 THE RESEARCH LEADING TO THESE RESULTS HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S SEVENTH FRAMEWORK PROGRAM (FP7/2007-2013) FOR CRYSTAL – CRITICAL SYSTEM ENGINEERING ACCELERATION JOINT UNDERTAKING UNDER GRANT AGREEMENT N° 332830 AND FROM SPECIFIC NATIONAL PROGRAMS AND / OR FUNDING AUTHORITIES.

CRitical S**YST**em Engineering **A**cce**L**eration

Use Case Demonstrator
Airbus-Germany
Environmental Control Systems
D201.021

DOCUMENT INFORMATION

Project	CRYSTAL
Grant Agreement No.	ARTEMIS-2012-1-332830
Deliverable Title	Environmental Control Systems
Deliverable No.	D201.021
Dissemination Level	CO
Nature	D
Document Version	V1.0
Date	2014-01-29
Contact	Dietmar Sander
Organization	A-G
Phone	+49 40 743 64199
E-Mail	dietmar.sander@airbus.com

AUTHORS TABLE

Name	Company	E-Mail
Dietmar Sander	Airbus Operations GmbH	dietmar.sander@airbus.com
Arne Rosenbohm	Airbus Operations GmbH	arne.rosenbohm@airbus.com
Mathias Maruhn	Airbus Operations GmbH	mathias.maruhn@airbus.com

REVIEW TABLE

Version	Date	Reviewer
0.1	24.1.2014	Andreas Mitschke – Airbus Group Innovations
0.1	24.1.2014	Thomas Kuhn – Fraunhofer IESE

CHANGE HISTORY

Version	Date	Reason for Change	Pages Affected
0.1	20.1.2014	Initial Description	all
1.0	28.1.2014	First Version after review	all

CONTENT

1 Introduction

1.1 Role of deliverable

This document has the following major purposes:

- Describe the technical status of the model based approach for the ECS Use Case
  - Provide model descriptions and feedback of the contributed domains
  - Provide dedicated model entities and feedback relevant for interoperability constraints and/or underlying framework
  - Provide assessment of supported engineering methods
- Provide input to WP601 (IOS Development) required to derive specific IOS-related requirements
- Provide input to WP602 (Platform Builder) required to derive adequate meta models
- Establish the technology baseline with respect to the use-case, and the expected progress beyond (existing functionalities vs. functionalities that are expected to be developed in CRYSTAL)

1.2 Relationship to other CRYSTAL Documents

The ECS Use Case Demonstrator describes the developed methods and tools their assessment during the use case experimentation towards the CRYSTAL consortium. The description is linked to the ECS Use Case description D2.1.1.1 which provides the technical context of the system to be designed by model based methods with interoperable link to model based safety analysis.

The document is also linked to the chapter 10 of Safety for Avionic Design and Analysis Framework supported by Airbus Group Innovations with dedicated implementations and method evaluations.

1.3 Structure of this document

The ECS Use Case Demonstrator description is structured in three main sections – status of the tool-chain and interoperability support with dedicated implementation, evolutions of the design and safety models performing towards the use case objectives and assessment of the supported engineering methods.

2 Envisaged Tool-Chain Overview

The Figure 1 below provides a first draft overview of the envisaged Avionic Design and Analysis Framework. The approach is extracted from chapter 10 of CRYSTAL deliverable D604.011 – Specification, Development and Assessment for Safety Engineering – V1. The framework is based mainly on input provided by the Airbus Environmental Control System Use Case. The core part of the framework is dedicated to the integration of safety and design models managed by Simulink. The Simulink Design Verifier will be used for analysis purposes. The framework will also include a dedicated tool that allows triggering of fault injections and visualization of safety analysis results. It is expected to later extend the framework to other tools such as Isograph FT+, IBM Doors, or Airbus internal tools for Particular Risk Analysis.
The connections between the different tools involved in this framework shall be based on the CRYSTAL IOS.

