On the Use of Qualitative Methods for Common Cause Analysis: Zonal and Common Mode Analysis

Cristina Johansson[a, b], Johan Tengroth[a], Jan Hjelmstedt[a]
[a] Saab Aeronautics, Linköping, Sweden
[b] Linköping University, Department of Machine Design, Linköping, Sweden

Abstract: While system safety analyses are mostly conducted on the basis of system schematics, this approach do not covers sufficiently the implication of the physical installation of the hardware, especially when the space inside an aircraft is very limited. Additional analyses focused on common causes are necessary and some of the methods used are common practice.
This paper presents an approach that combines the techniques for considering the interactions of logically unrelated systems in the same physical part (zone) of an aircraft with those able to identify failures that occur when multiple instances of a redundant system fail almost simultaneously, generally due to a single cause. Zonal Safety Analysis (ZSA) is employed for identifying failures due to location in the same zone, while Common Mode Analysis (CMA) is used to verify the redundancy/independence of failures assumed in other analyses such as FTA or independently of other analyses. First an overview of the methodology used is presented. Some of the finding from both ZSA and CMA are presented, as well as lessons learned. Reflections on the implementation of these qualitative methods are also provided in the paper with regard to advantages, limitations and difficulties.

Keywords: ZSA, CMA, system safety, common cause, aircraft design

1. INTRODUCTION AND SCOPE

During system design of military aircrafts, there are many aspects that need to be balanced against each other in order to achieve an optimal design. Among other things, the system needs to satisfy both the safety requirements and the reliability specifications, and perform the intended functions while remaining within specific budget limits. The systems to be built inside the aircraft are often highly integrated and the choice of their physical location of the items is often a challenge, given the limited space available inside the aircraft.

One approach is to break down the system safety requirements and reliability goal to item level and examine how the design meets these requirements. In this way safety and reliability requirements on both functional level and at item level are established. Furthermore, during the design phases, several analyses have to be made in order to examine whether the chosen design meets these requirements.

One commonly used method to analyze identified unwanted events is Fault Tree Analysis (FTA). While the fault tree can be developed to a level that encompasses dependencies between systems, it is difficult to determine or consider all possible common causes of failures. For complex, integrated systems, additional analyses focused on common causes are necessary and some of the methods used are common practice.

While system safety analyses are mostly conducted on the basis of system schematics, this approach do not adequately cover the implication of the physical installation of the hardware, especially when the space inside an aircraft is very limited. Zonal Safety Analysis (ZSA) is one of the qualitative methods, developed to allow designers to consider installation aspects of individual items/systems and their influence on other items/systems in close proximity. Common Mode Analysis (CMA) is another method that combines the installation aspects and considerations, together with system schematics.

The scope of this paper is to present an approach capable of investigating the problems described above, used by Saab in the design of military aircraft. This approach is mainly based on references [1] and [2] and engineering judgment from field experience. It combines the techniques for considering

the interactions of logically unrelated systems in the same physical part (zone) of an aircraft (for example equipment bays, nose, wings, etc.) with those to identify almost simultaneous failures caused by the same source. ZSA is used to identify failures due to location in the same zone, while CMA is used to verify the redundancy/independence of failures assumed in other analyses such as FTA, or independently of other analyses.

2. BACKGROUND

During a product development process (PDP), the system safety methods can be used in several product development steps [3]. One method can be used in several PDP phases, the detail level increasing concomitant with the settlement of the design.

