MISSA PROJECT FINAL REPORT

Extract of the Publishable Summary

Grant Agreement number: 212088

Project acronym: MISSA

Project title: More Integrated Systems Safety Assessment

Funding Scheme: FP7-CP-FP

Period covered: from 01/04/2008 to 30/06/2011

Name of the scientific representative of the project's co-ordinator[1], Title and Organisation:

Dr. Chris Papadopoulos,

Lead Systems Safety Researcher,

Airbus Operations Limited

Tel: +44-117-936-6170

Fax: +44-117-936-6279

E-mail: chris.papadopoulos@airbus.com

Project website address: www.missa-fp7.eu

[1] Usually the contact person of the coordinator as specified in Art. 8.1. of the Grant Agreement.

1. Final Publishable Summary Report

The following section provides:

- A one page executive summary,
- A four page summary description of project context and objectives,
- A 25 page description of the main Scientific & Technological results/ foregrounds,
- A seven page description of the potential impact of the project (including the socio-economic impact and the wider societal implications of the project so far) and the main dissemination activities and exploitation of results.

1.1. Executive Summary:

The increase of aerospace systems complexity has meant that by using existing methods for systems development, industry has reached a barrier to innovation and a risk to the competitiveness of products. This is characterized by an increasing time to market for new technologies, increasing costs to demonstrate safety, a greater demand for skilled resources and a limitation on design iterations, which means there is less time to optimise designs that are compliant with safety targets. The ESACS project (STREP Contract No G4RD-CT-2000-00361 - FP5) developed methods and processes that allow the reasoning about failure propagation within systems using a model based approach. The ISAAC project (STREP AST3-CT-2003-501848 – FP6) focused on expanding the scope of formal analyses techniques to deal with human error, common cause analysis, mission reliability analysis, and testability and diagnose-ability of systems. The techniques developed in ISAAC were successful in demonstrating the potential for a reduction in the time needed to carry out the analysis of systems. The VIVACE project (IP Contract No 502917 - FP6) looked at the design infrastructure, the exchange and sharing of data across an extended enterprise related mainly to the structural design and installation areas. The SPEEDS project (IP Contract No 033471 - FP6) looked at developing a communication backbone that allows the exchange of data between tools to produce a more seamless integration of systems specification. It also looked at modelling by contract and issues that surround the integration of models of heterogeneous elements of a system. So far very little work has actually looked specifically at refinement, composition, optimisation or the exhaustive search for solutions.

Summary description of the project objectives:
The objectives of the MISSA project are to develop systems safety analysis methods and tools that lead to a reduction in the time to complete subsequent design iterations, offering a reduction to the development costs, giving more time to the engineers to achieve greater levels of performance or weight optimisation, or to have an increase in agility of design. Hence the MISSA results aim to enable design organisations to respond to changing market demand through the design life, to improve the means to maintain the complete chain of evidence between safety claims and the evidence used to substantiate it. As a result of the work, MISSA has delivered 37 developments in four technical work packages

The MISSA project has delivered capabilities at the three Aircraft Systems Development Levels, at the Aircraft level, the Systems Architecture Level and the Systems Implementation level. MISSA has also considered the transverse aspects of systems development related to safety argumentation, evidence synthesis, traceability and configuration control. In Work Package 3, functional modelling, qualitative and quantitative requirements and safe space allocation and optimisation methods and tools were developed. In Work Package 4, reasoning algorithms that were used to analyse individual systems as well as combinations of systems were improved. Techniques were also developed for facilitating the review of the vast number of results that the approaches are producing. In Work Package 5, implementation level modelling and analysis dealt with mainly how to analyse Models that have a great degree of time dependent behaviour, non-linear mathematical operators and hybrid behaviour in the analysis. For the three first technical work packages the need to have consistency between results at the different levels was treated by ensuring that the results can be compared and that the tool that supports the comparison respects refinement rules and highlights when refinement rules are broken. Finally, to bring everything together, Work Package 6 looked at how the different safety models and analyses could be used and to what extend they should be used as evidence for primary and backing arguments that form part of the certification, safety arguments. Work Package 6 also looked at some of the transverse topics like traceability management between different types of evidence, models, documentation and argumentation.

1.2. Summary of Project Context and Objectives:

Background:

The increase of aerospace systems complexity has meant that by using existing methods for systems development, industry has reached a barrier to innovation and a risk to the competitiveness of products. This is characterized by an increasing time to market for new technologies, increasing costs to demonstrate safety, a greater demand for skilled resources and a limitation on design iterations, which means there is less time to optimise designs that are compliant with safety targets. The ESACS project (STREP Contract No G4RD-CT-2000-00361 - FP5) developed methods and processes that allow the reasoning about failure propagation within systems using a model based approach. The ISAAC project (STREP AST3-CT-2003-501848 – FP6) continued by focusing on expanding the scope of analyses techniques by developing formal techniques to deal with human error, common cause analysis, mission reliability analysis, and testability and diagnose-ability of systems. The techniques developed in ISAAC proved exceptionally successful in demonstrating the potential for efficiency gains that could lead to a reduction in the time needed to carry out the analysis of systems. The VIVACE project (IP Contract No 502917 - FP6) looked at the design infrastructure, the exchange and sharing of data across an extended enterprise that has focused mainly in the structural design and installation areas. The SPEEDS project (IP Contract No 033471 - FP6) has looked at developing a communication backbone that allows the exchange of data between tools to produce a more seamless integration of systems specification. It also looked at modelling by contract and issues that surround the integration of models of heterogeneous elements of a system. So far very little work has actually looked specifically at refinement, composition, optimisation or the exhaustive search for solutions.

Summary description of the project objectives:

The objectives of the MISSA project are to develop systems safety analysis methods and tools that lead to a reduction in the time to complete subsequent design iterations, offering a reduction to the development costs, giving more time to the engineers to achieve greater levels of performance or weight optimisation, or to have an increase in agility of design. Hence the MISSA results aim to enable design organisations to respond to changing market demand through the design life, to improve the means to maintain the complete chain of evidence between safety claims and the evidence used to substantiate it.

The MISSA project has delivered capabilities at the three Aircraft Systems Development Levels, at the Aircraft level, the Systems Architecture Level and the Systems Implementation level. MISSA has also considered the transverse aspects of systems development related to safety argumentation, evidence synthesis, traceability and configuration control. In Work Package 3, functional modelling, qualitative and quantitative requirements and safe space allocation and optimisation methods and tools were developed. In Work Package 4, reasoning algorithms were used to analyse individual systems as well as combinations of systems. Techniques were also developed for facilitating the review of the vast number of results that the approaches are producing. In Work Package 5, implementation level modelling and analysis dealt with mainly how to analyse Models that have a great degree of time dependent behaviour, non-linear mathematical operators and hybrid behaviour in the analysis. For the three first technical work packages the need to have consistency between results at the different levels was treated by ensuring that the results can be compared and that the tool that supports the comparison respects refinement rules and highlights when refinement rules are broken. Finally, to bring everything together, Work Package 6 looked at how the different safety models and analyses could be used and to what extend they should be used as evidence for primary and backing arguments that form part of the certification, safety arguments. Work Package

6 also looked at some of the transverse topics like traceability management between different types of evidence, models, documentation and argumentation.

Description of the work performed since the beginning of the project:
Since the beginning of the MISSA project the consortium has completed the requirements capture phase, and the three cycles of "development and evaluation" (Ref. Figure 2). The evaluation results from the three "Development and Evaluation Cycles" show significant progress for all the work packages. The project has delivered 37 developments in four work packages (Ref. Figure 1) through the creation of new methods and tools and through the further developments to existing methods/ tools (Ref. Figure 3).

Description of the main results achieved: The MISSA Project has developed methods and tools to support safety modelling and analysis at the Aircraft Level, Systems Architecture Level and Systems Implementation Level. Transversally across all levels methods and tools were delivered for performing safety argumentation and for the collection, referencing, and configuration management of representative design artefacts generated by these new model based safety methods and tools to substantiate a safety argument.

At the a/c level, seven methods and tools were developed to support the safety activities related to two themes, functional requirements apportionment and architecture optimisation as well as to help with space allocation and particular risk analysis. In line with the activities that are planned as part of the Preliminary Aircraft Safety Analysis considered in the latest SAE ARP4754A, and described in appendix B (of the next issue of ARP4761 that is expected soon), Functional modelling methods and analysis tools were developed to support the early qualitative and quantitative requirement allocations, architecture optimisations and contract based formalization of safety requirements, as well as a tool to facilitate the allocation of Development Assurance Levels (DAL). A method and tools for helping safety and installation engineers to converge on an acceptably safe installation that is optimised for some user selected performance criteria was delivered. Additionally a new early prototype concept for an image processing based product inspection/ audit tool that checks a fabricated product to see if it conforms to identified safety constraints was produced.

At the systems architectural level, work was performed in three general areas leading to twelve new developments, the first relates to creating a safety assessment model, the second relates to improvements in the analysis engines and the third relates to performing and managing incremental assessments. In order to create safety assessment models, a safety-modelling handbook was produced that details the possible new modelling approaches and suggests the best balance between the different approaches. A methodology was developed and demonstrated and a guide was written that details how multiple separate organisations can produce a single multi- system compositional model in order to perform a safety analysis that considers the multi-system synthesis. A couple of tools were produced that aim to facilitate the construction of models. The first tool constructs regularly structured models that contain large numbers of repeated elements that are connected in a regular fashion from an engineering database. The second tool, called "Schematic 2 Model Transformation (S2MT), takes a scanned image of a systems schematic that is made up of standard symbols, uses image processing to identify the symbols, associates them to pre-existing library elements, or allows the user to make an association of a symbol to a new component that can be detailed at a later stage, finally generating an output file in a format that can be opened by Dassault Aviation's Cecilia OCAS tool for further elaboration, and subsequently for safety analysis. The second theme deals with development of the analysis engines and analysing a single model. In the theme on Analysis Engines, significant improvements were made for minimal cut set generation to

the OCAS tool's native analysis engine and FBK's NuSMV-SA algorithm was plugged in to the OCAS tool. A study was performed on how to improve the accuracy of the current quantitative analysis that is used. A capability to export qualitative safety analysis results such that they can be used by COTS RAMS tools in order to perform a quantitative analysis was delivered. A methodology to perform verification of the DAL allocation using the compare tool was achieved as well as the ability to perform a symmetry/ asymmetry verification again using the compare tool. On the theme for Incremental Assessment, the "Model Compare" tool was developed with a focus on addressing lightweight refinement rules. The same compare tool is also used to compare safety analysis results from systems architecture models and Systems Implementation Level Models. A model-mapping concept enabled the use of the model compare tool for Verifying DAL allocation, Model Symmetry verification and for comparison of WP4 safety analysis results to WP5 results.

At the systems implementation level: work was performed on two themes, Methodology and tools for qualitative assessment and on Methodology and Tools for Model Correlation. For qualitative assessment, improvements were made to the way that the verification techniques work, in the case of Time Compression a mechanism was created to remove/ compress time where there are no state transitions that occur other than the increment of timers, the CEGAR algorithm had an abstraction and refinement capability added to it in order to better handle the state space explosion problem. A Monte Carlo Simulation Technique was implemented on the Statemate Verification Engine Safety Analysis Module to handle large models. The NuSMV-SA engine BDD/ SAT based routines were improved, integrated into the OCAS platform and tested on industrial case studies. Finally some work was performed to add the ability to model check hybrid models originating from Simulink using the NuSMV model checker and in Scade the Prover Design Validator was extended to accept more non-linear mathematical constructs. Regarding the theme for Model Correlation, work was performed in two directions. The first relates to an extension of the HRC framework (that was developed as part of the SPEEDS project and subsequently on CESAR) to handle safety contracts and perform compositional reasoning. The second relates to the compare tool developed as part of WP4 except this was to use it to compare between WP4 modelling results and WP5 results to determine whether an implementation level model still respects the same lines of redundancy or if there has been a worsening or an improvement in the qualitative behaviour of the systems architecture in its evolution from a systems architecture model to a systems implementation model.

The transverse Argumentation, Synthesis and Change WP has three main themes. The first relates to the development of a methodology and support material for the generation of safety arguments, the second relates to the synthesis of safety evidence for the preparation of a certification dossier and how argumentation can fit in to this. The third relates to improvements to the synthesis, argumentation and change tools. For the safety argumentation theme generic argumentation patterns were developed for certification and safety, and, primary and backing arguments were also created for each of the three safety modelling levels together with a methodology guide to instruct a user in developing and reviewing such arguments. Work was invested into defining what a certification dossier should contain in the case where a safety analysis was generated using a model based approach and how safety argumentation fits into the SAE's ARP Safety Process. For the Synthesis, Argumentation and Change theme, support was developed for being able to trace to the model component and equipment levels of both Scade and Cecilia OCAS models, a new trace and link engine was produced that allows the Atego Workbench to be independent of requirements databases, and adds a new ability that requirements databases lack, namely to trace the evolution of links within a design portfolio. Finally improvements were made to the GSN Modeller as well as integrating it with the Atego Workbench and enabling change management of the defined arguments.

Potential impact and use: A series of EU-wide research projects have demonstrated the applicability of these novel approaches to the complexity of real aeronautical systems; which has led to a partial up-take by some European aeronautical companies. The uptake so far is being applied through the use of internal approaches to modelling. The MISSA consortium has presented the results, potential gains and more specifically guidance material to Industry working groups, to gain support for the industrialisation of these methods and as a step towards harmonising these approaches across the industry. Additionally, tools have been developed not just to demonstrate the feasibility but also to be made available so that the approaches can be put to industrial use.

