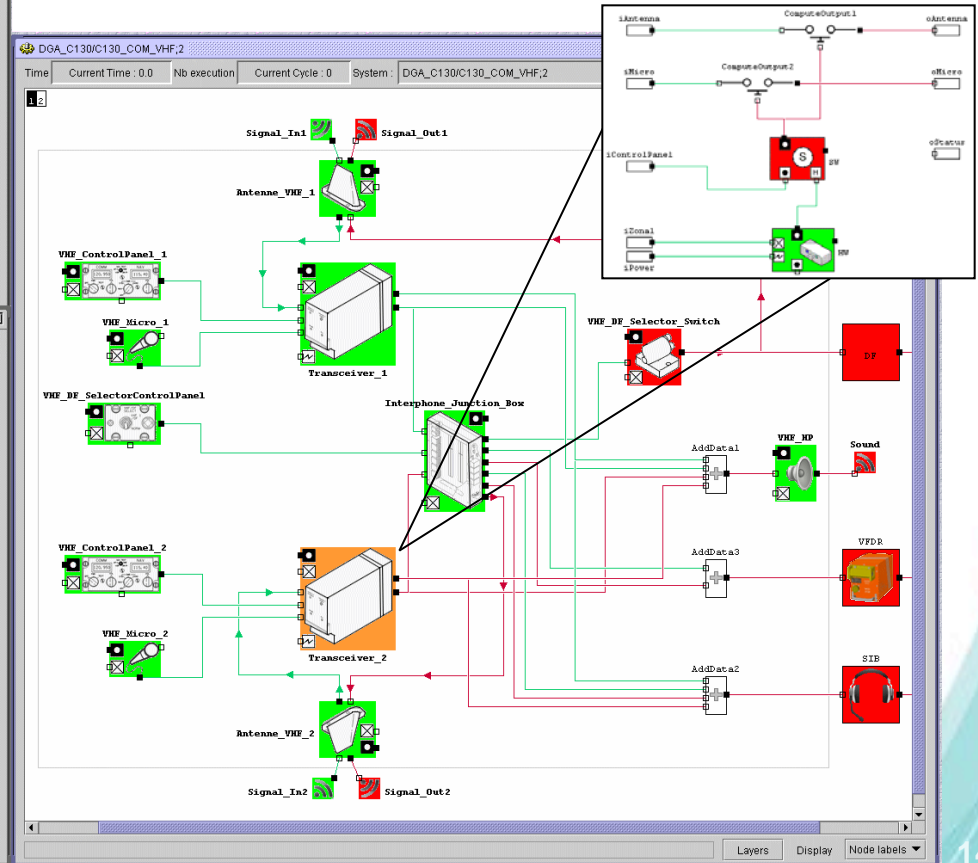


PRINCIPE

- Modélisation
- Simulation / Validation
- Intégration
- Analyses



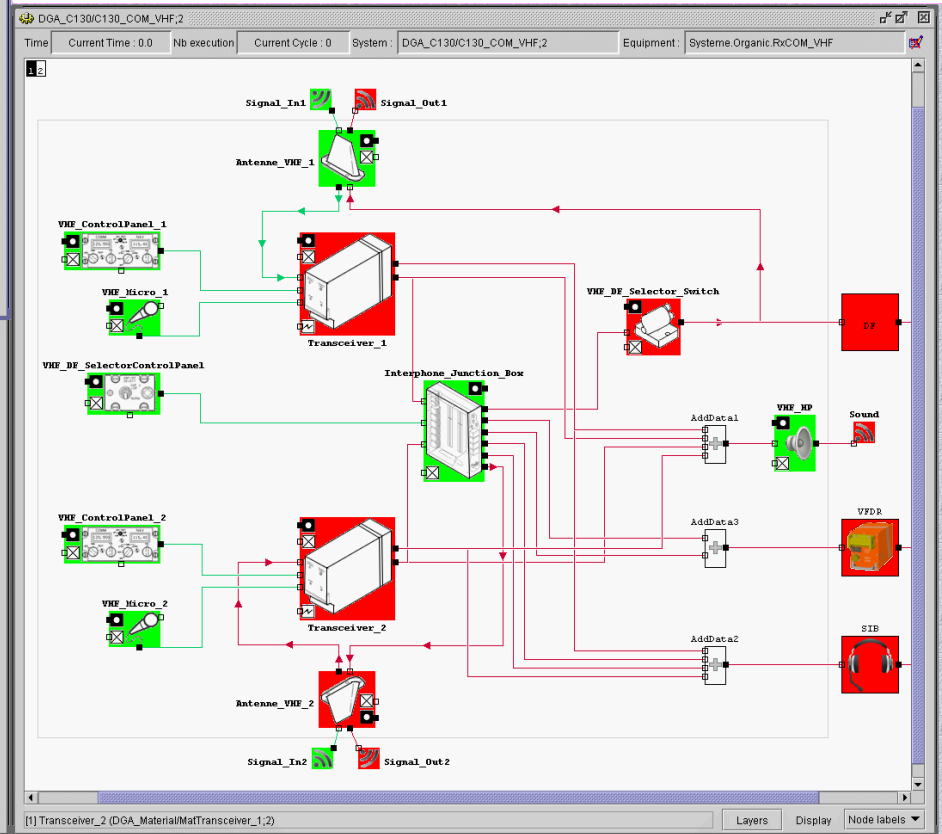
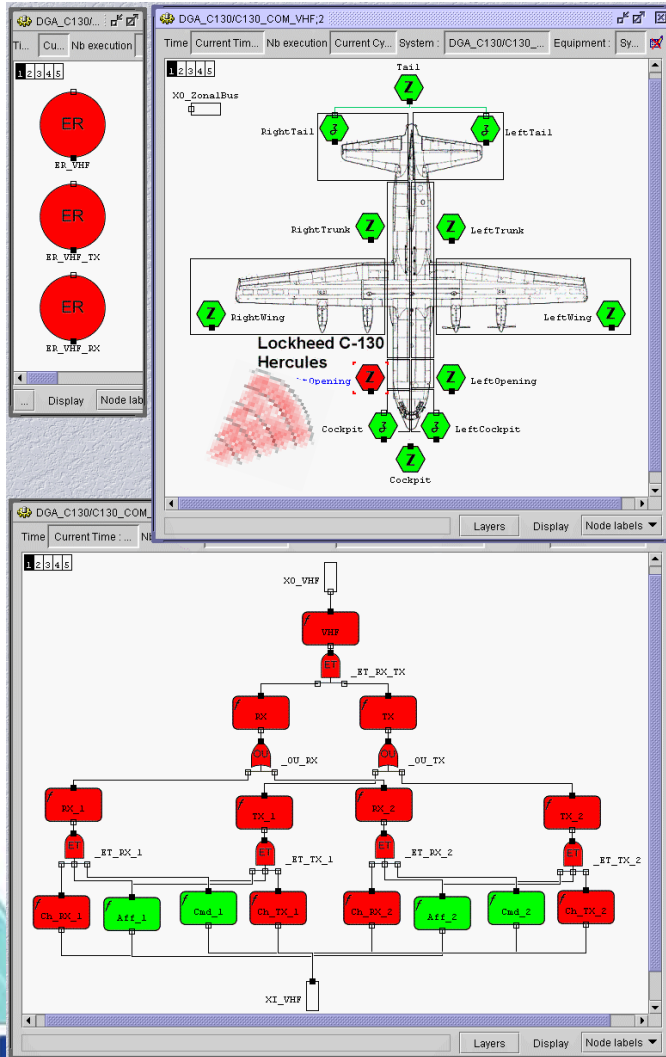
+ Erreur SW