Figure 1 System Safety and Reliability Methods during PDP*
(according to reference [3])

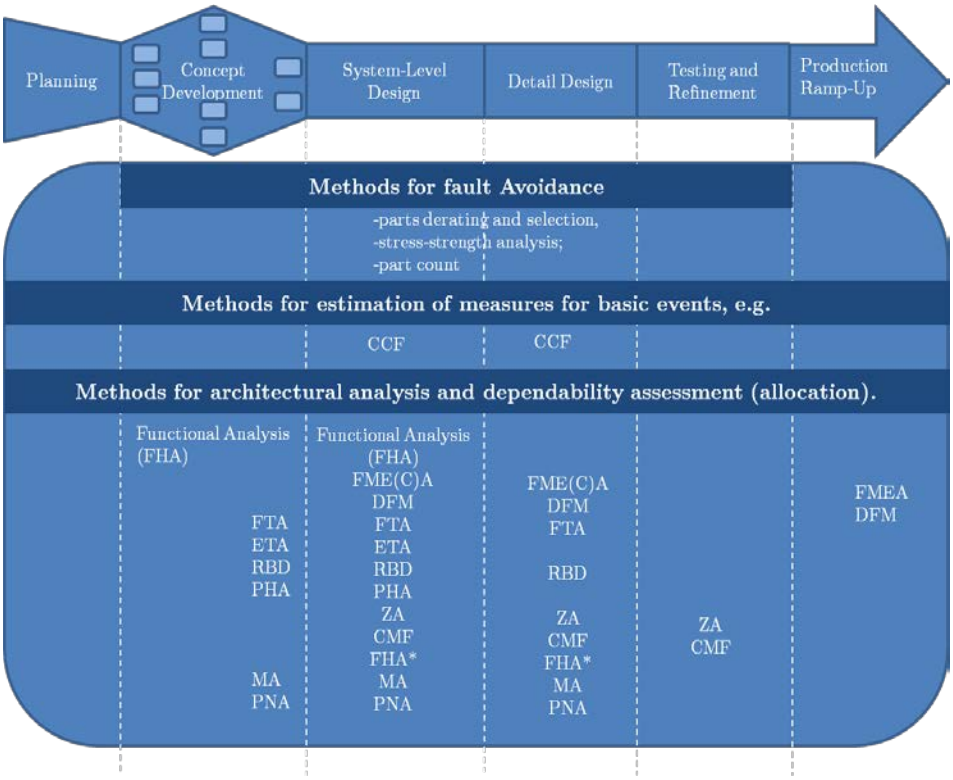


Figure 1 (according to [3]) presents a visualization of how system safety methods presented can be used during a Generic PDP. For example, a CMA or ZSA (ZA* in the figure 1) can be started in the system level design phase or anytime during detailed design and testing and refinement phases. Like most of the safety analysis, this is an iterative process [3].

---

*CCF	Common Cause Failure
FMEA	Failure Mode and Effect Analysis
FME(C)A	Failure Mode, Effect and Criticality Analysis
DFM	Double Failure Matrix
ETA	Event Tree Analysis
FTA	Fault Tree Analysis
ZA	Zonal Analysis (or Zonal Safety Analysis –ZSA used in this paper in accordance with [2])
CMF	Common Mode Fault
PHA	Preliminary Hazard Analysis
FHA	Functional Hazard Assessment
FHA*	Fault Hazard Analysis
MA	Markov Analysis
PNA	Petri Net Analysis
RBD	Reliability Block Diagram

CMA [2] is a method for identifying sequences of events leading to an accident (e.g. aircraft accident) and should be carried out to establish the requirements for the elimination of common cause failure between components of the architecture (e.g., total loss of deceleration capability, total loss of the communications system, or simultaneous failure of redundant hydraulic/electrical power supply). According to [1] and [2], the analysis can be carried out using several qualitative and/or quantitative methods such as ZSA and Common Mode Fault (CMF), and have the purpose to identify and analyse dependent failures.

The purpose of ZSA, as presented in this paper and according to [2], is to ensure that the equipment installation meets the safety requirement with respect to basic installation, interference between systems and maintenance errors. When a finding that may affect safety is identified, it will either result in a redesign or will be shown to be acceptable in the appropriate safety assessment.