The socio-economic impact: Recently similar research has emerged outside the EU. Hence, the opportunity to convert the research lead into a competitive EU industrial advantage is time-limited. The experience gained from the evaluation cycles show the promise from some of the developed techniques to significantly reduce the time and hence increase the agility of the systems developers, allowing them to produce better performing products within shorter time frames. This clearly strengthens industries socio-economic position so long as it is ready to be applied within a timely manner compared to the competition.

Wider societal implications of the project so far: MISSA, addresses key FP7 objectives in Aeronautics such as helping to reduce a/c development costs, creating a competitive supply chain to halve the time to market and reducing the accident rate, and contributes to achieving wider objectives set-out in the ACARE strategic research agenda, such as highly cost efficient, and ultra secure air transportation system, contributing to the fulfilment of the Lisbon Agenda and yielding real benefits in terms of competitive advantage of EU industries.

The MISSA project has produced a range of capabilities that will have different times to maturity. Some of the capabilities are quite mature that are either in a position to influence the use of the currently applied tools and so are immediately industrialise-able, and have benefitted e.g. the rail industry in the case of the Time Compression capability by Prover Technology, others need some additional consideration by the industry as a whole but are, nevertheless, close to industrialisation. MISSA has also produced some capabilities that are much less mature and as such will require further research before they are ready to be applied industrially.

Dissemination activities have exploited MISSA results in other industrial sectors, maximising the value to EU industry.

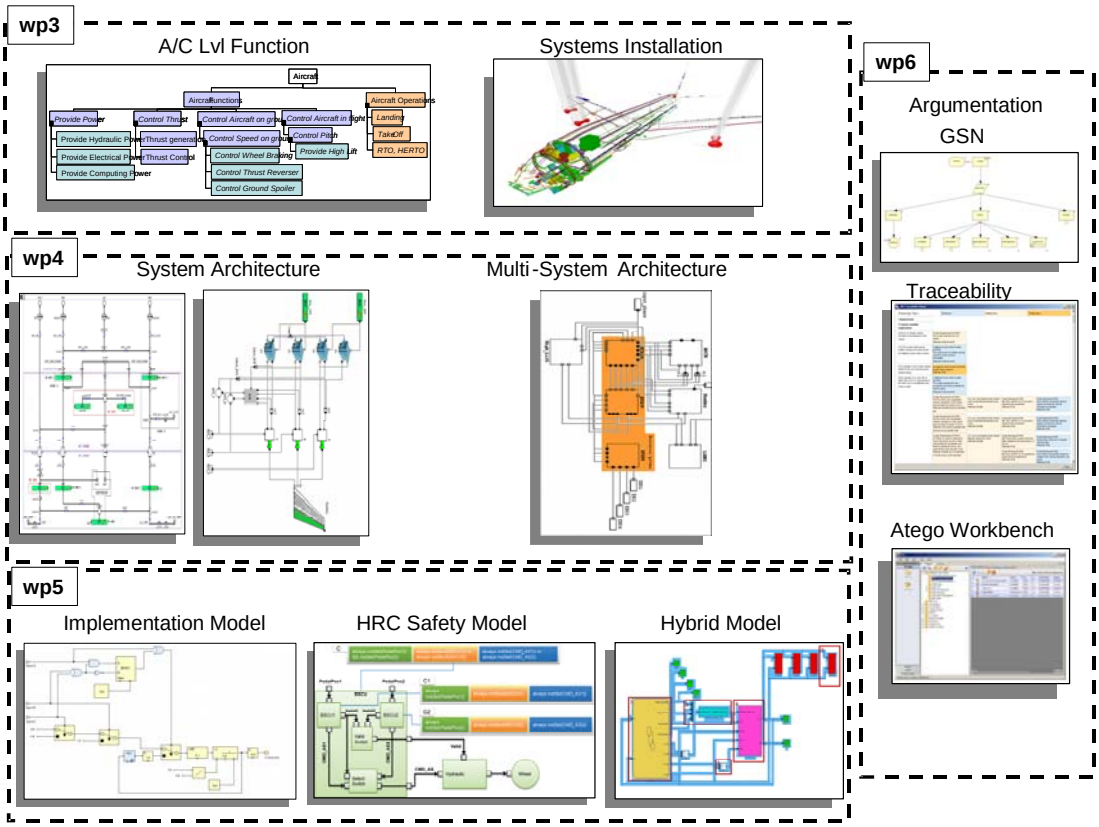

Figure 1: The MISSA Project has focused on Modelling, Analysis and Optimisation at the Aircraft, Systems Architecture and Systems Implementation Level, as well as across the levels to consider transverse themes such as Evidence Synthesis, Safety Argumentation and Change Control

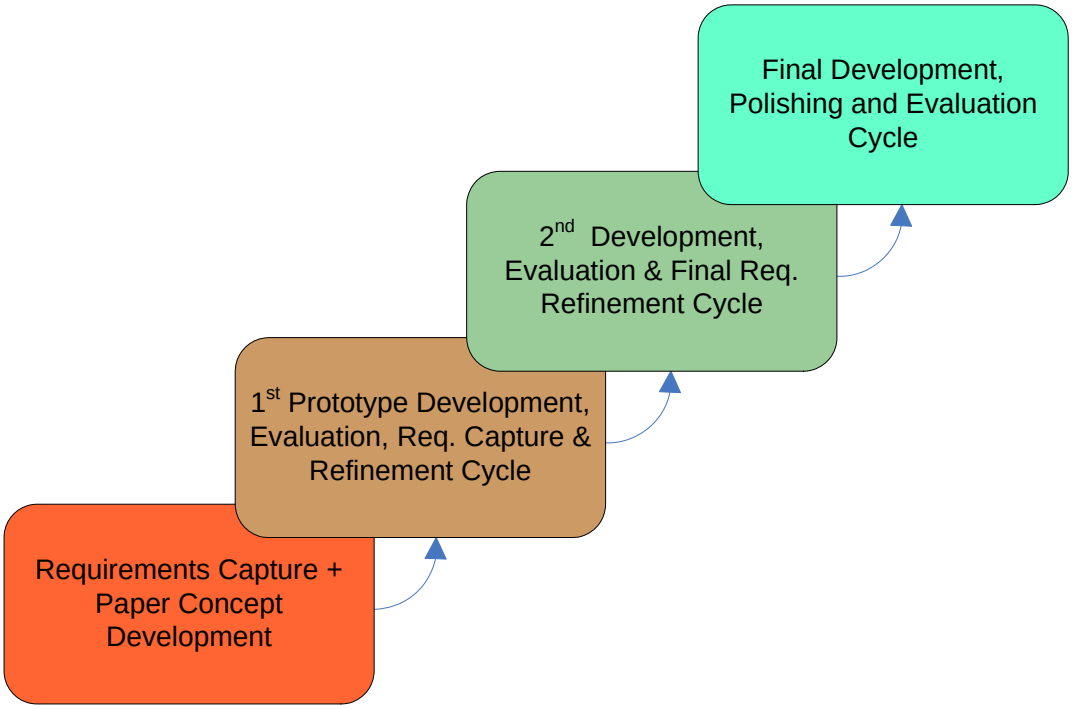

Figure 2: The MISSA Project had an Iterative Development Cycle with one cycle of requirements capture and preliminary development and three cycles of prototype development and evaluation

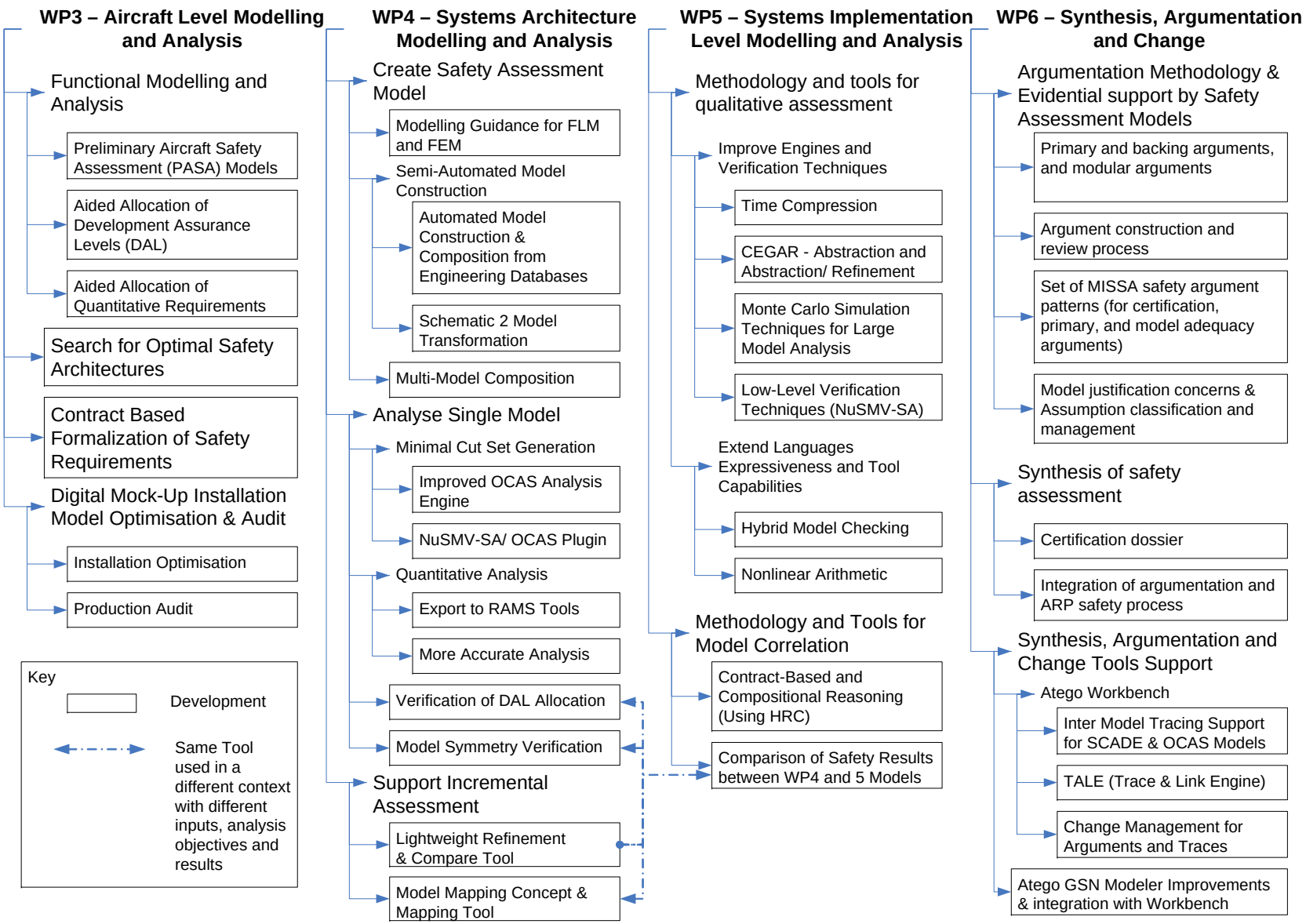

Figure 3: MISSA Delivered 37 Developments During the MISSA Project from 4 Work Packages

MISSA Project Coordinator: Airbus Operations Ltd.
Technical Representative for Airbus Operations Ltd.:

Chris Papadopoulos
Lead Systems Safety Researcher
Engineering Design, Systems General, Safety and Reliability Department
Phone: +44-(0)117-936-6170
<Mailto:chris.papadopoulos@airbus.com>

Airbus Operations Ltd.
New Filton House
Filton, Bristol BS99 7AR
United Kingdom

http://www.missa-fp7.eu

1.3. A description of the main S&T results/foregrounds:

Background:
The MISSA (More Integrated System Safety Analysis) project is a collaborative research project that is joint funded by the European Commission (EC) under the seventh framework program. EC 7th Research Framework Program (FP) Project number 212088.

The MISSA project built upon work from a number of projects, the most current with the strongest relationship being ESACS (Enhanced Safety Assessment for Complex Systems) during FP5 and ISAAC (Improvement of Safety Activities on Aeronautical Complex systems) during FP6.

The focus of ESACS was to develop the Formal Verification Technology to support mathematical proof of safety analysis, and in particular generating results such as Cut Sequences (similar to cut sets except that sequence and time are accounted for), a very computationally heavy task with significant complexity in the specification of problems, in the generation of results and in the presentation of the results in an understandable form.

The focus of ISAAC was to apply the proof engines to a number of themes, such as Safety Architecture Patterns, Common Cause Analysis, Testability and Diagnose-ability of Systems, and Mission Reliability Analysis amongst other themes.

Both ESACS and ISAAC looked at specification and formal verification of individual models. The results of which are expected to be composed as evidence to formulate a greater argument. The models were treated in the project as independent artefacts without consideration of how to compose the models or the results together. The details of model content was considered as far as compatibility with the formal verification engines was concerned, or where further development of the Formal Verification Algorithms was possible to allow for the specification used. Both did not aim to define a modelling policy that could be applied in a systematic repeatable manner.

MISSA has focused on defining the details of specification, depending on the intent of the models at each Aircraft Development Level, and also consider how to compose the different models or results from models at different levels, or within a level but where the models describe different systems or different domains.

Organisation of the work:
To address these two axes the technical work was separated into 4 work packages, three that address the hierarchical development levels and one that transects across the other three levels.

The hierarchical themes are:

- Aircraft Level Specification and Analysis
- Systems Architecture Level Specification and Analysis
- Systems Implementation Level Specification and Analysis

The transecting theme is:

- Synthesis, Argumentation and Change

The Hierarchical themes addressed specification and analysis according to the maturity of design during the respective stage of development. E.g. during the Aircraft level specification very little is known about the details of the equipment or behaviours of the systems reconfiguration. What is known is that in order to satisfy the aircraft level requirements there is a need to have a specific

number of redundant channels. Historical information that is known by the engineers allows them to imagine what could be possible at the lower levels and so are influenced by this knowledge when specifying the higher levels. At the aircraft level the installation problem is also treated. For example if there exists an external risk to an aircraft that affects multiple systems that are expected to deliver a contribution to a single safety critical function, then it is necessary to ensure, where the design calls for a guarantee of independence between redundant channels and systems, that this requirement is respected. The ISAAC project Common Cause Analysis (CCA) theme looked at how to take results from a Particular risk analysis, to consider the results in the model based functional safety analysis, and how to return the results to the geometric world to address the safety concerns.