PRINCIPE

- Modélisation
- Simulation / Validation
- Intégration
- Analyses

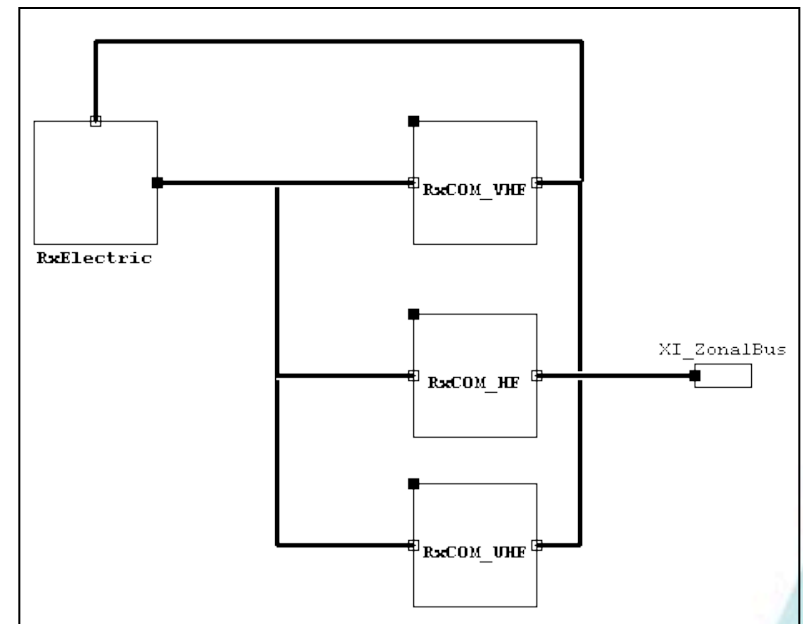
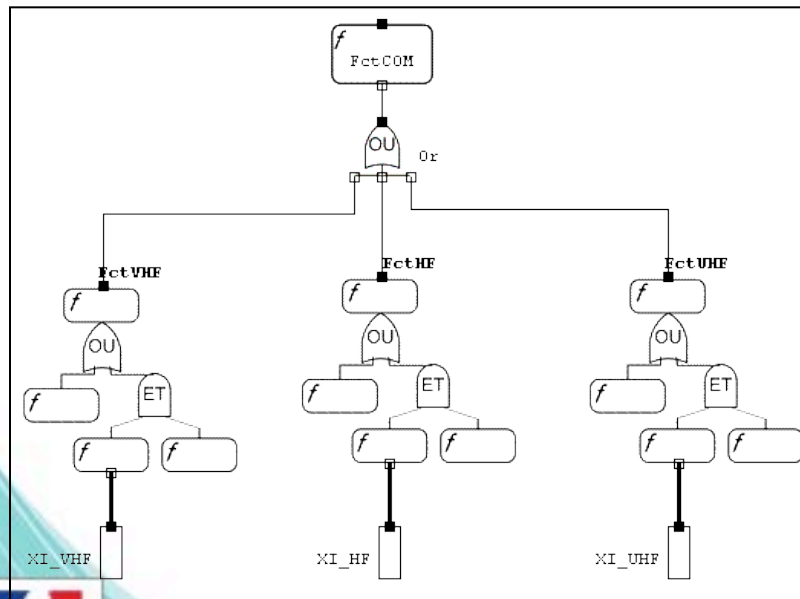
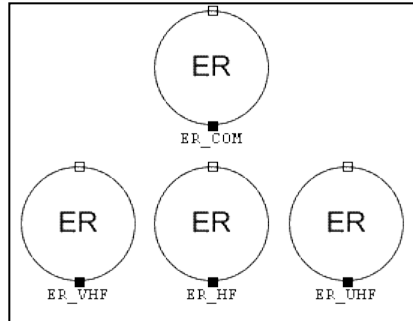
Agression HIRF