CMA at subsystem level aims to prove/argue that the independence assumed in the fault tree analysis is valid. CMA is a time-consuming method and needs adjustment to fit the project and specific subsystem. The findings of CMA are either that the independence claim has been verified, or some design weaknesses found. These weaknesses will be addressed by for example redesigning, re-evaluating the method used or, like the ZSA's findings, will be shown to be acceptable in the appropriate safety assessment.

The CMA at aircraft level aims to confirm the independence principles applied to aircraft design level and justification for the acceptance or traceability to the design changes is provided for every finding (compromised redundancy or independence). This CMA analyzes combinational failure conditions that are not considered in the subsystem safety analysis.

3. ANALYSIS

3.1. Zonal Safety Analysis

The objective of ZSA is to ensure that the system design and installation meets the safety objectives regarding basic standards of design and installation, effect of failures (such as physical damage, fire, leakage, etc.) on the aircraft and the implication of maintenance errors [2].

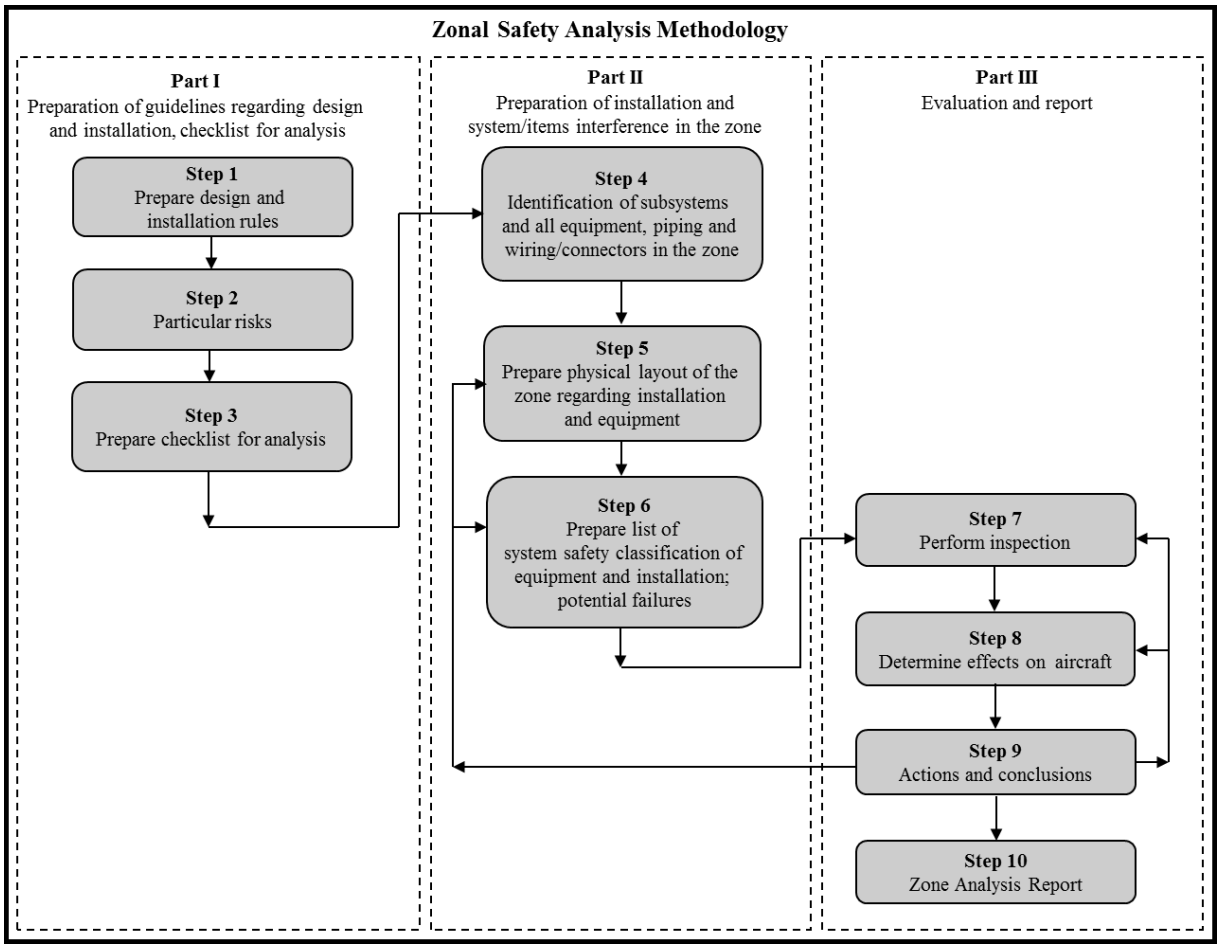
Historically, at Saab, ZSA has been performed on the physical aircraft, starting with the prototype or demonstrator aircraft. The difficulty of performing the analysis when the aircraft has already been built was the inspection itself, but also the correction of possible findings. The inspection is difficult to perform (to actually see) when the space inside an aircraft is very limited and everything is already in place. The possible findings are more difficult and expensive to correct when the design is finished, which among other things, causes more delay to the project. Several of these findings might have been able to be corrected easily if they had been detected in early design phases, before the aircraft had been built.