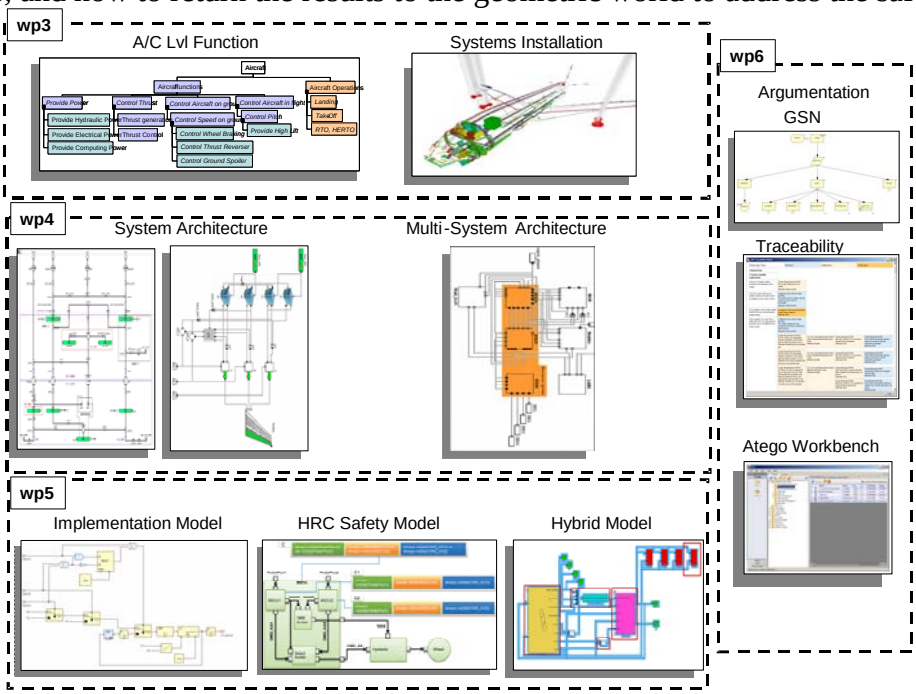

Figure 4: The MISSA Project has focused on Modelling, Analysis and Optimisation at the Aircraft, Systems Architecture and Systems Implementation Level, as well as across the levels to consider transverse themes such as Evidence Synthesis, Safety Argumentation and Change Control

MISSA extended this capability by calculating potential solutions to the installation problem allowing the installation engineers to focus their attention to installation strategy, constraints, and optimisation of installation rather than ad hoc optimisation through trial and error.

The Transverse theme, “Synthesis, Argumentation and Change”, looked at how design arguments specifically related to the safety of systems are considered, and how they are decomposed and assigned to the various sub systems and domains at each level. An advantage that the Transverse theme provided was related to the practical side of managing information. It is understood that, with the vast amounts of information and interdependencies between information that is required in the specification of aircraft systems, and with the need to show that every element has been designed in a systematic way, there is a need to bring the information together in a manageable and navigable form. The theme also looked at how the traditional approach to managing this complexity led to the development of mechanisms, such as personal checklists, that are used by engineers to prepare evidence, to review and audit the design and the analyses results, with the aim of convincing ones self that the delegated work has been carried out to a sufficient level of quality.

Together these four work packages have delivered 37 scientific and technological results. The following figure shows how these 37 development fit together under each of the work packages.

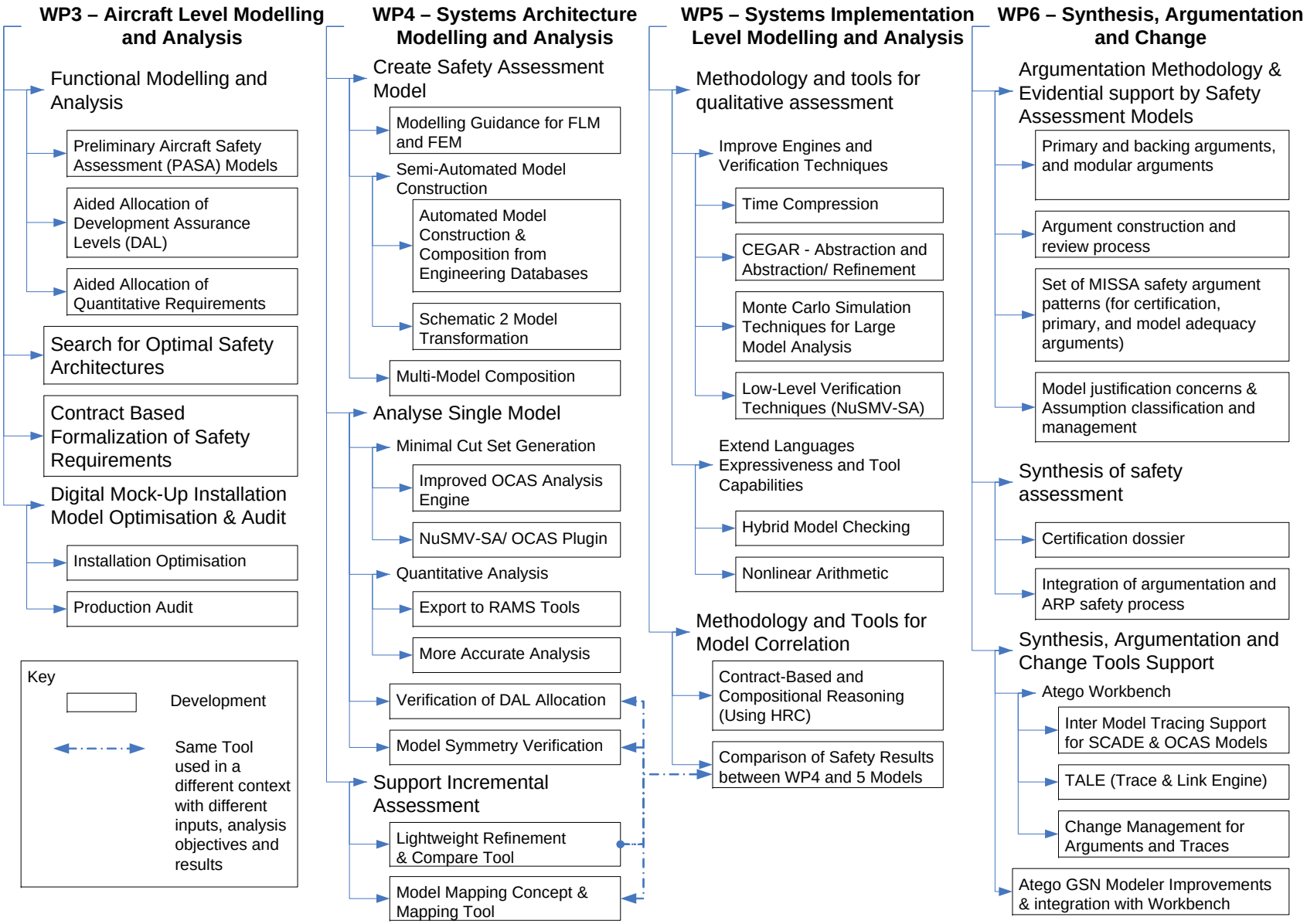

Figure 5: Development Over the Course of the MISSA Project

1.3.1. The aircraft level modelling and analysis work package (WP3)

The aircraft level modelling and analysis work package has delivered new capability in six areas related to Aircraft Functional Specification and two areas related to Systems Installation. These capabilities are described below.

1.3.1.1. Preliminary Aircraft Safety Assessment (PASA) Models

PASA is a new kind of analysis that has been incorporated into ARP4754A. MISSA WP3 has made progress to support this kind of analysis using a model-based approach. A number of types of models were needed to describe each aspect that is considered within PASA. These models include a Functional Dependency Model and a Flight Operations Model.

The functional dependency model (Figure 6) was developed that decomposes functions into sub-functions that correspond to classes of or levels of performance or functional failure modes that impact the effects of a function failure condition and consequently, the FHA output. When all functional failure modes and all classes of functional performance encountered in the FHA can be related to a function or sub-function name, then the decomposition is closed by allocating physical resources to implement the function. This last step has two interests. First, it may put-in-evidence shared resources that create physical dependences between functions that are not logically dependent. Second, it enables establishing a link between FHA models and system models used for Preliminary System Safety Assessment.

Likewise a Flight Operations Model was defined that represents flight phases, adverse operating conditions and pilot procedures. Nominal flight phases are modelled together with phases associated to specific adverse conditions or degraded operation modes planned by emergency procedure (e.g. take off phase after reaching high speed, rejected take off). Dependencies between phases are also modelled. Dependencies are not static: they put constraints on the temporal chaining of phases.

1.3.1.2. Aided Allocation of Development Assurance Levels (DAL)

Once the models and safety requirement observers described in the previous section are defined, it is possible to start the analysis activities. The analysis is a two-step approach:

Step 1 = Sequence Generation: for each safety requirement observer, ISAAC safety analysis tools are used in order to generate minimal sequences of failure modes (safety results file) that lead to the failure condition described by the observer. (Figure 6, step 1)

Step 2 = Result Verification and Requirement Generation: For each safety result file, tools developed within MISSA check that sequences are consistent with respect to qualitative objectives derived from the classification of the failure condition. The tools also analyze safety results in order to generate new types of requirements: function independence and Function Development Assurance Level (FDAL) (Figure 6, step 2)

The upper part of Figure 6 shows the functions: e.g. Deceleration. Each function contains a set of safety requirements, e.g. two requirements are associated with the ThrustReverser function: “Total Loss is Catastrophic” and “Partial Loss is Major”.

During step1, sequences are generated for each the safety requirements. during step 2 the tools check that qualitative requirements are enforced e.g. that no sequence with strictly less than NSev failures leads to a SEV (Severe) failure condition, where the relation between NSev and Sev is given by the following table:

Sev	MIN	MAJ	HAZ	CAT
NSev	1	2	3	3

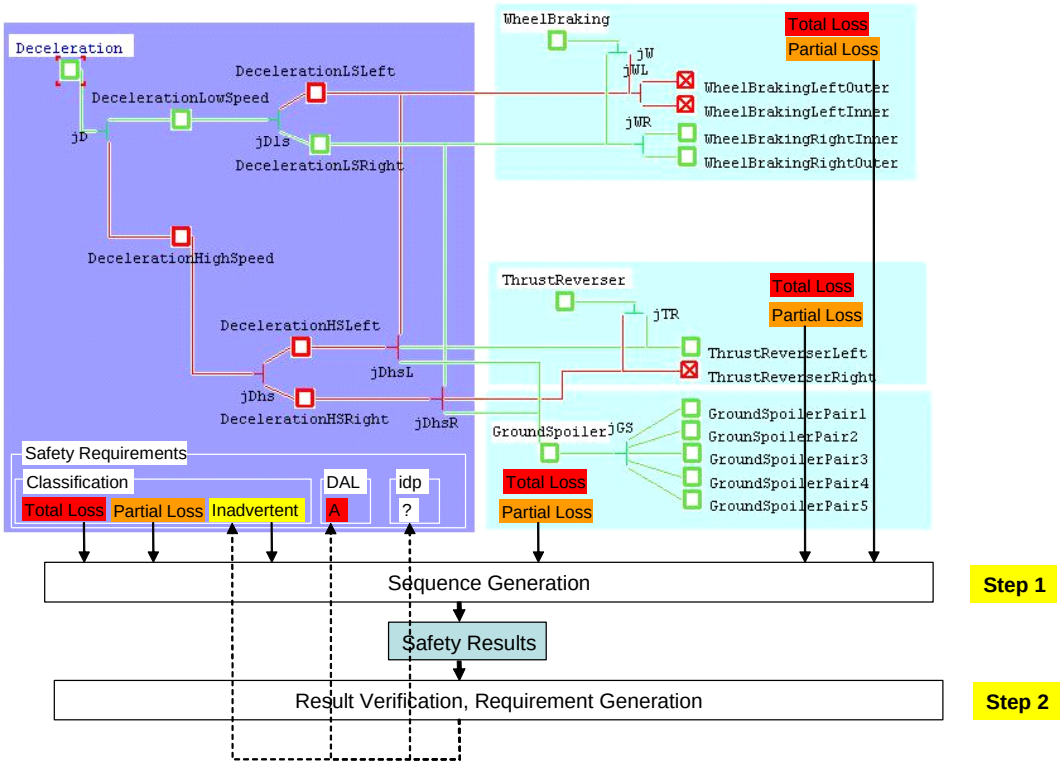

Figure 6: Principles of the verification and generation technique

Then the analysis tool checks that independence and DAL requirements that are provided in the Safety Dependency model are consistent. When no requirement is provided, the tool generates a set of requirements e.g. in the Figure above, DAL A is associated with the Deceleration function but no DAL is associated to other functions. So the tool will check that DAL A is consistent and it will propose a DAL assignment for other functions.

1.3.1.3. Aided Allocation of Quantitative Requirements

A method and tool were developed that look for the maximal failure rate and inspection interval of system functions such that the mean probability of the loss of an aircraft function is under a given bound. The main approach is to approximate the probability by a multivariate polynomial over failure rates and inspection intervals. The problem is formalized as linear constraints on the logarithm of failure rates. This simple formalization is made possible by focusing on the probability of the failure during the worst-case flight, using synchronized discrete inspection intervals and by evenly distributing the bound over all minimal combination of failures. The set of linear constraints is solved using MILP (Mixed Integer Linear Programming) solvers to find acceptable failure rate and check interval values.