PRINCIPE

- Modélisation
- Simulation / Validation
- Intégration
- Analyses

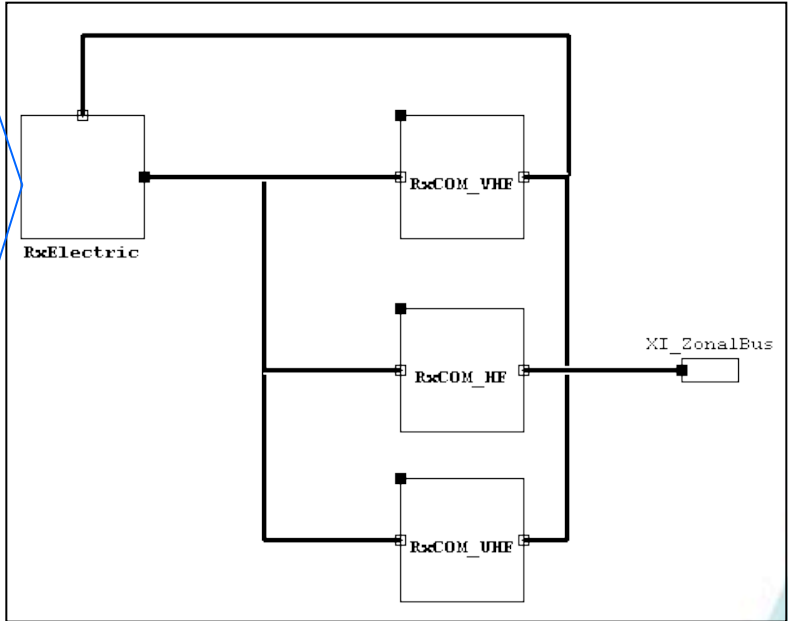
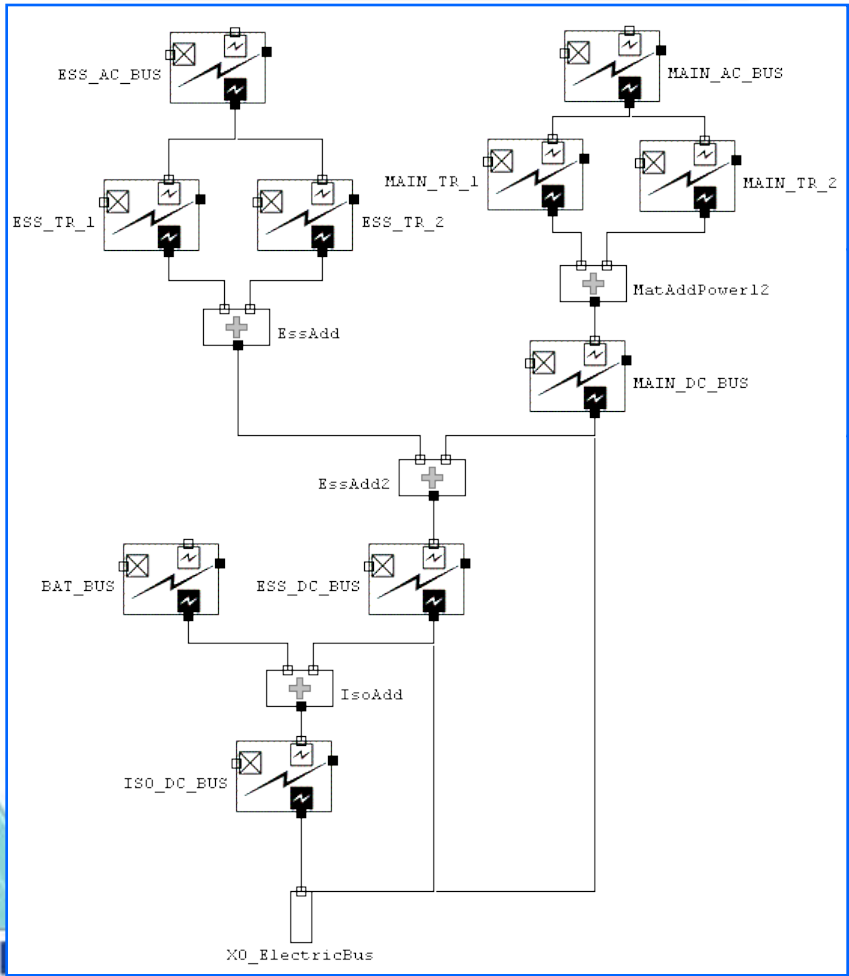
Fonction Communication : VHF + HF + UHF ...