In order to overcome these disadvantages, in the new generation of aircraft projects using model based design, ZSA is begun in early design phases. Inspection is carried out on the physical layout drawings from CATIA. On the virtual physical layout all the details can be seen, different angles can be used, without risk of errors. The distances between items can be measured and subsystems or items can be highlighted.

ZSA uses the partitioning of the aircraft into zones. Zones can be defined for maintenance purposes and follows the physical aircraft fuselage compartments. According to reference [2] and as shown in Figure 2, the ZSA steps are grouped into three equally important parts:

- part I: Preparation of guidelines regarding design and installation, checklist for analysis
- part II: Preparation of the installation and system/item interference in the zone
- part III: Evaluation and report

Figure 2 ZSA Methodology



The first part consists of three steps. All three steps in part I are analysis preparation steps. The second part is zone specific and consists of preparation steps. The third part is the actual evaluation including inspection/review as well as documentation of analysis.

In step 1 (part I) the design and installation rules were established. Independent of the analyzed zone, the overall aircraft level requirements were taken into account, as well as some considerations from Preliminary System Safety Assessment. The zones were defined and system specific design rules and requirements are collected. Considerations based on field experience accumulated from previous programs were also valuable input. Saab has its own incident data base, accumulated from the first built aircraft at Saab and ongoing. This database provides the designers with valuable cumulated field experience. Examples of these general rules are considerations related to critical parts, installation separation, environmental conditions specific to every zone, or maintenance errors.

Step 2 considers particular risks such as fire hazard, bird strike, etc. Particular risks analysis is one of the three components (together with ZSA and CMA) of Common Cause Analysis performed by Saab. The particular risks as mentioned in the checklist from step 3 were identified from the field experience, the incident data base using mirrored user data from previous similar product and the system safety analysis (FMEA, FHA, PHA). The historical events in respective zone were also reviewed and used.

For example, fire risk is one of the particular risks analyzed. The analyses are based on general and specific requirements derived from MIL-HDBK 516B, legacy requirements from similar previous product and the fire triangle principle (presence of ignition source, fuel and oxidant). Based on this information, the risk of fire is assessed for each zone. The statement when a corrective action has been suggested could be "*the risk of fire appearance is not able to be completely assessed (pending action). The fire hazard requirements applicable for the zone are fulfilled given the action outcomes from the*

table…". When the risk is assessed low, the statement could be "*based on the fire triangle principle, the fire risk of fire appearance is assessed acceptably low. Justification: lack of flammable fluids*"

The analysis checklist is prepared in step 3. The checklist included particular risks as well as flight safety critical installation and separation requirements, interference between systems and maintenance errors.

Step 4 is zone specific and consisted of identification and presentation of the zones and subsystems included in each zone. The content and installed equipment, wiring and piping, normal operation conditions, possible contaminators, kinematics and closed volumes, connectors and communication with adjacent zones were established.