The tool was first applied on basic examples to check the correctness of the approach. Results computed with the tool were compared with analytical solutions. Limited differences were found,

that can be explained by the linear approximations used by the tool. For small values of probability (less than 10^{-4}) the differences are acceptable. Then the tool was applied to larger size case-studies, the tools computation time performance is good (less than a minute) when check intervals are not fixed for only a limited number of function failures. This last assumption seems consistent with the industrial practice.

The SAE ARP4754A that was issued in December 2010 defined new DAL allocation rules, so the work is likely to be highly innovative.

In conclusion the results are promising and more experiments are needed to increase the maturity level of the method and tools and tune the tool with more optimization criteria proposed by the experts.

1.3.1.4. Optimisation allocation of safety/ reliability/ costs requirements

This line of activity is concerned with an optimisation study of different system parameters (related to safety, reliability and costs) and architectures for the determination of a solution that is optimal with respect to some user-defined criteria. The activity on optimisation allocation had not been previously investigated in the ESACS and ISAAC projects. The progress beyond the state-of-the-art mainly consists in developing a tool to perform the optimisation trade-off analysis and allocation of safety, reliability and cost requirements (qualitative and quantitative) in an automated way, which is not possible with current practices.

The tool has been positively evaluated by the users. The case study that has been investigated, although simple, allowed us to derive several useful information on the system and the possible candidate architectures. The possibility to perform trade-off studies has been considered very important, and positively evaluated by the users.

For future work, we plan to investigate further the possibility to define proper and useful “multi-parameters” expressions. Moreover, the NuSMV model checker was considered adequate for solving the problem at hand, where it is possible to “discretise” the values that the system parameter may assume. As a suggested point for future work, it is suggested to consider problems where values are not discretised. These problems can be naturally solved by the extension of NuSMV that contains the MathSAT SMT solver.

1.3.1.5. Contract Based Formalization and Analysis of Safety Requirements for the Aircraft level modelling and analysis.

In MISSA, the contract based formalization and analysis of safety properties have been investigated. This work has been integrated with the HRC formalism originally developed in the SPEEDS projects. It has extended the RSL framework with the necessary pattern to adequately describe the safety properties developed and the algorithms necessary to perform virtual integration testing for safety contracts. These algorithms have then been implemented in a tool chain that integrates with the DOORS Requirement Engineering tool and provides an analysis engine that performs Compatibility and Dominance checks for the defined safety contracts. The results from this work were published at the 7th European Systems Engineering Conference.

Method and tools were developed successfully to support the requirements capture and formalization under the form of safety contracts.

Finding the “safety contracts” is still quite a hard manual activity. So, further experiments are needed to increase the maturity of the current results in the short term. In the longer term, some complementary kinds of help/ guidance should be investigated to help the designer to fix an invalid requirement breakdown. Finally, more guidance (e.g. design patterns) should be offered for developing correctly the initial requirement breakdown.

1.3.1.6. Installation Optimisation

The Installation Optimisation capability extends work from the ISAAC project. It is a customised application of MathSAT3D. Referring to the figure below, MathSAT3D is given 3D geometry from a mock-up tool, such as Catia, particular risk volumes, installation constraints as equations or allocation volumes for each or combinations of equipment, safety requirements and optimisation criteria such as, “minimise the number of components to be moved”. The algorithm returns installation solutions. In the case where no solution exists due to an over-constraint problem, the UnSAT-Core functionality generates the minimal set of constraints that make a given formula un-satisfiable, then the tool returns a list of relaxations that could lead to solutions. MISSA developed the core functionalities of the tool. The algorithm was developed to support very basic primitive representations of an installation, e.g. cube, parallelepipeds etc. It provides support for, curved surfaces such as cylinders, cones and spheres by simplifying them into polyhedra, the automatic rotations for all the shapes, some object proximity predicates and distance constraint between two points. All of these features are based on a discretization of the space due to the linearity of the formulas needed by MathSAT3D. The tool suggests translations and rotations. The tool generates a vrml representation of the result, which can be re-imported into Catia. Pipe and electrical routings have not been considered at this stage.

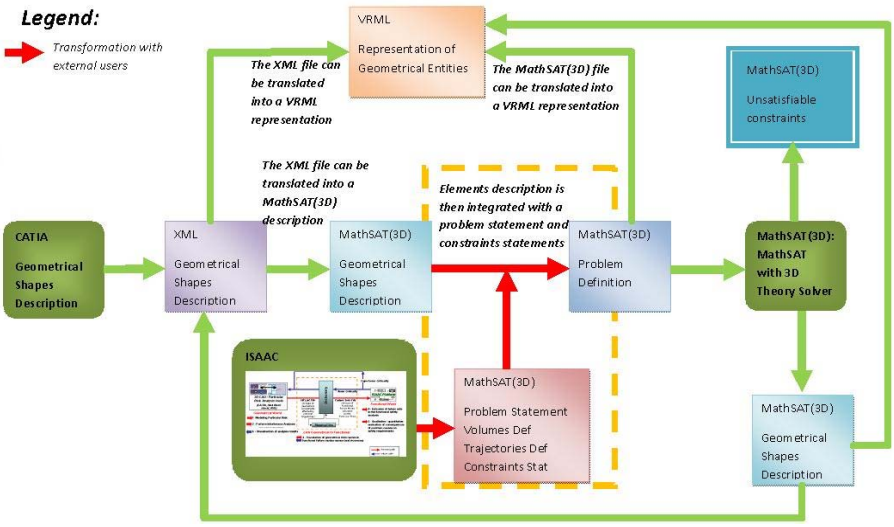

Figure 1-7: Schematic of the Modules developed within MISSA and the interrelationships

Future work for MathSAT3D can be the integration of non-linear solvers to enable support for curved surfaces, continuous rotations and distance measures without approximation, and the management of pipes i.e. objects with variable shape). The main problem of this methodology is the difficulty of the computation, which is currently too high to manage when the approach is applied to real industrial models.

1.3.1.7. Production Audit

The production audit work developed two prototype tools that together should audit a product during final assembly or in line-maintenance against safety installation constraints to ensure quality or to check for the acceptability of damage respectively. The first is a 3D Measurement tool that uses multiple views of a scene and calibration grid captured by a basic digital camera. The application corrects for perspective, and various optical aberrations. The application indicates the distance between every permutation of pairs of consistent manually selected points from the images and from a defined reference plane. The second application is a 3D Model Matching tool that creates two 3D point clouds, the first from the objects identified within a set of images and the second from a digital mock-up of the scene. Referring to the figure below, the two clouds are aligned such that a common selected datum has the lowest positioning error, based on feature extraction and comparison techniques. The rest of the recognised equipment are aligned and offsets between the coincident equipment are reported as positioning errors used to check for acceptability to installation tolerances derived from zonal safety installation constraints. The measurement error of the tool is estimated from the measurement error of the calibration grid.

The applications are early prototypes. The accuracy needs to be improved. The workflow seems to fit the needs of the engineers in both use scenarios. The user experience needs to be polished.

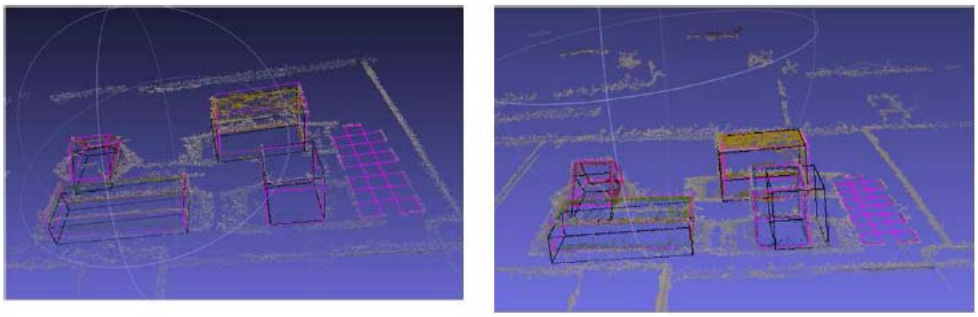

Figure 1-8: Original Fitted and Blue shift Fitted cloud

1.3.2. Systems Architecture Modelling and Analysis

This work package has delivered four new capabilities to support Creating Safety Assessment Models, six new capabilities to support the analysis of these models and two new capabilities to support the incremental evolution of these models. The capabilities are described below.

1.3.2.1. Modelling Guidance for FLM and FEM

Guidance has been written for the two ‘pure’ approaches: ‘Failure Logic Modelling’ and ‘Failure Effects Modelling’:

- **Failure Logic Modelling (FLM) Handbook:** this describes a general family of approaches, which rely on dedicated safety models. The models are modular and the component dependencies are captured in terms of the deviation of behaviour from that intented (Failure Mode). The output failure mode of the component can be caused by input and/ or internal failures. The dependency between output FMs, input FMs and internal failures is referred to as “component failure logic characterisation” and is described at the level of components. FLMs can be constructed in custom- / purpose- defined notations (e.g. FPTN and HiP-HOPS) or in a general engineering language (e.g. AltaRica, SCADE, Simulink, etc).

- **Failure Effects Modelling (FEM) Guidance:** this describes an alternative general approach to safety-related modelling. FEM may be considered closer to the design world, since components and interdependencies are in terms of (abstracted) designed interactions and flows of energy, matter and information. Each component can operate nominally as designed or under abnormal circumstances caused by internal failure. FEM is sometimes especially effective for systems with failure detection and mitigation or that are highly reconfigurable. However, this approach is not able to capture effects of failures that cause entirely unintended interactions (e.g. leakage, short circuits, etc.). It may also be less applicable at the earliest stages of system design, where proposed designs are immature and exact reconfiguration logic remains unspecified.

Initial versions of the guidance documents have been developed during the MISSA project. It is expected that improvements will be made after the MISSA project is finished.

1.3.2.2. Automated Model Construction & Composition from Engineering Databases

A method and tool was developed that demonstrated the ability to use industrial databases to generate safety models encoded in the AltaRica language. The relationships between design and safety models have been addressed in two distinct scenarios:

- **At component level:** Components, such as controllers, can store complex behaviours or reconfiguration logics. This logic is detailed in databases in a format not usable when constructing models. This work characterized an input format as close as possible to the existing format used by engineers and created a tool able to translate this logic into AltaRica code.
- **At system level:** The system architecture is generally illustrated by a functional diagram that gives the high-level principles, but detailed information is then stored in dedicated databases depending on the system's topology. The work developed a way to translate this topology into as detailed a Failure Logic Model as possible. This implied the automatic creation of equipment / component with inputs / outputs and links.

The automated model construction concepts were applied successfully on various case studies, e.g. an Air Data Communication Network System. One of the results was a concept for automatically generating a systems resource component, called "MUX", that shows the host model only the useful information from a system resource. This methodology was further consolidated by the development of an 'integrated model', derived from several systems safety models created using various preferred modelling approaches: in order to integrate these models without the need to modify them, a MUX component was generated, that was partially achieved using hand-coding techniques and incorporated into the integrated model. This work highlighted the desirability and feasibility of a fully automated generation process.

1.3.2.3. Schematic 2 Model Transformation

MISSA WP4 has developed a Java-based Schematic to Model Transformation Tool (S2MT), which automatically interprets schematic designs e.g. of aircraft hydraulics systems, into model formats compatible with the Cecilia OCAS tool. In order to enhance the recognition performance of the S2MT tool as much as possible, the tool provides several options for the user to develop the best conversion performance. The tool contains two different vision-based recognition algorithms for the recognition process, orientation invariant solutions, a user feedback and revision function, library modification methods and global/ regional recognition. An interactive graphical user interface is also integrated into the tool, to assist the user. To date, the S2MT tool has been tested using an

experimental case-study comprising a component library and images. The tool's performance is not always optimum, but with help from the user and with properly pre-defined component attributes, the tool is able to detect most components effectively and to generate a model which can be recognised and used by schematic model design applications like OCAS. Use of this process may result in savings in the time and effort required for the re-use of existing systems designs that are only available as paper or on digital image files, and can also reduce the level of expertise required from the staff involved in the initial model construction process.

This tool has been developed as a functional prototype. The process for using the tool and the features of the tool make it feasible to use it today though there is an expectation for improvements to be made for the symbol recognition step to reduce the manual non-value adding activities.

1.3.2.4. Multi-Model Composition

Methods and processes were proposed to enable multi-system assessment in a realistic industrial settings. In particular, techniques were developed during this strand of work that allow for the relatively non-intrusive composition of system models defined by different stakeholders, and for their subsequent analysis. The composition approach allows the aircraft integrator/ airframer to take responsibility for model integration and overall aircraft-level safety assessment while also 'ring-fencing' suppliers' responsibilities for the generation of individual safety models.

The proposed techniques cover the technical aspects of model composition (harmonisation of interfaces, definition of translation components etc), of data interchange formats for models and associated guidance (covering, for example, component visibility and access rights in the library, library organisation and naming conventions), as well as a model documentation framework (the V&V portfolio). The project has then demonstrated though a practical example that model-based safety assessment of multiple integrated systems is feasible in an industrial context.

Further work in the area of model integration for MBSA is desirable. In particular, work should be carried out to investigate how the safety process could exploit results obtained from the observation of an aircraft Failure Condition by means of a multi-system model to facilitate the recognition of compliance / non-compliance with safety requirements, the independence level reached and the principal systems and sub-systems involved in the main contributory cut sets. There is also a need for a Simplified Interface Component – an interface-focussed abstraction mechanism - to tackle the complexity of aircraft-level safety assessment models.