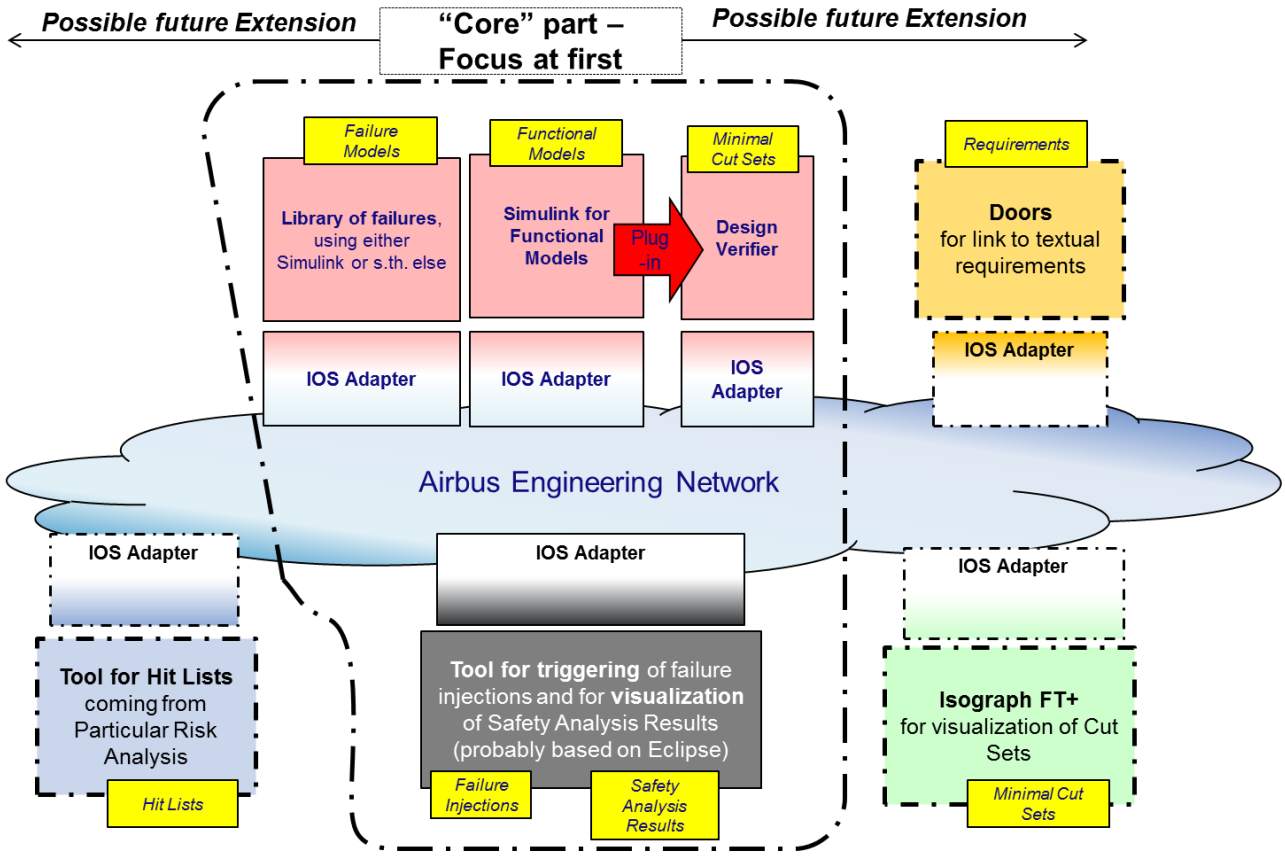

Figure 1 Avionic Design and Analysis Framework

The Safety framework for Avionic Design and Analysis is currently driven mainly by the Use Case 2.1a – Airbus Environmental Control Systems.
It is expected to extend the framework such that it can also support the Use Case 2.1b – Airbus Simulation for Particular Risk Analysis, and Use Case 2.1c – Airbus Fuel Management Risk Analysis.
The definition of the core part of framework is tightly linked to the definition of the SEE of the Airbus Environmental Control System Use Case as described in the deliverable D2.1.1.1-1.