PRINCIPE

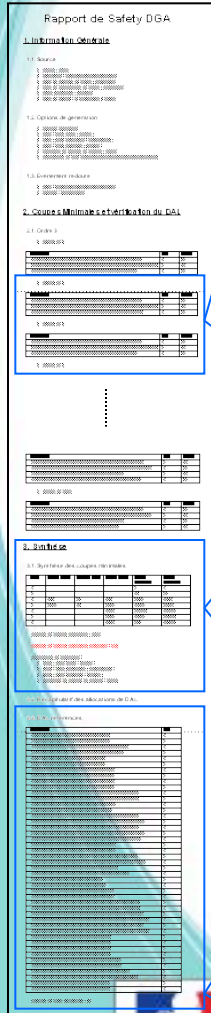
- Modélisation
- Simulation / Validation
- Intégration
- Analyses

... + réseau électrique



PRINCIPE

- Modélisation
- Simulation / Validation
- Intégration
- Analyses



• Coupe n° 56

Evénement	DAL	Check
SysCOM.Organic.RxCOM_VHF.synchro_SW_eMisleading_TransceiverVHF	B	OK
SysCOM.Organic.RxCOM_UHF.UHF_HP.HW_eFailure	B	OK
SysCOM.Organic.RxCOM_HF.synchro_HW_eMisleading_TransceiverHF	A	OK

• 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

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

Rapport SdF :

- Production exhaustive des Functional Failure Sets

= coupes minimales
+ erreurs de développement (SW & HW)

- Pour le moment, pas d'analyse sur les arbres de défaillances (calcul probabilistique)

SOMMAIRE

- Définition et objectifs
- Principe
 - Modélisation
 - Simulation / Validation
 - Intégration multi systèmes
 - Analyses
- **Plus-values illustrées**
- Perspectives