1.3.2.5. Improved OCAS Analysis Engine

AltaRica is one of the main languages used for model-based verification and safety assessment. A variant of this dialect is supported by the Cecilia OCAS tool platform, developed by Dassault Aviation. The work focused on evaluating the OCAS tool chain through a series of case studies and identifying and improving the Cecilia OCAS tool in a number of directions:

- ***Treatment of temporal events.*** The semantics of temporal events have been clarified, and the native Sequence Generator has been updated to reflect the consensus view.
- ***Treatment of non-determinism between instantaneous events***. A special case of temporal events are instantaneous events identified in OCAS by the *Dirac(0)* "probability law". These are fired immediately after their guard evaluates to true. The execution order can be controlled explicitly by a *priority* operator. In some cases a deterministic priority cannot be meaningfully established.The tool can now be configured to detect and warn of non-deterministic conflicts.
- ***Performance with respect to model complexity***. Certain features of the models disproportionately increase the time-complexity of the sequence generation. A new sequence

generation algorithm was added in OCAS, allowing for exploitation of modern multi-core processing and distributed processing technology which solves this problem.

- ***Possibility of parallel analysis of multiple FCs***. The sequence generator was extended to be able to observe multiple failure conditions while performing a search of each permutation (i.e. sequence) effect on the set of observed failure conditions. For combined analysis, the stopping condition for a trace is the conjunction of stopping conditions for the analyses with respect to the individual FCs.

1.3.2.6. NuSMV-SA/ OCAS Plug-in

A new analysis tool based on the NuSMV model checker was developed for the Cecilia OCAS tool. NuSMV is one of the most powerful and popular model-checkers currently available. The development of the tool is motivated by:

(i) The limitations of the native sequence generator detailed above;

(ii) The objective of decoupling modelling and analysis tools and establishing interoperability between a number of alternative tools;

(iii) An opportunity to utilise some of the techniques for managing the complexity of models and analysis developed for the implementation level for the needs of the systems architectural safety assessment level.

The NuSMV/OCAS plug-in implements a translator to convert AltaRica models into NuSMV format. The translation uses HyDI as an intermediate language between AltaRica and NuSMV. HyDI provides primitives to deal with networks of automata, and different mechanisms for synchronizing them. The translator has been incorporated as a plug-in into the OCAS environment, and functionality has been made available via the NuSMV model checker, which provides standard BDD-based (CTL and LTL) model-checking techniques as well as SAT-based LTL Bounded Model Checking. The plug-in facilitates the performance of guided and random simulation and the re-execution of partial traces. It also provides optimised model-checking algorithms that aim to reduce the state explosion problem with techniques, which combine BDD and SAT for the verification of invariants. For formal safety assessment, the NuSMV/OCAS plug-in relies on an extended version of the NuSMV model checker – the NuSMV-SA Platform.

1.3.2.7. Export to RAMS Tools

Data interchange between the Cecilia OCAS tool and two other tools has been established, namely Isograph's Fault Tree Plus software and EADS-APSYS' SIMFIA tool.

Data interchange / export has been established between Cecilia OCAS and Isograph's Fault Tree Plus software. The primary goal of establishing interoperability between the tools is to facilitate adoption of model-based safety assessment methodologies by the industry while minimising the disruptive effect on existing processes in the companies. The achievement of interoperability contributes to the objective of decoupling modelling, quantitative, and qualitative analysis tools.

Adaptation of the SIMFIA quantitative analysis tool for Cecilia OCAS. SIMFIA is a mature tool capable of approximate calculation of average probability of failure conditions per flight hour. In addition to the goal of breaking strongly coupled tool chains, the objective of developing a new version of the SIMFIA tool that is fully compatible with Cecilia OCAS is to provide industrial partners with a functionality for more accurate calculations.

1.3.2.8. More Accurate Analysis

The calculation of the probability of system Failure Conditions is based on three technical concepts: Minimal Cut Sets (MCS), Component failure rates, and Check intervals.

The computation of probability figures is achieved using several different fault tree tools with at least two alternative stochastic models:

- ***Unavailability Model***. Under this model, a failure condition *F* is associated with the function $Q_F(t)$ which is, informally, the probability that *F* is present at time t. Typically, when this stochastic model is used, fixed exposure intervals are assumed[2] and $Q_F(t)$ is pessimistically approximated by the value that corresponds to the end of the exposure interval.
- ***Average Probability per Flight Hour***. This model is defined by the Airworthiness Requirements of CS25 paragraph 1309 (and associated guidance material) as: "a representation of the number of times the subject Failure Condition is predicted to occur during the entire operating life of all aeroplanes of the type divided by the anticipated total operating hours of all aeroplanes of that type (Note: The Average Probability Per Flight Hour is normally calculated as the probability of a Failure Condition occurring during a typical flight of mean duration divided by that mean duration)".

The majority of commercially-available fault tree analysis tools (such as ARBOR/ Aralia and Fault Tree Plus) are based on the Unavailability Model. Some tools developed specifically for the aerospace domain (such as SIMFIA) are capable of approximating Average Probability per Flight Hour. Both types of tools are widely used in the civil aerospace sector.

In the context of some maintenance and inspection strategies, the two probabilistic models yield significantly different results[3]. Some deferred maintenance strategies (e.g. dispatching an aircraft with an unserviceable item under the condition that a positive test result is achieved for other, possibly redundant, items) can introduce stochastic dependencies between seemingly independent basic events in Minimal Cut Sets.

A research report has been compiled on this issue by Airbus D[4] specifying the precise nature of the problem, surveying the current state of practice and art and identifying promising areas of further work / improvement.

1.3.2.9. Verification of DAL Allocation

A method has been developed that addresses the issue of *verifying* that a design respects Development Assurance Levels (DALs) allocation constraints.

ARP 4754 sets requirements, which must be demonstrated by the safety analysis, depending on the severity classification of the failure condition concerned. In addition to quantitative requirements, two types of qualitative requirement are set:

- The minimum permissible size (cardinality) of the minimal cut set, and
- The DAL(s) of the components that contribute to each cut set.

---

[2] The assumption of fixed exposure intervals may be very inaccurate for some maintenance and inspection strategies. In some cases the only obvious 'safe' approximation available can be as pessimistic as the life of aircraft (or, more realistically, a period of the C- or D- Check of the aircraft)

[3] The unavailability-based calculations in this context can yield significantly pessimistic approximation of the certification-mandated average probability per flight hour measure. This pessimism may greatly affect the maintainability characteristics of the aircraft as, thus, its competitiveness.

[4] With contributions from OFFIS and supported by discussion between DASSAULT and Alenia.

For Catastrophic and Hazardous failure conditions, the Standard permits two alternative DAL allocation strategies. In one of these, a single component is allocated the highest necessary DAL. In the other, it is permitted to reduce the DAL by one level at the cost of allocating this level to at least two components in a cut set.

Provided that all dependencies between system components are captured by the safety assessment model, verification of these rules can be carried out by an algorithmic inspection of the minimal cut sets for a given failure condition in the context of a mapping between components and DALs. Logically, such an allocation would comprise two steps:

1. A translation of minimal cut sets into the vocabulary of DALs;
2. An examination of whether each translated minimal cut set respects the DAL allocation constraints.

During the MISSA project, the Compare tool has been developed and adapted to automate the verification task. The Mapping tool facilitates the definition of the DALs of different components.

1.3.2.10. Model Symmetry Verification

MISSA investigated the structural property *symmetry*. Many aircraft systems (and their models) are based on the principle of symmetrical structure: the standard "Side 1 / Side 2" architecture of aircraft systems, for example. Consider the simplified architecture of an Aircraft Electrical Power Distribution System in Figure 9. The system is clearly symmetrical. It can be divided into three parts ("sides"): Side 1, Side 2 and Essential Side. Side 1 and Side 2 are clearly symmetrical – they contain identical types of components in identical arrangements. In this case, 'Side' may be regarded as an axis of symmetry.

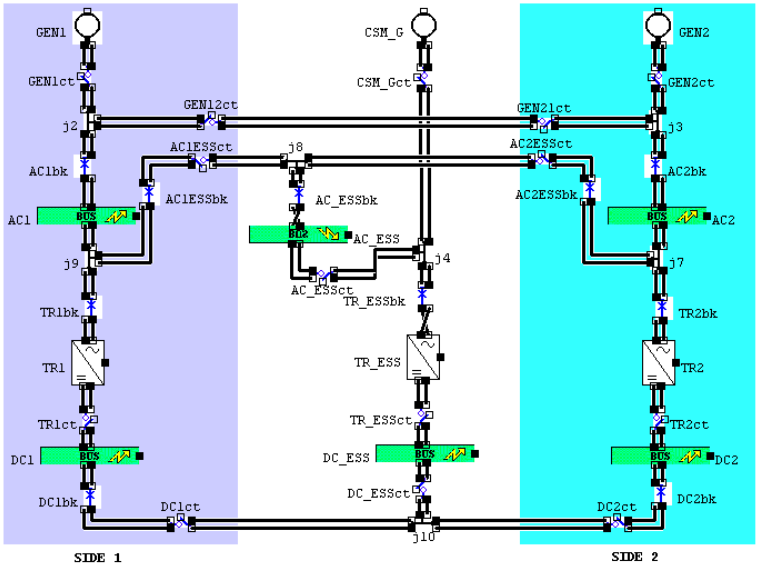

Figure 9 - Electrical Power Generation and Distribution System

Naturally, we expect that the symmetry property will be reflected in the analysis results.

The (informal) definitions of symmetry conditions above would be simplified if we were to consider that all components that lie on the axis of symmetry (and their respective failures) are themselves symmetrical. Then we can say that "symmetry" is a binary relation – or a mapping – between two component failures. This relation is on a single set (set of all unique failures in the model), it is a bijection, and – unsurprisingly – it is symmetrical.

Most importantly it is a mapping that can be easily handled by following a procedure using the Mapping Manager and the Compare tool described in a following sections. So whilst symmetry properties cannot be checked using a sequence generator, if the sequence generator is used to generate results for individual failure conditions then the mapping and comparison tools can be used to check whether expected symmetry properties hold in and between the results files.

Checking symmetry properties appears to be an interesting potential approach to model validation, which "tests" the model from a somewhat different perspective to that held by the engineers who defined it.

1.3.2.11. Light Weight Refinement & Compare Tool

A tool was developed that enables the comparison of results between stages of refinement. The comparison of the results is based on the following notion of *refinement*.

The definition assumes that Minimal Cut Sets are defined over the same set of literals (i.e. failure and component identifiers). Informally, the idea is that fault tree F_2 is a refinement of F_1 if a single failure in F_1 becomes a single (or double or triple) failure in F_2 due to "refinement of analysis". The converse should be forbidden: a double failure in F_1 should not become a single failure in F_2. Informally:

> *For every minimal failure combination A_2 related to F_2 there exists (at least one) failure combination A_1 related to F_1, such that A_1 is a subset of A_2.*

A stepwise approach was developed for comparing results. The comparison process is based on the following steps:

1. Identification of the results (or model) files, and establishment of unique elements (failures and/or failure modes).
2. Interactive establishment of a mapping between the two models – establishing equivalence relationships between the two vocabularies.
3. Preparation of the result file identified by user as "abstract" for comparison: here, the abstract results are translated into all possible concrete interpretations. This allows a comparison to be performed over two *homogeneous* sets of results in the next step of the process (below).
4. Discovery of every MCS in the concrete results that breaks the "refinement" relationship, if any exists.

The comparison between safety results obtained for two models – 'abstract' and 'concrete' – has been found to be very useful in analysing the quality and meaningfulness of the results, answering the question of whether the new / concrete analysis has forfeited any commitments from the earlier / abstract analysis. It is possible to perform comparisons between results from different tools.

1.3.2.12. Model Mapping Concept & Mapping Tool

A graphical tool has been developed to aid the definition of the mapping between models (i.e. steps 1 and 2 of the process above). The tool allows the user to open two files: each being either a model file or special export file that contains a list of a model's unique failures. The tool then presents the user with a GUI (Figure 10), which lists all of the unique failures of two models in a hierarchical fashion and allows the user to establish mappings through a simple and intuitive "drag-and-drop" functionality. The tool not only permits one-to-one mappings between two individual failures of two respective components, but also provides shortcuts for the definition of various one-to-many

mappings as well as sets of mappings of predefined general shapes[5]. Use of the tool is not a "one shot" exercise. The tool allows the user to load and edit a previous mapping file, and also to add new mappings or delete incorrect ones.

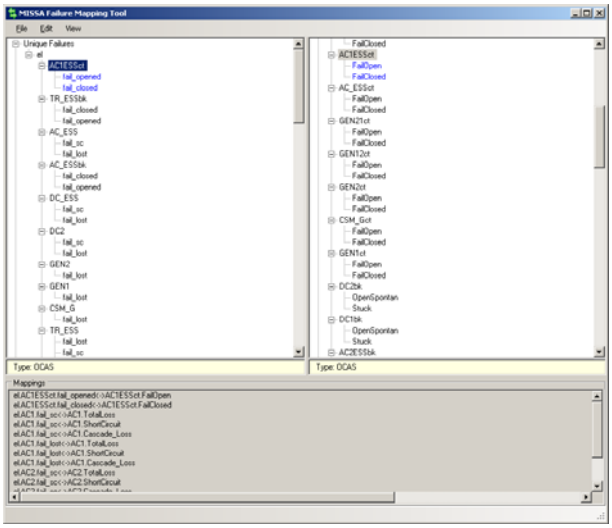

Figure 10 - Graphical User Interface (GUI) of the Mapping tool

1.3.3. Systems Implementation Level Modelling and Analysis

This work package has delivered six new capabilities to support methodology and tools for qualitative assessment, and two capabilities related to model correlation. The capabilities are described below.