3 MBSE in VCS Use Case Demonstrator

Currently, functional models are developed in Matlab/Simulink for design verification and requirement validation by simulation. Additional safety requirements are modelled as observers as an integral part of the design model in order to apply the dedicated Simulink Verification Module 'Design Verifier'. Due to the restricting nature of the Design Verifier to a number of Simulink blocks, the model has been simplified by reduced SimScape blocks to model pneumatic equipment. Feedback of control loops has been also omitted as first order assumptions since only few monitors are providing signals back to the controller.

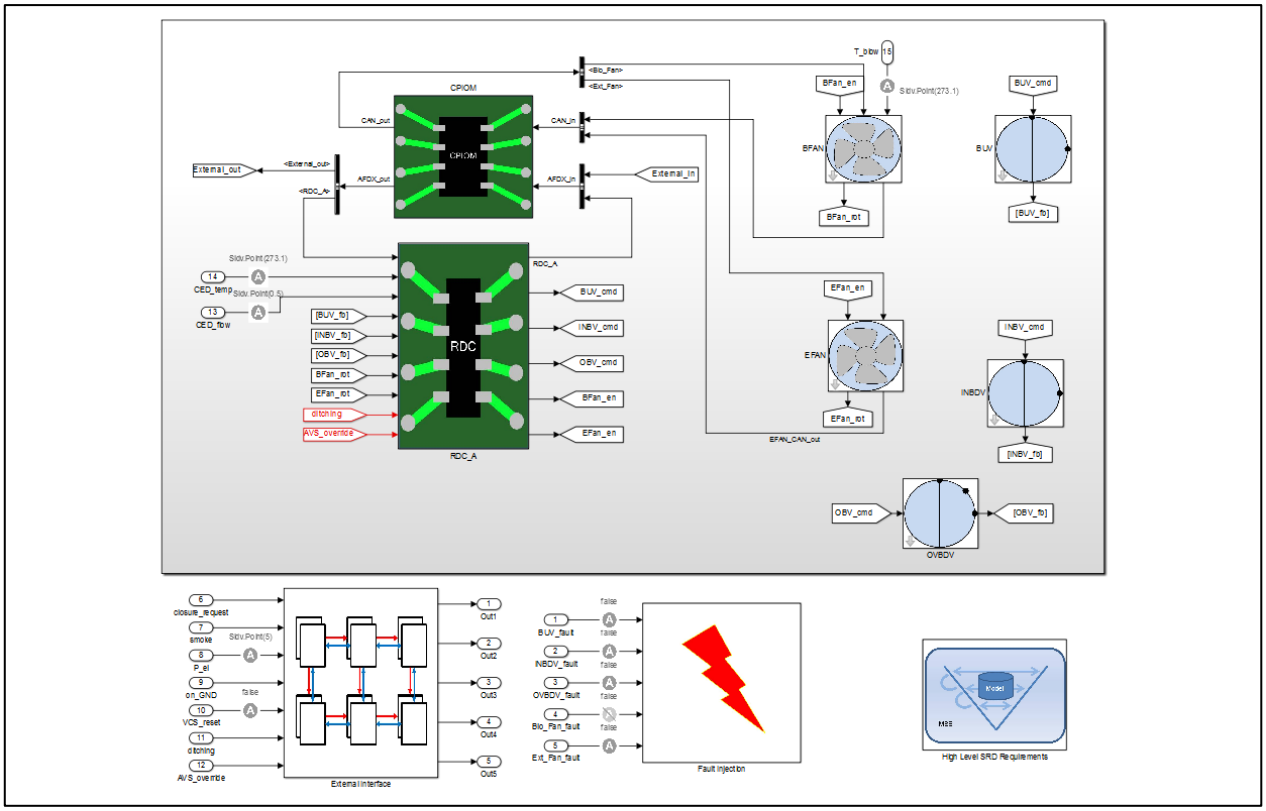

Figure 2 Avionics Ventilation Model

The model for the Avionics Ventilation System is a subset of the Ventilation Control System consisting only of equipment of on side of the aircraft dedicated additionally to the ventilation and air extraction to the avionics compartment. All other compartments and areas of the Aircraft like cabin, cockpit or cargo are not considered in the simplified model to enable non-confidential model distribution amongst partners and easier approach to dedicated development of IOS and tool-chains.