PLUS-VALUES ILLUSTRÉES

A400M – Cargo Handling System

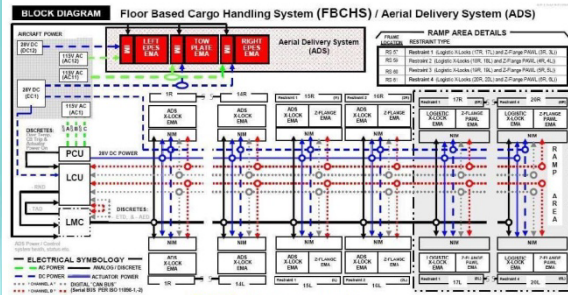
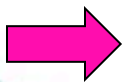
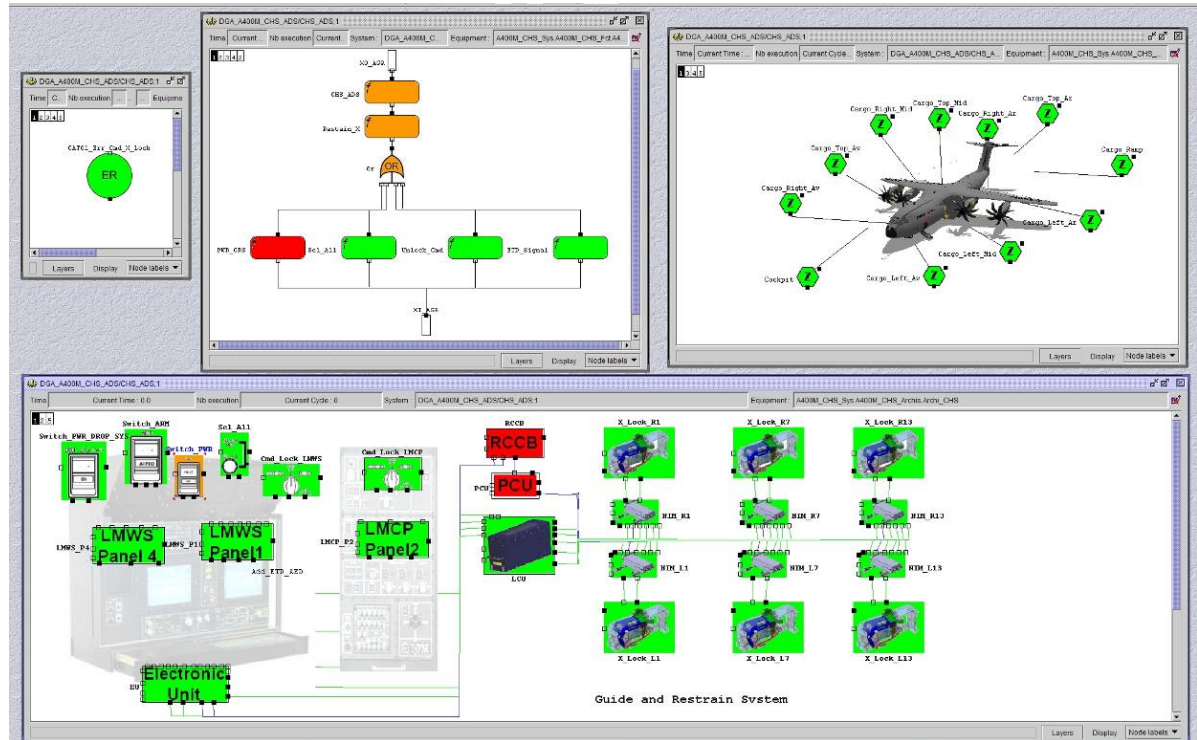
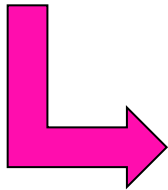