The physical layout (external view and internal layout) of the zones (step 5), with respect to installation and equipment have been prepared using actual drawings from CATIA. At one occasion, the whole aircraft have been considered as a zone in order to highlight the wiring. For example, wiring included in functions with separation requirement, could be in two different zones, separated only by a wall (not enough distance separation). This aspect could be missed with other approaches.

In step 6, output from system safety analysis (FMEA, FHA, PHA) and the incident data base from previous similar product have been considered. The historical events in respective zone have also been reviewed and used as an input.

The inspections carried out in step 7 were made by a dedicated forum with members of various key competences (such as system safety, installation, fuselage, system knowledge, etc.). One member representing department of survivability, as well as a flight safety investigator was always present during these reviews.

The same forum determined the effects on the aircraft in step 8, and in step 9 drew conclusions from the inspections that were made and recommend actions. Such conclusions might be that the installation is robust and accepted or that, as result of the findings from the review, corrective actions, further investigations or design changes/modifications were required. In this case steps 5 to 8 can be repeated. The last step is to document the performed analysis.

3.2. Common Mode Analysis

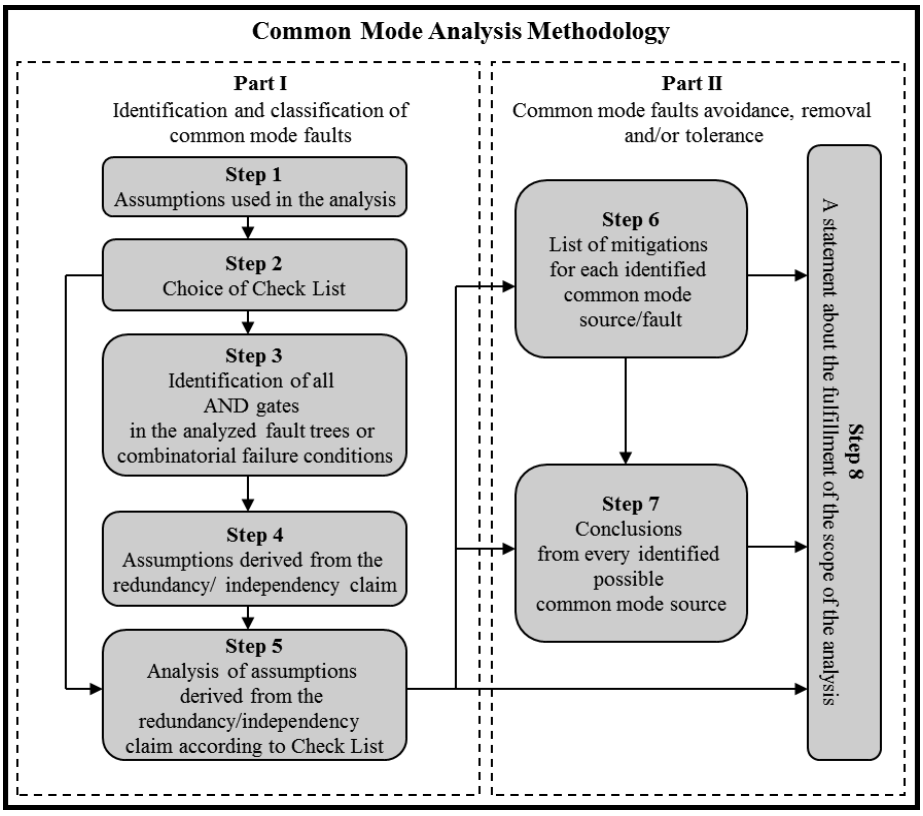
While using common mode analysis is considered common practice in the civil aircraft design when conducting safety assessment, the military aircraft design not always follows these rules. However, the new generation of military aircrafts is designed to meet most of the requirements of civil aircrafts with regard to safety assessment process. Therefore, two different CMAs have been performed: CMA for each subsystem and one CMA at the aircraft level.