The computer network in the model is reduced to a controller hosting the application and to a remote data concentrator as the front-end to the signal transmission of equipment - see Figure 2. Currently, the system behavior is modelled by discrete and time-dependent states of all equipment and computer whereas no transient properties of ongoing/closing valves and starting/decelerating fans are considered.

A set of safety requirements is captured for avionics ventilation which can be observed by common failure scenarios modelled by Simulink blocks in the standard library. In order to separate failure models in Simulink into a 'stand-alone' failure library – see Figure 1, first investigations towards rule based integration of different models has been performed via an Eclipse Framework and the Matlab Automation Interface. Results are expected in the next version of this document.

The most critical safety requirement is identified as the 'Total Loss and Single Failure' in the T205:

A single failure shall not result in a complete loss of one side of blowing airflow to essential avionics equipment. (Entire functional architecture consists of right-hand and left-hand part)

As a result, two independent controller applications have to be implemented of the Controller Functions and the Monitor Function (a pair for each aircraft side). The Monitor Function enables detection of failures and awareness to the Crew by Build-In-Test-Equipment (BITE) which is essential for Fail-Safe scenarios.

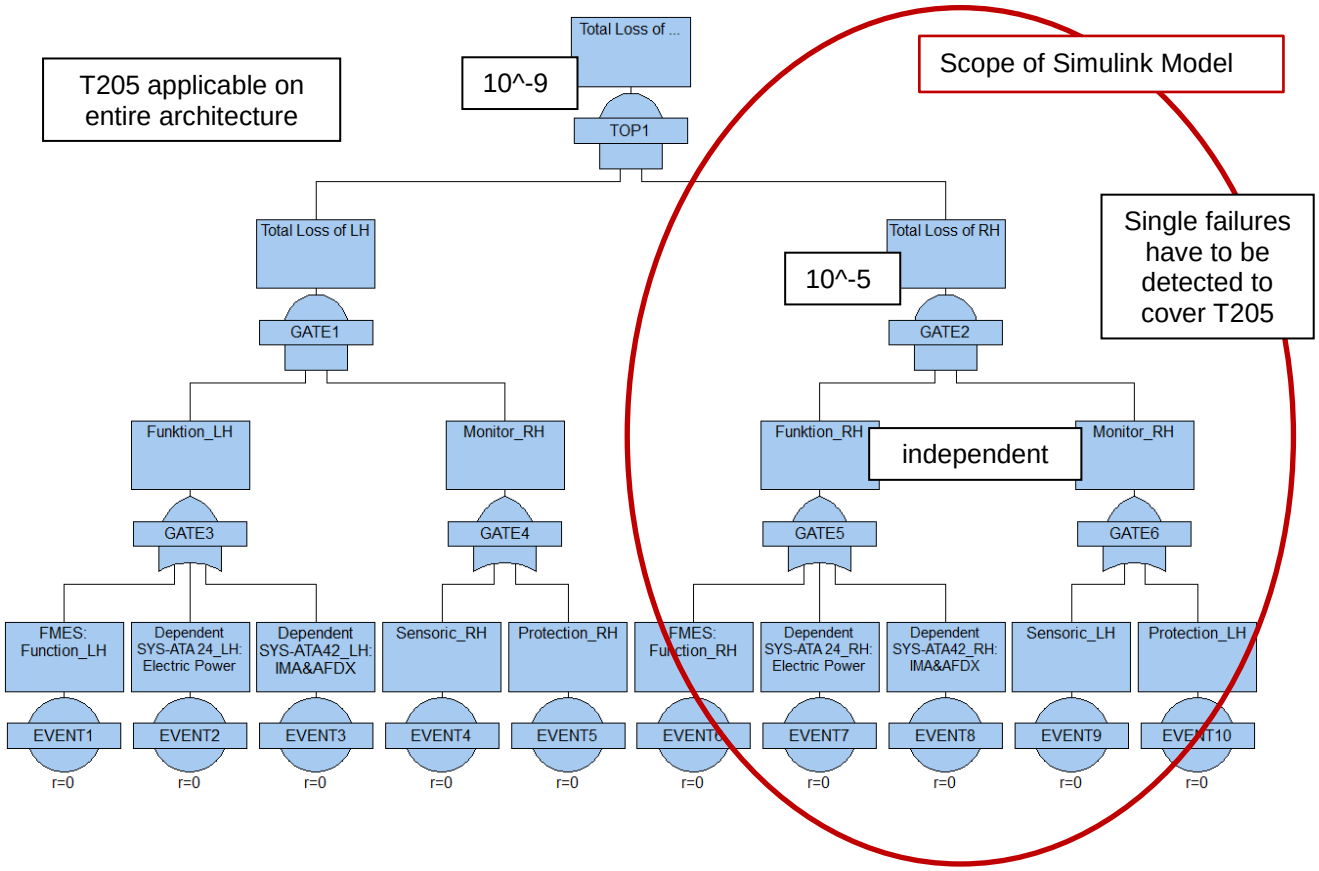

Figure 3 Functional Failure Model of Avionics Ventilation Model

Observer Requirement

No single failure of the model leads to total loss of the Avionics Ventilation Model which is linked to the AND-Gate2 – see Figure 3. At least two failures must occur for total loss failure in Function and failure in Monitor.

Model Preconditions and Observables

- Model Input Vector and initialization:

Power Supply ATA-24 Power Supply = TRUE