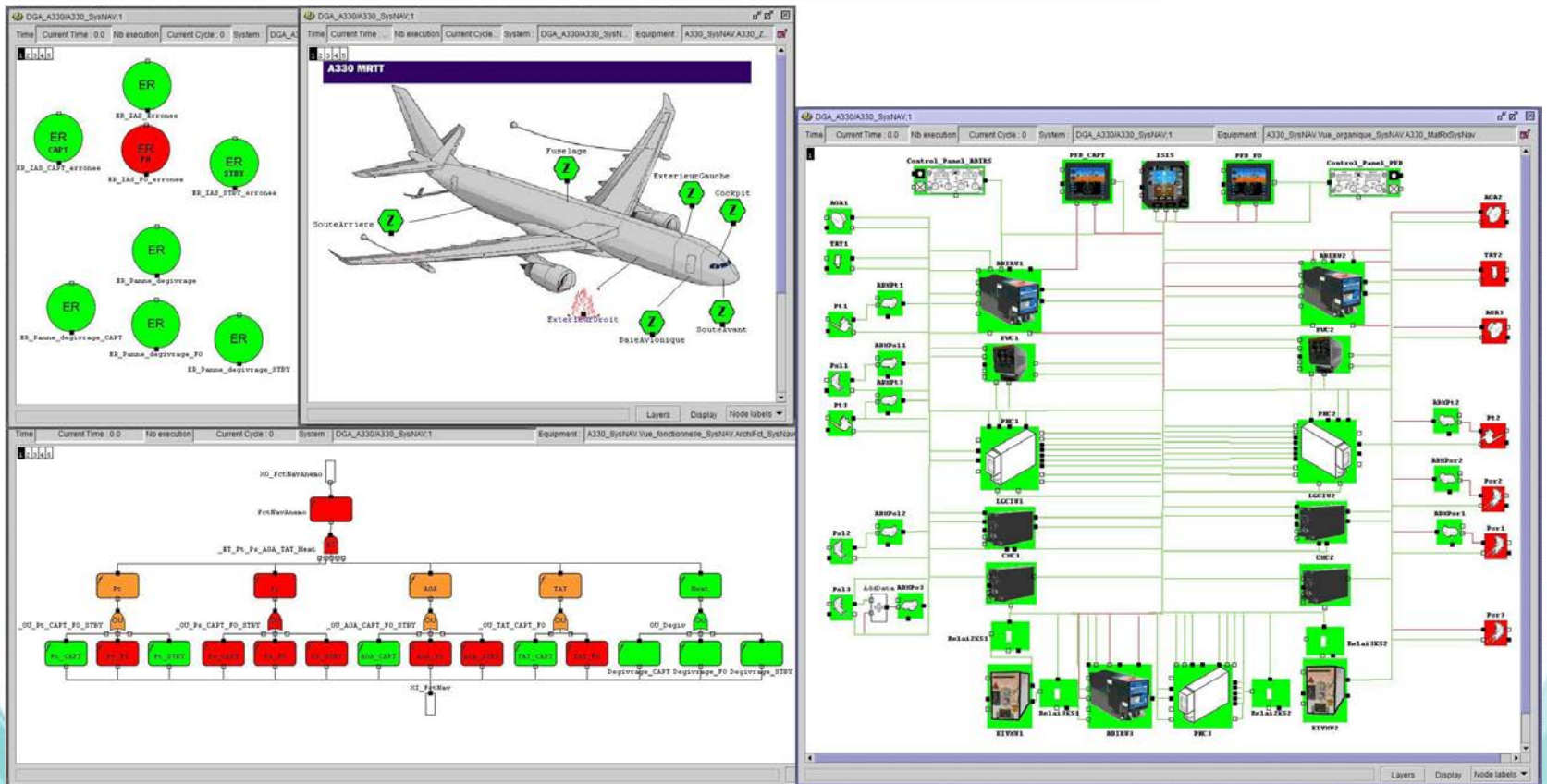
Schéma fonctionnel



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

PLUS-VALUES ILLUSTRÉES

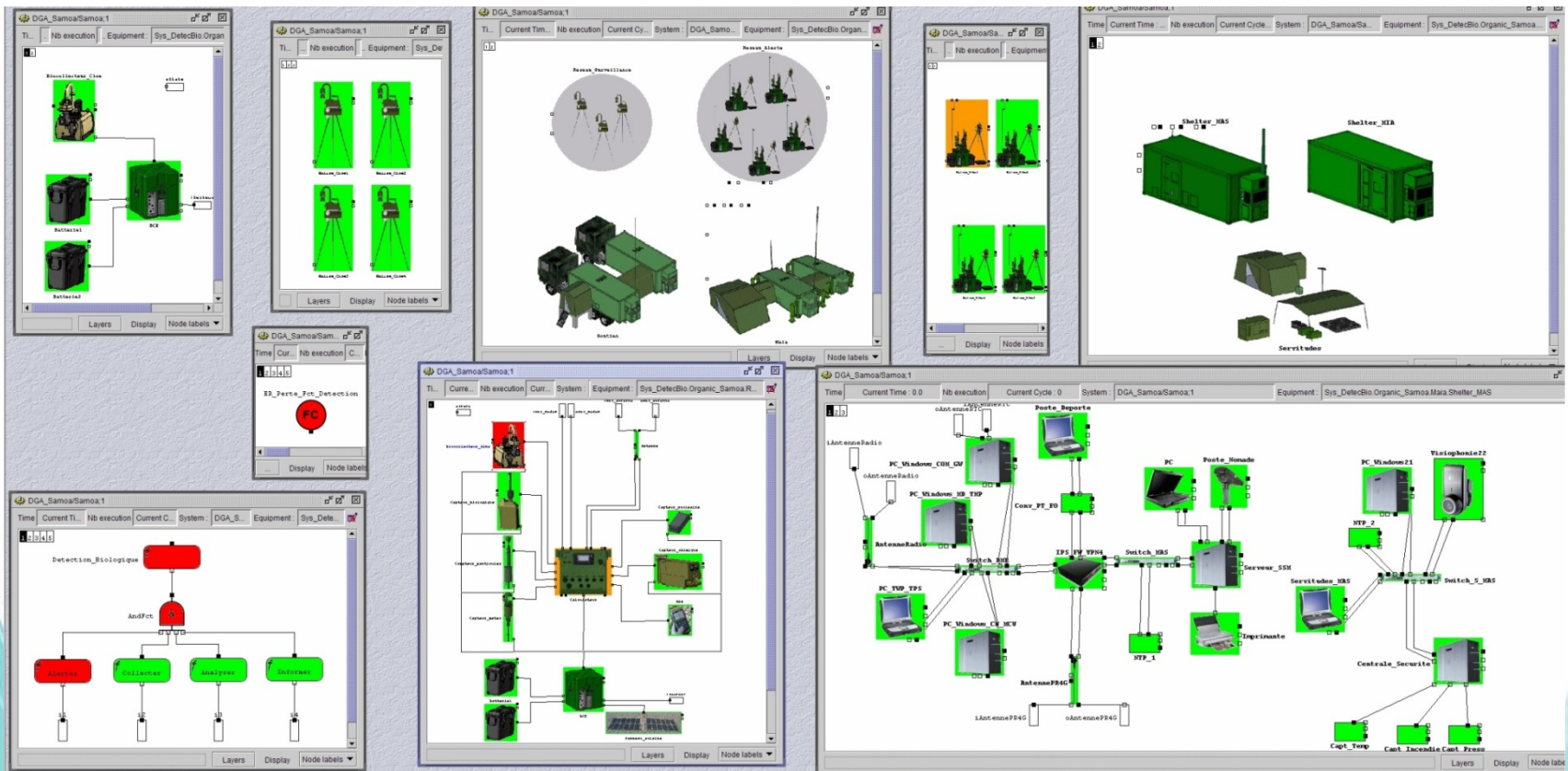
AF447 – Système de réchauffage des sondes