The scope of CMA at subsystem design level is to prove/argument that the independency assumed in the fault tree analysis is valid. The scope of CMA at aircraft design level is to confirm the independence principles applied to aircraft design level.

Both types of CMAs follow the same methodology. According to reference [2] and as presented in Figure 3, the CMA steps used are grouped into two equally important parts:

- Part I: identification and classification of common mode faults
- Part II: common mode faults avoidance, removal and/or tolerance.

Figure 3 CMA methodology



The first part consists of five steps. The scope and assumptions of the analysis were established in step1. These assumptions may concern general considerations (e.g. no warnings shall be issued on known bad data, loss of power supply is always considered a detected fault, etc.), overall design considerations affecting the analysis (such as flight envelope), interface with other subsystems in the case of CMA at subsystem design level, etc.

Step 2 was the choice of check list (according to [2]) to perform the analysis. Only the parts considered relevant for each type of CMA were included in the list. The *check list* used in the CMA was:

- Design Architecture
  - Common External Sources
  - Common Technology, Materials, Equipment and/or Component Type
  - Common software (application, platform)
  - Common electrical interfaces (connectors)
  - Operating characteristics (normally running, stand-by, etc)†
  - Equipment Protections†
  - Internal and Initial Conditions (temperature and pressure ranges) †
- Common Location (physical location in the a/c)
- Wires routing (physical location: inside the equipment and a/c)
- Common Manufacturer
- Environment (the factors with influence on the equipment)
  - Non-compliance with environmental requirements
  - Non-compliance with electrical and radiation requirements

In step 3 the failure conditions or fault tree with all AND gates to be analysed was identified. The result of this step in the case of CMA at subsystem level is structured in a table containing the relevant

† only in CMA at subsystem level

information such as *gate ID and description, notes, if and why is analysed* and *requirement derived from the AND-gate*. An example taken from the analysis of the Electrical Power Supply system is as shown in table 1.

Table 1 Example of identified AND gate to be analysed (From CMA of Electrical Power System)

Gate ID	Gate Description	Notes	Analysed / Why?	Assumptions derived from the AND-gate
FHA 39.04.02	Emergency battery not available (failure to start and manual activation fails)	This is included in a functional chain of another subsystem	Yes/ Redundancy requirement of the battery activation	No single failure should cause loss of both manual and automatic activation of emergency battery
G3959A22	Loss of power supply to Battery Bus X 28V	Loss of Battery Bus X 28VDC loss of auxiliary power supply	Yes/ Separation requirement	No single failure should cause loss of power via relay XX and Main Bus Y 28VDC

In step 4 the assumptions derived from the AND gates or redundancy/independency claim from the combinatorial failure conditions, were established. These assumptions have to be proven by using the check list. Examples of such assumptions are:

- *No single failure should cause loss of both manually and automatically activation of emergency battery*[‡]
- *No single failure should cause loss of power via relay XX and Main Bus Y 28VDC*[‡]
- *No single failure should cause loss of landing steering and landing braking*[§]
- *No single failure should cause loss of transponder and radio communication*[§]

In the step 5 the analysis was performed on each assumption according to the check list. An example of parts of the analysis of an AND gate is shown in table 2.

Table 2 Example of parts of analysis of an AND gate from electrical power system

Assumption AA: No single failure shall cause loss of both manual and automatic activation of emergency battery	
Design architecture	Loss of manual activation of TB occurs due to faulty battery, relay XX, circuit breaker XY and XZ, switch ZZ, resistor YY and the main bus bars X1 and X2 28VDC. Loss of automatic activation of emergency battery also occurs due to faulty battery. Analyzing the equipment included in the two chains of the analyzed gate no common items have been found. *Potential Common External Sources:* control unit, air supply (bleed air and pressure air) No common mode fault for control unit or air supply causing loss of both manual and automatic activation of emergency battery has been found. *Technology and Materials* Two circuit breakers use the same technology and materials. Faults related to the same materials and technology, are of common mode. *Common software (application, platform):* not found
Common manufacturer	Two circuit breakers have the same manufacturer. Failures due to manufacturing errors are of common mode.