1.3.3.1. Time Compression

Real time systems usually contain operators that count execution cycles. In a synchronous model each cycle has a fixed time length, so we will generally refer to such operators as *timers*. The Prover SL DE proof engine, used in the SCADE Design Verifier, has a specific construct intended for modelling timers that can be used for modelling any *linear function over time*.

By using the timer construct, we enable the proof engine to compress long sequence of cycles into a single transition. This often leads to significant time saving and smaller memory foot prints. The basis for this *time compression* technique is the observation that cycles in which nothing but values of timers change, do not need to be considered individually. This is achieved by generalizing the basic transition model used in the analysis, such that timers may be updated several times in each transition. The difference is illustrated in the diagrams below.
Time compression can improve the analysis performance greatly, but depends on the ability to identify states where nothing but timers change. If some system timers are not mapped to the accelerated timer construct, or if the properties analysed depend on other functions over time, the time compression may not be effective.

[5] For example, it is possible to create a many-to-many mapping between all of the failures of some abstract component *A* and some concrete component *C*, by simply dragging *A* onto *C*. Alternatively, a set of one-to-one mappings from each failure of *A* to a parallel failure of *C* can be created (by dragging one component onto another while keeping the CTRL key pressed)

The Time Compression Capability was developed. Experiments were carried out on small models and isolated parts of larger models, showing positive results. Difficulties were encountered when working with large models, as identifying all variables whose value changes while waiting for timers can be difficult. Work concluded by focusing on minor improvements, bug fixes and support to users to help convert existing SCADE models to evaluate time compression.

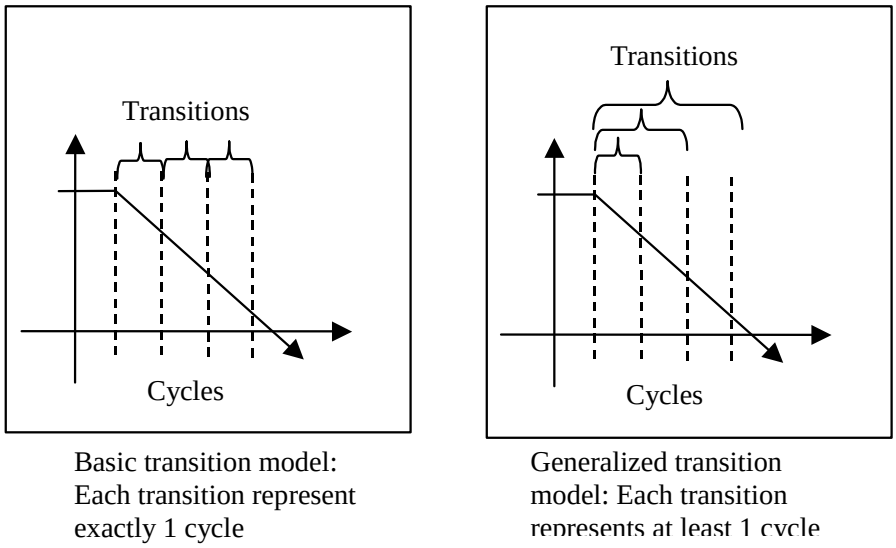

Figure 11: Illustration of A Basic and the Generalized Transition Model used in time compression

1.3.3.2. CEGAR-Abstraction and Abstraction/ Refinement

This work is based on Counter-Example Guided Abstraction Refinement (CEGAR) illustrated below.

CEGAR uses conservative abstractions, i.e. each trace in the concrete space has a counterpart in the abstract space. So, in the case of invariant properties, if the analysis in the abstract space reveals no bugs, then the concrete system is also correct. However, if an abstract counterexample exists, there may not be a corresponding counterexample for the concrete system. Such an abstract counterexample is then called a *spurious counterexample*. Then, abstraction-refinement iteratively tries to discover a new more detailed abstract model, that rule out spurious counterexamples until the property is either proved or disproved. This is done by extracting information from counterexamples generated by the model checker.

The ISAAC project considered abstraction refinement, but didn't manage to automate it.

In the MISSA project, predicate abstraction has been implemented. The abstraction algorithm has been integrated in a complete CEGAR loop, and implemented in the NuSMV model checker, combined with the MathSAT SMT solver. The experimental evaluation has shown very promising results.

The following points have been left for future investigations:

- Evaluation of abstraction refinement in the Altarica/OCAS implementation line.
- Use of abstraction refinement (CEGAR loop) for verification (SMT-based Bounded Model Checking) of hybrid models.

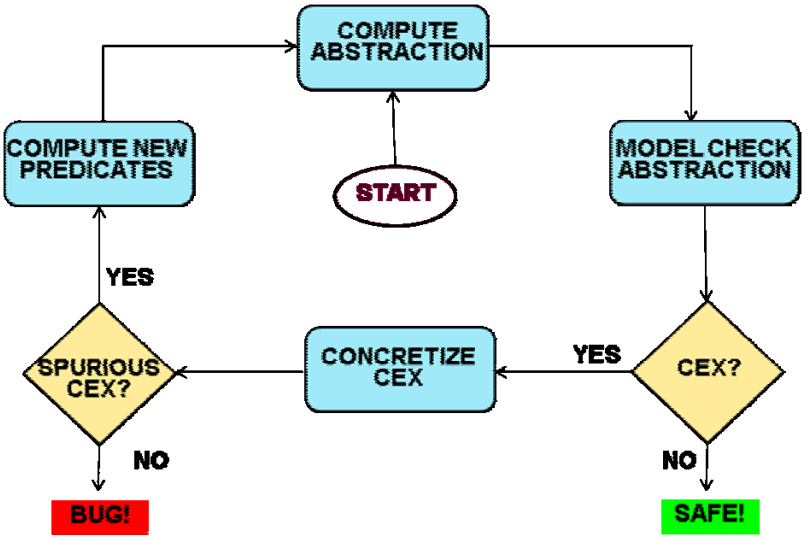

Figure 12: CEGAR Loop

1.3.3.3. Monte Carlo Simulation Techniques for Large Model Analysis

Results from methods based on model-checking are good but complexity is a primary issue and simulation as an analysis technique can offer solutions for many of them.

- Simulation can easily cope with models that are larger by several orders of magnitude and which contain features not supported by model-checking.
- Simulation can analyse very long systems runs
  - traces can cover several hours of simulated time, even when very small/ simulation steps are required.

A simulation based FTA has been developed and tested during MISSA. It makes use of the basic methodology for model based FTA that has been adopted from ESACS and ISAAC.

Evaluations that were performed have shown the following results with respect to the performance of the simulation based FTA:

- On very small models is it slower than model-checking, which is expected since there is an overhead in the setup for the analysis task (code generation and compilation) as well as due to the time that is required to sample a large enough number of simulation runs required to reach good coverage.
- On medium and large models the performance is very good.

The major drawback however is that the generated analysis results are not guaranteed to be complete. This problem has two different aspects. First there is the problem that the generated cut-set are minimal only with respect to the investigated simulation runs and second, not all cut-sets may have been identified. This limitation may be addressed by developing a hybrid approach that combines simulation with model-checking. Further work is required to improve the simulation based analyses in these areas.

1.3.3.4. Low-Level Verification Techniques (NuSMV-SA)

The implementation of BDD-based routines for Fault Tree Analysis was first undertaken in the ESACS project. In the ISAAC project, two main extensions were achieved. First, BDD-based

routines were optimized by implementing *dynamic pruning*. Second, SAT-based routines, using Bounded Model Checking (BMC) were implemented.

The main achievements within the MISSA project include the implementation of improved SAT-based routines for Fault Tree Analysis - based on Simple Bounded Model Checking - with completeness checks, and the integration of BDD-based and SAT-based routines for Fault Tree Generation.

The routines described above have been evaluated within OCAS, and they have shown that the (complete) mixed BDD/SAT based routines may be more efficient than purely BDD-based routines, and competitive with purely (incomplete) BMC-based routines.

1.3.3.5. Hybrid Model Checking

During MISSA, a preliminary analysis and translation from the Matlab-Simulink environment to the NuSMV model checker was developed that provides a limited conversion capability. Concurrently, some technological advances, including the introduction of interpolation based routines, for verification of hybrid models, based on SMT model checking, were added to the NuSMV engine. In this framework, an important result was the full integration into NuSMV of the MathSAT SMT solver and the deployment of complete decision procedures for safety properties relying on SMT techniques.

The main development activities related specifically to hybrid model checking involved:

- The identification of suitable user-level modelling guidelines (syntactic restrictions)
- The definition of a formal semantics for the language, based on the theory of hybrid automata
- The design and development of a translator from MATLAB-Simulink to NuSMV, based on the HyDI intermediate language
- The design and development of a Matlab plugin, used to expose all of the aforementioned functionalities to the end user, hiding tool complexity behind an easy-to-use GUI
- FTA and FMEA procedures have been developed and integrated in the plugin

The development and evaluation of the toolset has been performed in close loop with the users. In particular, the formal semantics has been defined taking into consideration feedback and expectations of Matlab users. A point of improvement for future work is the relaxation of some of the restrictions that are currently enforced at modelling level, and the support for additional Matlab blocks and constructs. Finally, future work could address the implementation of automated techniques to carry out approximation for non-linear systems.

1.3.3.6. Non-Linear Arithmetic

This technique aims at improving the SCADE Design Verifier to add support for non-linear constructs.

The SCADE Design Verifier relies on SAT-based symbolic model checking to verify safety properties. It supports bounded model checking for the purpose of producing counter-examples. In the case where the system fulfils the requirement, proof by induction is used. SAT-based model checking is capable of handling Boolean systems, i.e. systems where the only data types used are either simple Booleans, or composite data structures built on top of Booleans. SAT-based model checking can be extended to support numeric data types by translating non-Boolean data to Boolean, which can be done in the case of data types with finite domain such as bounded integers. SCADE Design Verifier uses this technique.

Support for debugging non-linear systems is a new capability of the SCADE Design Verifier developed during MISSA. The feature should be considered experimental, and its applicability to industrial-scale models is currently limited. Although non-linear solvers such as SUNDIALS KINSOL have been successfully used to analyse systems with hundreds of variables, they require a significant amount of manual tuning and expertise from users. Integrating a non-linear solver in SCADE Design Verifier and making it user-friendly would require the development of pre-processing algorithms capable of extracting good sets of parameter values for the non-linear solver. The ability to produce sequences of input values for non-linear systems has multiple applications, ranging from understanding systems with design faults, producing dynamic cut sets, automatically generating test cases and simulation stimuli.

1.3.3.7. Contract-Based and Compositional Reasoning (Using HRC)

Contract based Modelling promises to improve scalability, compositionality and abstraction. Re-use of components and design patterns, developing libraries of design components and better support for using COTS (components off the shelf) are use-cases that benefit from this approach. Existing designs can be easily changed in order to adapt for new requirements or to support product family development.

The main initial work in MISSA was focussed on adapting and extending contract based specification methods for checking compliancy between contracts and implementation.

- Extending the HRC framework from SPEEDS with the necessary methods for safety analysis.
- Develop suitable formalism for specification of safety requirements and failure-modes in the context of a contract.
- Implementing techniques for model based FTA and FMEA, developed during ESACS and ISAAC, based on the (extended) HRC framework.
- Developing export tools that allow the translation of models from high level COTS modelling tools (IBM Rational Statemate) into HRC

Subsequently the initial tool-chain was further refined and extended. The main improvement has been to adapt to new development in HRC. The CESAR project has taken up the HRC formalism from SPEEDS and further enhanced and improved it. One especially important addition is a new language for formalization of requirements and system properties to be used in the definition of contracts. The RSL (Requirement Specification Language) provides several patterns that enable the user to easily formalize system properties in a language that is both easy to use (because the patterns are constructed to resemble natural language requirements) and at the same time has a well defined formal semantics which is necessary for it to be usable in the model based FTA.

1.3.3.8. Comparison of Safety Results Between WP4 and WP5 Models

This topic is concerned with establishing a link between safety results obtained in WP4 and in WP5 for the same model, at different levels of detail. In general, the link between the two models is a sort of refinement, that is, the implementation-level model is expected to be a refinement of the corresponding architectural-level one. Similarly, it is expected that the safety results obtained at the two levels enjoy a corresponding notion of refinement.

The core principles of a comparison process – including definition of the lightweight refinement relation – were developed. Two tools were developed that are used to implement the comparison

process. The tools ensure that all formats of analysis results, used by MISSA partners, can be treated without the need for manual pre-processing. They currently accept XML and textual file formats generated by the native sequence generator of the Cecilia OCAS modelling tool as well as SCADE/FTA-manager analysis tool. The tools are:

- A graphical Mapping Tool developed by ATEGO that is used to establish “equivalence” relationships between the two vocabularies from the architectural and implement level models.
- A command-line comparison tool developed by FBK that translates abstract results into all possible concrete interpretations thus allowing the comparison to be performed over two homogeneous sets and finding every (if any!) MCS in concrete results that brakes the “refinement” relationship.

The comparison between safety results obtained for architectural-level models (WP4) and the corresponding implementation-level models (WP5) answers the question whether the new / concrete analysis has forfeited any commitments of the earlier / abstract analysis. This facilitates the iterative and incremental approach to system safety assessment called for by ARP4754 and ARP4761 documents.

Furthermore, the flexibility of the developed tools allows their use in the context of multiple “competing” models of the same system and for validation of the new model analysis tools developed in the MISSA project.

1.3.4. Synthesis Argumentation and Change

This work package has delivered four new capabilities to support Argumentation Methodology & Evidential support by Safety Assessment Models, two capabilities related to Synthesis of Safety Assessment and four capabilities related to Synthesis, Argumentation and Change Tool Support. The capabilities are described below.

1.3.4.1. Primary and Backing Arguments and Modular Arguments

In MISSA, the feasibility of the adoption of an argument-based approach into the demonstration of aircraft safety and the justification of the validity of safety assessment models was extensively explored. MISSA elaborated argument-based methodology as applied in civil aerospace in three aspects.