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

PLUS-VALUES ILLUSTRÉES

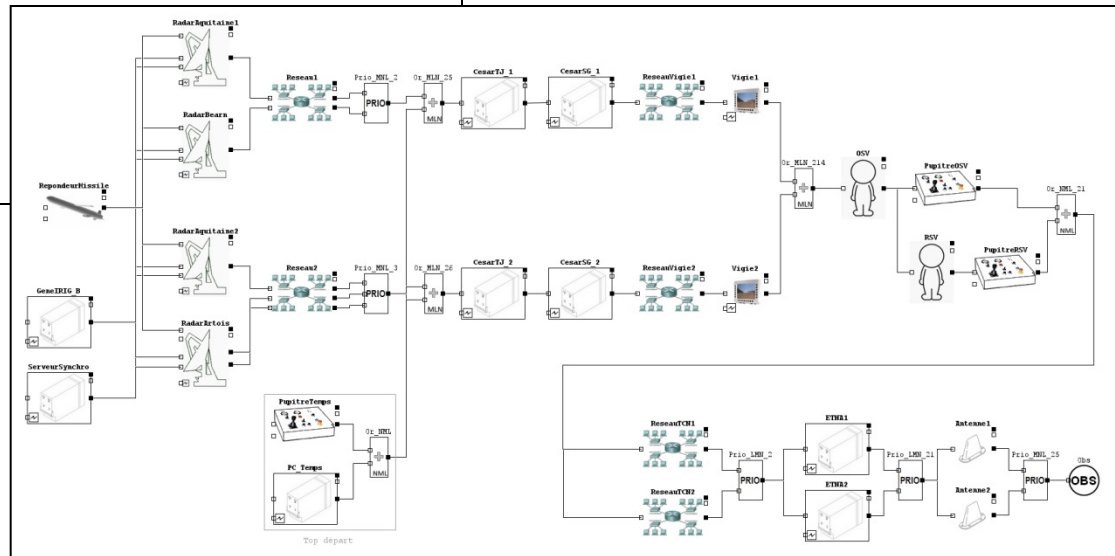
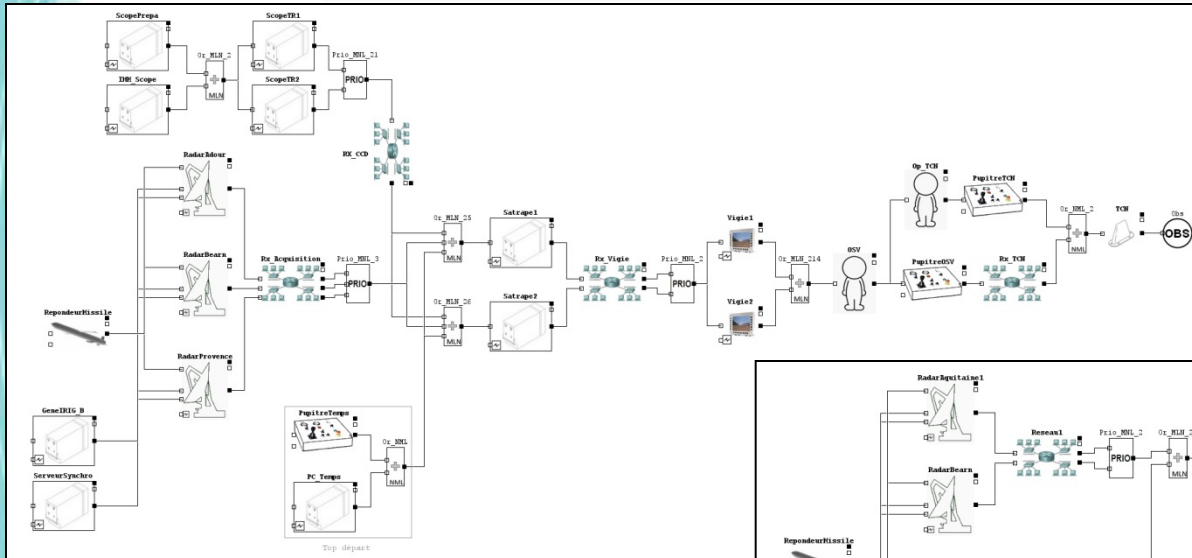
DetecBio (UM NBC)