[‡] CMA at subsystem level
[§] CMA at aircraft level

After analysis of all assumptions to be proved, a list of mitigation of all common mode failures had to be provided in step 6.

A conclusion referring to all analysis, findings and mitigations, regarding each assumption was drawn in step 7. An example of such conclusion:

- *The common mode sources identified regards technology type and materials, and manufacturer (example from table 2). Two circuit breakers have the same technology and materials and are purchased from the same manufacturer. However, the failures due to manufacturing defects or technology are specified in the FMEA from the vendor and the failure rates are according to design requirements. Assumption AA (table 2) is therefore considered verified and the analysed AND gate valid.*

The last step in a CMA was to issue a statement about the fulfilment of the scope of the analysis. Examples of such statements are:

- *Some possible common mode faults between components of the electrical power system have been identified, but with implemented mitigations the design is considered robust enough against common mode failures.*
- *The fuel subsystem architecture is considered to verify all the assumptions derived from the AND gates analyzed in this CMA.*
- *The CMA analysis performed in this document confirms the independence principles applied to aircraft design level and, for every finding (compromised redundancy or independence), justification for the acceptance or traceability to the design changes is provided.*

4. RESULTS

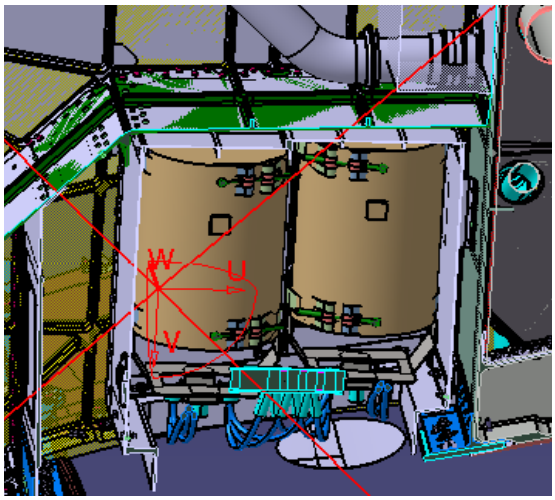
The results will be presented in the form of findings from ZSA and CMA and lessons learned. The findings are these that will be difficult to detect otherwise or very expensive to rectify later.

4.1 ZSA Findings

Some examples of findings from ZSA with respective correction have been:

- The location of batteries was identified to be too near fuel pipes and fuel tank. In case of thermal runaway of the batteries, there was a risk of fire and explosion considered not acceptable. The separation principles and rules were not possible to be followed with the location of batteries as presented in figure 4. The batteries have to be moved and concept totally changed.

Figure 4 Example of CATIA layout



- Liquid cooling circuit pipes were routed through the fuel tanks. The fuel is not compatible with the coolant and, in case of leakage there was risk of engine flame out. The pipes were rerouted outside the fuel tanks.
- Venting tube from the fuel tanks were routed parallel with the bleed air tube. The fuel vapors in the venting tube in contact with high temperature from the bleed air tube could create a risk for fire and explosion. The venting tubes were rerouted.
- Hydraulic system pipes and tubes were routed through the same clamping point. This compromised the separation requirement of redundant subsystem. The pipes and tubes were rerouted through different clamping points to achieve a good physical separation.
- Few main wiring ducts to perform a good physical separation of the signals. This compromised the redundancy requirement of several functions in the aircraft. A number of additional wiring ducts were fitted.
- Rubber suspensions did not have mechanical stops. In case of rubber release, the apparatus could fall off inside the zone, causing physical damage to installations and equipment located in the same zone. Several redundant functions might be lost. Mechanical stops were installed.
- The presence of foreign objects (for example objects lost during maintenance, pieces from a bird strike, dust, etc.) could cause short circuits, clogged pipes or tubes, physical damage inside the zones, with various consequences. The design has been revised so that the existence of foreign objects should not have any impact on safety or the functionality of the aircraft. The spots difficult to inspect for foreign objects have been deleted. Examples of these revisions are: stronger walls where risk of bird strike was high, moving different pieces of equipment, revised maintenance routines, and physical layout changes, etc.