1. Clarification of argument-related concepts. The concepts of claim, argument and evidence are clarified within the context of aircraft safety assessment and safety synthesis.
2. Differentiation of primary and backing arguments .The role of safety cases was further distinguished into two parts. The primary argument aims to address safety concerns and demonstrate compliance with various safety requirements. The backing argument, on the other hand, addresses the concerns of the validity of both traditional and novel safety assessment models.
3. Modular organization of safety arguments. The amount of data from safety assessment and justification along with aircraft development process can be large. For this reason, the notion of modular arguments was introduced in MISSA in order to help the management of the increasing scale of the structure of safety cases.

1.3.4.2. Argument Construction and Review Process

As a part of MISSA's WP6 tasks, a guide was authored that explores and develops the structure of arguments for aircraft safety. The objective of the document is to provide guidance to engineers on how to link together the safety objectives of aircraft systems and the results of the safety assessment performed on them. The document is intended to assist and facilitate the application of safety arguments in the MISSA project. Firstly, guidance on the key concepts of safety arguments, the symbols of Goal Structuring Notation (GSN), and the safety argument construction process are given. Then the updated argument structures/ patterns developed for the MISSA project are described. Some exemplar arguments are constructed on the basis of the argument patterns presented in this report. The report has been updated to account for feedback from its use during the MISSA project.

1.3.4.3. Set of MISSA Safety Argument Patterns (For Certification, Primary and Model Adequacy Arguments)

Three types of argument patterns were developed. Certification, Primary and Backing Argument Patterns. The Certification Argument Pattern shows how the airworthiness regulations are justified by the various means of compliance. The Primary and Backing Argument Patterns are sub-grouped according to project work packages. The primary arguments that were developed are in-line with the safety argument components of an 'assured safety argument'[6]; the backing arguments serve the same role as the 'confidence argument' components of an assured safety argument. Separating these two interrelated parts explicitly helped us to have a better view of what the direct evidence is offered in support of a given claim and why we can trust the evidence on an individual basis.

The 'primary' argument that was developed within MISSA, directly documents how the results of the safety analysis models in the project address the satisfaction and decomposition of the top-level safety objective. The standard ARP4754A provides a clear thread for primary arguments of aircraft safety. MISSA developed three primary argument patterns: a primary argument pattern related to Aircraft Level Modelling and Analysis (WP3), Systems Architecture Modelling and Analysis (WP4), and Systems Implementation Level Modelling and Analysis (WP5).

The backing argument addresses issues concerning the degree of confidence, which can be placed in the results of the primary argument – i.e. why the results of safety assessment models should be trusted, and whether these models are good enough to satisfy their modelling intent. In the MISSA context, the backing argument pattern may also be referred to as the model adequacy pattern. Three backing argument patterns were developed for MISSA related to WP3, WP4, and to WP5.

The patterns were considered for each of WP3, 4, and 5 in the context of the Brake Control Function Case Study.

1.3.4.4. Model Justification Concerns & Assumptions Classification and Management

Assumptions in safety assessment are an important issue. Practitioners of "safety analysis and review" constantly make assumptions about the system under study (e.g. the function, composition, failure mechanism, operational procedure, environment, or data). It is observed that 'inadequate identification of assumptions about the relationship between a model and the system it models, or between the environments of the model and what it models, may result in unexpected differences

[6] Richard Hawkins, Tim Kelly, John Knight and Patrick Graydon, A New Approach to creating Clear Safety Arguments, in Proceedings of 19th Safety Critical Systems Symposium (SSS'11), February 2011

between predicted and actual behaviour of that system'[1].

A review was performed of what kinds of assumptions are made and how they are reported and managed. We have proposed an embedded assumption management process in the safety assessment process to stress the importance of assumptions in justifying the adequacy of models. A classification of modelling assumptions is also presented from the feedback of some of the exemplar assumptions in the novel models built in the project.

1.3.4.4.1. References

1. Shore, A., *Managing assumptions for safety critical projects*. Computer Science Msc Thesis. 2008: Department of Computer Science, University of York.

1.3.4.5. Certification (Verification/ Validation) Dossier

The adequacy argument described above provides answers on the issues of the confidence in the results of the primary argument. It is based on the performance of a Validation/Verification activity (including reviews) in accordance with the ARP 4754A. This Validation/Verification activity generates a deliverable (the Validation/Verification dossier) subject of a review:

The structure and content of the dossier has been detailed based on an understanding of what is required from an airworthiness perspective from experienced members of the MISSA project that have participated in certification reviews with the airworthiness authorities. Each MISSA model shall be associated with a Validation/ Verification dossier.

A complete Validation/Verification dossier content is provided in MISSA D6.20 Appendix C. This dossier should be built with the information contained in the MBSA tool. It addresses the Validation/Verification of the model, observers as well as the verification of the technical results of the model activation to perform a MBSA.

1.3.4.6. Integration of Argumentation and ARP Safety Process

Within MISSA the integration of safety arguments with the well-accepted ARP safety process was established on the basis of safety review activities and a variety of safety deliverables. The information flow passing through the system development activities, system safety activities, and the safety model validation activities was defined. Two types of relationships were established for the integration, the relationships between safety requirements and safety claims, and the relationships between safety assessment outputs and evidence. Furthermore, the informal and implicit inference steps between safety requirements and safety analysis outputs were explored. MISSA showed how these inference steps can be presented and enforced through argument construction. A typical information flow with WP5 modelling and justification is shown in the following picture.

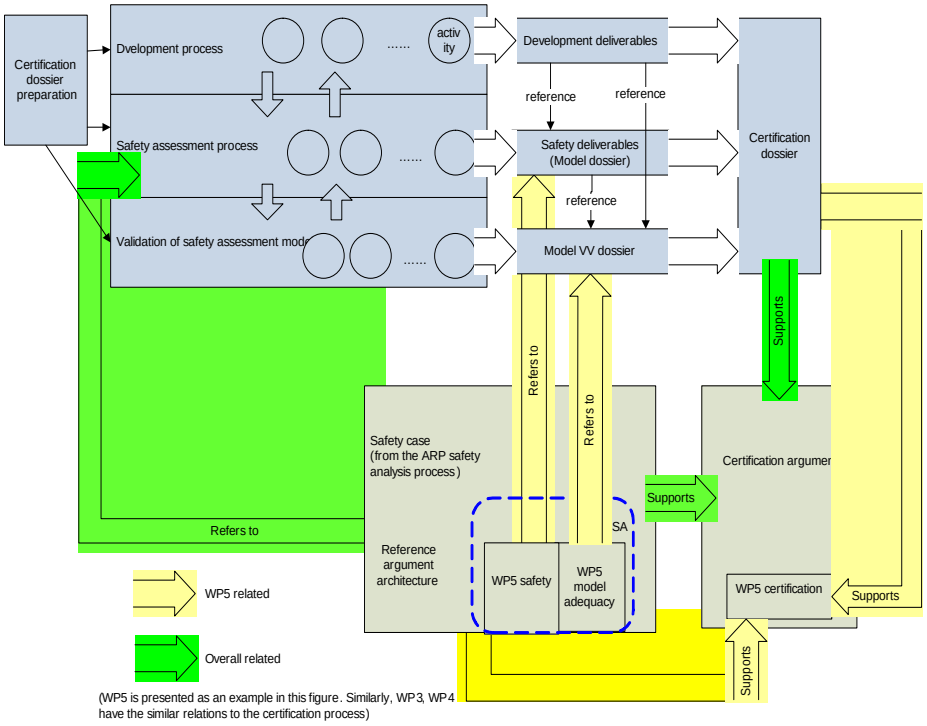

Figure 13: The relationship of arguments, deliverables, safety process and certification

1.3.4.7.Inter Model Tracing Support for SCADE & OCAS Models

SCADE Tool Integration: A new integration with Esterel SCADE 5.1.1 has been developed to allow SCADE entities to be created, updated and maintained within Atego Workbench. This version of SCADE does not have an API and so cannot be automated by Atego Workbench. As a result the integration required the user to use SCADE in a slightly modified way to standard file-based entities. The use of SCADE within Atego Workbench is described in more details in D.4.7.

OCAS Tool Integration: A new integration with OCAS 4 has been developed to allow OCAS entities to be viewed and version controlled within Atego Workbench. However, Workbench does not support live tool launching of OCAS, so it is not possible to develop the entity within Workbench. An OCAS entity is updated via the import mechanism, which supports the native OCAS export file type (*.exp). OCAS entities are viewed using the Atego Workbench Viewer. Tracing is supported to element level with many elements types valid for tracing.

HRC Tool Integration: Access to HRC data is provided using the generic tool integration, providing a capability to import and store HRC data in Atego Workbench. There is future scope to provide HRC tool integration, similar to the OCAS integration, allowing the user to view an XML representation of the data in the Atego Viewer, with trace support for individual elements.

1.3.4.8.TALE (Trace & Link Engine)

The Atego Workbench initially used DOORS to support its traceability functions. This had some severe limitations in terms of performance and capability. The traceability also required a DOORS license, an expensive licensing overhead if DOORS was not the tool used for requirements management. During the 2nd cycle a rich trace and link engine (TaLE) that provides greater functionality and a more generic solution based upon a relational database has been developed. This has its own API and is capable of supporting link sets for entire projects that can be version rich. It also offers improved reporting capability that can be tailored to the requirements of any project.

The TaLE has been integrated into Atego Workbench using a service, which is interchangeable with the original capability supported by DOORS. This enables existing users to continue with the DOORS version using existing functionality.

For those connected to the TaLE service additional features include:

- A migration from the old DOORS traces to new TaLE database.
- Provision for configuration of trace relationship types and states.
- Access to the historic traces.
- Improved traceability view report, giving clearer information.
- Ability to save the traceability report output as a PDF entity.
- The Atego TaLE is license free to Atego Workbench users.

Atego Workbench does not currently support PDF files as input to the DocGen tool. This is a possible future enhancement.

1.3.4.9. Change Management for Arguments and Traces

MISSA looked at the management of change within the safety engineering domain and considered this in the context of modelling to ensure that system safety is evaluated and maintained.

The intent was to model and automate a change management process such that it is controlled and is as automated as possible within the tool environment to increase the efficiency of the process.

It is important to remember that this work package is concerned with change management of the argument and also all the design information for the system.

A great deal of emphasis is placed upon traceability within the standards and guidance that are central to the MISSA project. This is evident in the construction of a safety argument. The argument is constructed and this in turn links to evidence. This linkage is one example of traceability and is the key to the argumentation process. Once traceability has been established between the argument and the evidence, then this data is put under configuration management – i.e. copies of the argument and its corresponding evidence are placed in a secure read-only environment. For safety critical systems this configuration management is key in gaining approval from regulatory bodies and allowing the system to be used. Once the argument has been established, the evidence provided and the approvals gained, then this data needs to be rigorously maintained to ensure that unauthorised changes are not made to the system. The way that any change is made is subject to Change Management.

A change process has been devised, and is supported by the Atego Workbench, to address all of the needs identified for the safety process. The change process is described in D6.20.

1.3.4.10. ATEGO GSN Modeller Improvements & Integration with Workbench

The MISSA project has enabled Atego to enhance both the Atego GSN Modeler tool and the integration of this tool with Atego Workbench.

The Atego GSN modeling tool initially was only provided as an integral part of the Atego Workbench product. As part of the project this has been decoupled to enable the partners and future users to enjoy the benefits of GSN modeling in a standalone environment; but they still are able to

maintain the benefit of being able to bring models into the controlled environment of Atego Workbench.

Improvements to the integration of the Atego GSN Modeller with the Atego Workbench include:

- Atego Workbench has been updated to permit the import/export of GSN entities, which are classified as repository based tools. The update has been made in such a way that it will be possible to add this functionality to other repository-based tools on a case-by-case basis.
- The “recover” capability is now available for GSN entities that allows if required to overwrite the latest version of a GSN with a version recovered from the past.
- The provision of logical and branch entities for GSN modeler entities

Improvements to Atego GSN Modeler include:

- The GSN Modeler has been enhanced to support GSN Templates. There is still scope for more improvement, ideally when a template is used within a GSN entity; it should reference an Input Resource to provide control over the version and user access. Other tools like DocGen and EMT use Input Resources – controlled versions of entities. At present any template can be used/ accessed from within a GSN entity.
- Correction of errors in the XML data that is generated prior to a review taking place, and used for import/export.

1.3.5. Conclusion

The objectives of the MISSA project were to develop systems safety analysis methods and tools that lead to a reduction in the time to complete subsequent design iterations, offering a reduction to the development costs, giving more time to the engineers to achieve greater levels of performance or weight optimisation, or to have an increase in agility of design.

Starting with various modelling and analyses approaches that were defined within a number of previous project (ESACS, ISAAC, SPEEDS, CESAR), the MISSA project has extended the modelling approaches to better fit the needs of the systems safety development process as defined by SAE ARP4754A and have developed the necessary prototype tools to use, analyse, perform optimisations, and trade studies, for the systems and their installations that these models represent. Additional tools were developed to help with the speed for assessing the validity of the models, reviewing the large sets of results, highlighting the differences between the evolution and refinement of the design, and showing the compliances and non-compliances to the development assurance level required.

The transverse theme has further developed and demonstrated the application of an argumentation framework to bring together the models, results and supporting validation and verification evidence, and to control the management of information in order to allow the use of these models within a certification process. The organised layout of the evidence, traceability and navigation improves the control of the design tasks as well as the speed of review.

The evaluations have been performed on various sized case studies from toy examples to industrial sized case studies.

The final result is the successful advancement and/ or delivery of 37 capabilities. With these, MISSA has delivered capabilities that should enable design organisations to respond to changing market demand through the design life, and to improve the means to maintain the complete chain of evidence between safety claims and the evidence used to substantiate it.