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

PLUS-VALUES ILLUSTRÉES

DGA EM – chaîne de sauvegarde

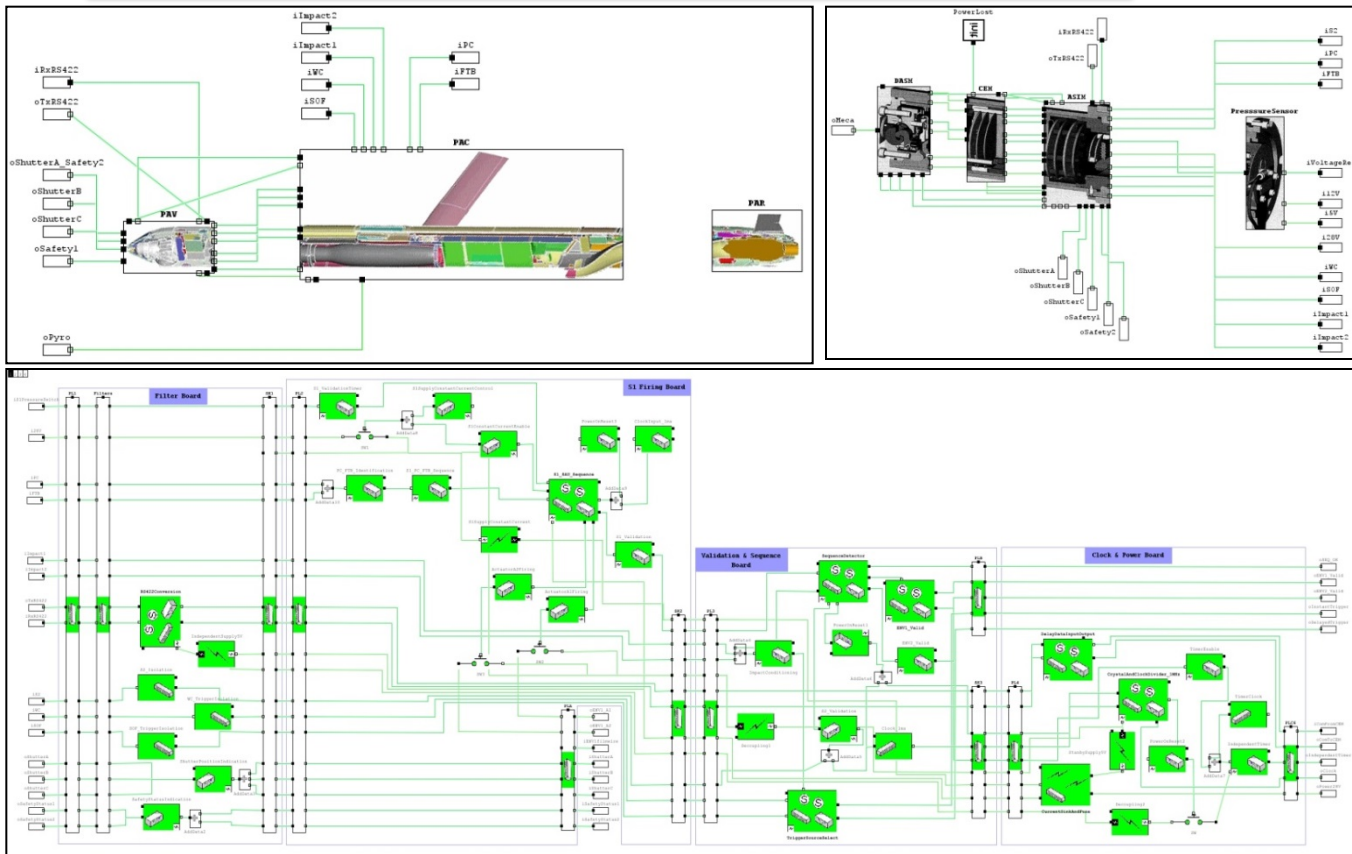


Comparaison des architectures: Ile du Levant vs Biscarrosse



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

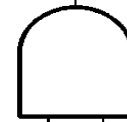
Cougar – Système lance-leurres



Orientation des essais HIRF:

- zone à agresser
- fonction à surveiller

Loss of jettisoning command combined with an emergency landing








Emergency landing

Loss of jettisoning order



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

SOMMAIRE

- Définition et objectifs
- Principe
 - Modélisation
 - Simulation / Validation
 - Intégration multi systèmes
 - Analyses
- Plus-values illustrées
- Perspectives

PERSPECTIVES

- Liens entre Ingénierie Système (MBSE) et Safety (MBSA)
 - En interne (stages)
 - Ecosystème Industrie / Recherche
- Modélisations à venir
 - Concepts d'opérations de drones (ONERA)
 - FCAS (Future Combat Air System)
 - FTI (Frégate de Taille Intermédiaire)
- Formations MBSA interne et externe
 - Légère : pour l'architecte
 - Lourde : pour l'expert Safety

QUESTIONS ?