Communication ATA-42 (IMA) AFDX = TRUE
System Internal CAN = TRUE
System Internal Controller Input = [Request = TRUE; Status = OK]

- Model Output Vector

Actuators (FAN, Valve) ⇨ Status = [OK (open/closed;Blowing/Idle)]

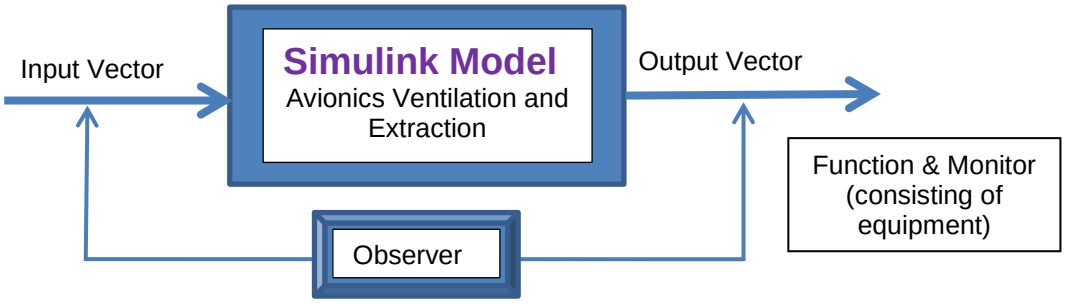

Figure 4 Avionics Ventilation Model applied to Design Verifier

With respect to D2.1.1.1-1, failures according to their classification of 'Omission', 'Commission' and 'Value Range' will be modelled into a failure library for the next version of the document. Additionally, with an integration and rule-based injection concept will be elaborated as requirements for a cross-tool-support of the novel engineering methods. Partners working on the Environmental Control Use Case will proceed on interoperability and the framework.

4 Assessment of the Tool-Chain-Demonstrator

At the current status of the project – the framework to support the avionic design and safety analysis is under definition. Dedicated requirements are derived from the use case descriptions for the Interoperability Standard (IOS). Commercial and established technologies such as OSLC are under evaluation to study and assess its applicability for the envisaged Tool-Chain-Demonstrator. Currently, no final statement can be derived out of the investigations neither any first rough result for dedicated implementations needed to run the use case.

First implementations on interoperability are expected in the next version of the document.

5 Assessment of supported Engineering Methods

At the current status of the project – the applied engineering methods are limited to standard and ‘stand-alone’ model based methods in common-off-the-shelf-tools (COTS). Data interoperability is not supported by the current approach – in particular, this limitation shall be covered in CRYSTAL and the Environmental Control Use Case. First assessment on such interoperating engineering methods will be performed for the next version of this document.