1.4. The potential socio-economic impact, wider societal implications of the project so far, and the main dissemination activities and exploitation of results (not exceeding 10 pages)

1.4.1. Potential Socio-Economic Impact:

Potential impact and use: A series of EU-wide research projects have demonstrated the applicability of these novel approaches to the complexity of real aeronautical systems; which has led to a partial up-take by some European aeronautical companies. The uptake so far is being applied through the use of internal approaches to modelling. The work developed in MISSA so far has produced guidance material that is being targeted to the industry standards bodies as a step towards harmonising these approaches across the industry. Additionally, tools have been developed not just to demonstrate the feasibility but also to eventually be made available so that the approaches can be put to industrial use.

The socio-economic impact: Recently similar research has emerged outside the EU, e.g. USA. Hence, the opportunity to convert the research lead into a competitive EU industrial advantage is time-limited. The experience gained from the evaluation cycles show the promise from some of the developed techniques to significantly reduce the time and hence increase the agility of the systems developers, allowing them to produce better performing products within shorter time frames. This clearly strengthens industries socio-economic position so long as it is ready to be applied within a timely manner compared to the competition.

1.4.2. Wider Societal Implications of the Project so Far:

Wider societal implications of the project so far: MISSA has addressed key FP7 objectives in Aeronautics such as helping to reduce a/c development costs, creating a competitive supply chain to halve the time to market and reducing the accident rate, and contributes to achieving wider objectives set-out in the ACARE strategic research agenda, such as highly cost efficient, and ultra secure air transportation system, contributing to the fulfilment of the Lisbon Agenda and yielding real benefits in terms of competitive advantage of EU industries.

The MISSA project has produced a range of capabilities that will have different times to maturity. Some of the capabilities are quite mature that are either in a position to influence the use of the currently applied tools and so are immediately industrialise-able, others need some additional consideration by the industry as a whole but are, nevertheless, close to industrialisation. MISSA has also produced some capabilities that are much less mature and as such will require further research before they are ready to be applied industrially.

1.4.3. Main Dissemination Activities:

There have been four types of dissemination activities, workshops, publications, exhibitions and the project website.

Dedicated workshops: were organised for the MISSA Project and on Model Based Safety. The objective of the workshops were to present on the progress of the various work packages to a

specifically targeted audience. The intention was to receive feedback from the workshops regarding the ideas that were presented, the problems that were encountered, and to also give an opportunity to have competing ideas to present their progress, to encourage a discussion about what is the best way forward. The four workshops that were organised are:

- Model-based Safety Assessment - Journées MISSA-CISEC (Club Inter-association A3F SEE SIA des Systèmes Embarqués Critiques), February 2010, organised by ONERA.
- 2nd MISSA Workshop (co-located with IET System Safety Conference), October 2010, organised by UoY
- MISSA Dissemination Event Presentation: Formal Verification of Models Containing Non-Linear Arithmetic, March 2011, organised by AUK
- Model Based Safety Assessment Workshop, March 2011, organised by ONERA

Exhibitions: MISSA partners participated to two Exhibitions in order to disseminate and encourage research, namely:

- Researchers night 2010, FBK
- Digital Shoreditch Festival, 05th – 7th of May 2011, QMUL

Publications: Additionally there were 26 Publications in the form of a book and 25 peer reviewed conference papers, the full list of papers can be found on the project website.

Project Website: A project website was set up to provide general information regarding the project. The website has accumulated more than 10,000 visits with peaks occurring just prior to and after the dissemination events. The list of visitors has been looked at and a significant number of universities, research organisations as well as recognised industrials have visited the site.

Month	Daily Avg				Totals					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
	107	83	57	15	5431	842348	13978	51885	76116	97651

Figure 14: Website Data and Visit Statistics

- The project website. <http://www.missa-fp7.eu>

The most valuable resource in terms of making connections was through the organisation of workshops, presentations at conferences and the exhibitions. The website has given a good mechanism to collect statistics regarding who is interested and how interested they are simply by looking at the number and frequency of visits by particular companies and the amount of data they have downloaded each time and in total. The following lists the Engineering Companies, Research Organisations and Institutes and Universities that have visited more than once.

List of Engineering Companies, Research Institutes and Universities that have visited the website more than once.

Adelard
ADIT
Aeroconseil
Aerospace Valley
Aristotelio University of Thessalonica
Astrium
Audi
BAE SYSTEMS plc
Bureauveritas
Centre de Recherche Public Henri Tudor:
CENTRE NATIONAL D'ETUDES SPATIALES
Computer Science Laboratory - SRI
Critical Software
Daher
DASSAULT SYSTEMES
Dept. of Electrical & Electronics Engineering – METU
Dublin City University
EADS CASA
EADS Astrium
Electricite de France Service National, R&T / ONR
Embedded Engineering and Enabling Solutions
Embraer
ENSEEIHT
ESSCA
European Space Agency
Ford
FR-SNECMA
Grenoble Institute of Technology
IET
Infineon Technologies AG
Institut National De Recherche Et De Securite
Institute for Experimental Software Engineering Fraunhofer Institute
IRISA – Institut de Recherche en Informatique et Systèmes Aléatoires. (CNRS)
Irit
ISAE
Japanese Aerospace Exploration Agency
Karolinska Institutet
LAAS
Ludwig-Maximilians-Universitaet Muenchen
Megatel
Microsoft Corp
Tohoku University
Oldenburg University
Piaggio Aero
PMDTEC
Project Place
Prover
PSA PEUGEOT CITROEN
Queens University of Belfast
Resilans AB
Rohde & Schwarz Instrumentation
Manufacturer
Satellite Services
SESAR Joint Undertaking
Snecma - Villaroche
Softcom Technology Consulting
Stanford University
Supelec Grand Ecole
Technical University of Muenchen
Tecnalia
THALES SYSTEMES AEROPORTES S A
THE BOEING COMPANY
Science and Tech. Research Council of Turkey
Turbomeca
United Technologies Company
United Technologies Research Center
Università degli Studi di Cassino, Facultà di Ingegneria - GARR Italian Research and Academic Network
Universität Karlsruhe (TH), Institut für Produktentwicklung
University College Cork
University of Agder
University of Zilina
Uppsala universitet
valeo
VDO (Continental Automotive GmbH)
Volvo

1.4.4. Exploitation Results:

The ESACS, ISAAC and MISSA projects have developed and matured methods and tools in the field of model based safety. In order for these techniques to be adopted there is a need to ensure that the techniques are familiar to the practitioners and that the practitioners are happy to use them, that there is a business case for the vendors to want to support them, that the manager are sufficiently aware of the techniques to be happy to trust their practitioners to use them, that aircraft programmes are happy with the means of compliance evidence that is generated by them and finally that this evidence can be accepted by the relevant authorities as the way to demonstrate the safety of the aircraft systems. The following section describes the types of exploitation that is being carried out, the activities that are working to ensure that exploitation is successful for every respect.

It is believed that due to the nature of the technologies that have been developed, that the targeted area of industrial exploitation will be:

- By the Industrials mainly:
    - Development of new aircraft programmes
    - Development of new technology systems on existing programmes
    - Where there is an opportunity, applying on previous aircraft programmes
- By the Technology Providers
    - Extension of existing tools
    - The release of new tools

It is expected that the research/ technology partners will contribute to the exploitation of the project results in other safety critical domains (like automotive, energy, etc.) and in the academic and scientific world.

The technology providers are engaged regularly with industry and so it is expected that the research will be developed to address the real industrial needs. Further research proposals are expected to focus on the collaborative aspect of the application of these techniques within an extended enterprise, something that requires further investigation, especially when considering the interaction with multiple disciplines. Each of the partners has a planned exploitation strategy, with some of the capabilities already being made available for trials outside the MISSA consortium in an attempt to expand the user base.

In addition, the industrial partners are influencing tool vendors external to the project for systems and safety analysis tools by actively engaging with them to inform them of the developments from the MISSA project and are giving an insight of the motivation that led to the development. This activity includes working with the tool vendors to consider their business plan and to assess the size of the market. The technology providers are key enablers for such marketing activities since they have the best view regarding the route to commercialisation. They are in the best orientation to transfer knowledge or collaborate with the external tool vendors to bring a capability to market.

The project has delivered a large number of results with various potentials for being exploited by the different partners:

Generally all the partners have and will carry out some form of the following activities to maximise the exploitation:

- For the technologies that are not yet ready to be industrially exploited, the ideas have and will be used to propose further research projects, collaborative where beneficial.

- Further research to exploit aspects that were not developed within the MISSA project will be proposed.
- The Evaluation Material, Results and Experience will be used as evidence, where permission have been given, that can be shared with the standards bodies.
- Internal Meetings will be carried out with the process owners from each organisation to demonstrate the use and value of the developed capabilities.
- Meetings with the practitioners and experts will be performed to define routes to industrial deployment.
- Meetings/ workshops with the practitioners to offer hands on use of the capabilities will be carried out.
- Communication of the defined procedures for the use of the capabilities and their incorporation into the practiced safety procedures will be performed.
- Preparation and provision of training in the application of new methods and tools will be carried out.

The following types of partners will perform the following additional exploitation activities:

- Industrial Partners
    - For the mature technologies, the industrial partners will focus on communicating the achievements across their organisation and identify entry points for the applicable techniques into their current development processes and for some target product.
    - Disseminate the techniques to encourage similar developments within neighbouring disciplines, such as diagnostics and operational reliability.

- Technology Developers
    - Communicating the research results at various conferences to promote the wider use of the developed capabilities generally across the transport sector and within other applicable industries.
    - As Training Material
    - As prototype tools available on a trial basis

The task of exploitation has already started in a number of areas:

- With respect to the capabilities that are not yet mature enough to use in an industrial context, investigations regarding potential future collaborative research projects has already commenced with various companies and research organisation outside of the MISSA Consortium being involved in workshops and two general themes being considered for future research.
- With respect to the technologies that are closer to industrialisation, the practitioners have been involved from the start; by involving them during the requirements capture activities, and in the evaluation cycles. It is expected that they will participate in promoting the industrial exploitation within safety.
- Internal activities have started to communicate to the wider community of the potential for exploitation in other engineering fields, such as operability and diagnostics at various technical review meetings.

Finally, it was recognised from the previous projects such as ISAAC and from the start within MISSA that the evolution of the safety processes that are followed by the Industrial partners is closely linked to the evolution of the various standards, such as SAE's ARP4761, ARP4754 and DO178, and EUROCAE Workgroup 63's European Equivalents in their current versions. Any changes to these standards will affect the safety process that is followed. Hence the SAE S18

Committee and the EUROCAE/ workgroup 63 (“Complex Aircraft Systems”) that contain members from Industry, Research Organisations, and Certification bodies, has been kept informed regarding some of the more mature developments that have been delivered. The standards are being updated to account for various new techniques including model-based safety.

In Conclusion, exploitation activities have started from the beginning of the MISSA project by both the Industrial partners as well as the Technology Providers. Steps towards exploitation have been in the form of communication and influencing all the stakeholders to ensure that they are more ready to adopt these techniques in the near future. Communication has been within and outside of the organisations of the MISSA consortium of the developments from MISSA. The objective of the communication has been to encourage planning for routes to implementation by influencing established vendors to take an interest in and to work on understanding how these developments fit within the market and more specifically with their commercial offerings. Work has started on seeing where it is necessary to create complementary exploitation opportunities to help fill in the business case to make it commercially feasible, identifying routes to using the developments within existing and future aircraft programs, within safety or even across other disciplines, within the aerospace industry but also to the other transport sectors and possibly further afield. Finally it is recognised that the standards bodies must support new techniques in order to enable the route to adoption. Hence the standards bodies have been kept informed of these techniques. Additionally MISSA project members that contribute to the standards working groups have encouraged the inclusion of provision for the use of model-based techniques within the latest standards.

1.4.5. List of All Beneficiaries:

Bene-ficiary	Company Name	Contact Surname	Given Name	Email
01	Airbus Operations Ltd.	Papadopoulos	Chris	Chris.Papadopoulos@airbus.com
02	Airbus Operations GmbH.	Bretschneider	Matthias	matthias.bretschneider@airbus.com
03	Alenia Aeronautica SPA	Cavallo	Antonella	acavallo@alenia.it
04	Dassault Aviation SA	Gauthier	Jean	Jean.gauthier@dassault-aviation.com
05	APSYS SA	Trouilloud	Jean	jean.trouilloud@apsys.eads.net
06	Atego Systems Ltd.	Larkham	Adrian	adrian.larkham@atego.com
07	Fondazione Bruno Kessler	Bozzano	Marco	bozzano@fbk.eu
08	Office National d'Etudes et de Recherches Aerospatiales-ONERA	Seguin	Christel	Christel.Seguin@onera.fr
09	OFFIS EV.	Josko	Bernhard	bernhard.josko@offis.de
10	Prover Technology AB	Deneux	Johann	johann.deneux@prover.com
11	Queen Mary and Westfield University of London	Izquierdo	Ebroul	ebroul.izquierdo@eecs.qmul.ac.uk
12	Thales Avionics SA	Morel	Marion	marion.morel@fr.thalesgroup.com
13	University of York	Kelly	Tim	tpk@cs.york.ac.uk

The address of the project public website, if applicable as well as relevant contact details.
www.missa-fp7.eu

MISSA Project Coordinator: Airbus Operations Ltd.
Technical Representative for Airbus Operations Ltd.:

Chris Papadopoulos
Lead Systems Safety Researcher
Engineering Design, Systems General, Safety and Reliability Department
Phone: +44-(0)117-936-6170
<Mailto:chris.papadopoulos@airbus.com>

Airbus Operations Ltd.
New Filton House
Filton, Bristol BS99 7AR
United Kingdom