4.2 CMA Findings

Some of the most important findings of the CMA with respective corrections have been:

- *Common manufacturer* as well as *technology and materials* were identified as common mode sources in several subsystems CMAs (for example the same type of relay, switch, valve, jet pump, etc.). These findings have been handled from case to case. If the failures are already accounted in the fault tree, with probabilities to satisfy the system safety requirements, they were considered acceptable. In other cases, redesign or new purchasing procedures have been suggested.
- *Location* was also identified as a common mode source in several subsystems CMA, for several items (for example wires or pipes in the same zone, two items that belonged to redundant functions in the same zone). These findings were handled by following the physical separation distance prescribed in design rules or by rerouting the pipes or wiring where possible.

4.3 Lessons Learned

Sections 4.1 and 4.2 give examples of ZSA and CMA findings. However, many lessons were also learned during the course of the analysis. Some of the advantages and draw backs of each method are presented in this section.

Some of the advantages of the ZSA performed are:

- Regarding the results of the analysis:

  The main advantage was the possibility to highlight the design errors and weaknesses, in an early design phase and rectify them. Potential risks have been avoided, increasing the survivability and robustness of design.

- Regarding the methodology of the analysis:

The systematical way of working gave opportunities to reflect on earlier weaknesses or possibilities to improve the design. Using the forum's broad range of competence, new ideas caused several aspects to be detected.

- Regarding the preparation phases:

  The virtual physical layout (from CATIA) gave visual access to all equipment and installation in each zone. It was easier for all involved to understand and clarify what the zone contained and how the system works. It also allowed us to view the aircraft as a zone. The approach was particularly useful when investigating the wiring signals.

  The inspection checklist and the list of installation and equipment failures provided an opportunity to systematically use not only the whole incident database from earlier programs, but historical events in the respective zones.

The drawbacks of the ZSA performed are:

- The ZSA was time consuming
- The analysis begun in an early design phase. The environmental conditions of each zone and the criticality of installation and equipment, used the earlier program as a starting point, and needed to be reviewed and updated several times during settlement of design. Changes of the design due to other causes than ZSA findings, caused also several reviews and updates of ZSA.

Some of the advantages of the CMA performed are:

- Regarding the results of the analysis:

  As in ZSA, the main advantage of CMA was the possibility to highlight design errors and weaknesses, in an early design phase. Potential risks have been avoided at minimal cost increasing the robustness of the design.

- Regarding the methodology of the analysis:

  The analysis systematically tries to identify failures that often are not identified by other analysis. This increases knowledge and understanding of both the subsystems and the aircraft and even helped to identify errors or weaknesses in other safety analysis.

- Regarding the preparation phases:

  This analysis uses the system schematics, but also the virtual physical layout (from CATIA) used in the zone analysis. This increases the knowledge and understanding of both the subsystems and the aircraft.

The drawbacks of performed CMA are:

- The CMA was time consuming.
- The analysis findings are sometimes in direct conflict with the decisions from economy department and difficult to correct. These kind of finding are often subject of further investigations and CE approval.
- The analysis begun in an early design phase when the design was not mature enough and information was not available or was changed. The CMA needed to be reviewed and updated several times during settlement of design.

5. CONCLUSION

The main advantage of ZSA and CMA is the possibility to highlight design errors and weaknesses, in an early design phase.

Potential risks such as fire and explosion, engine flame out, physical damage causing loss of several functions, etc. have been avoided, increasing the robustness of the design and survivability.

Acknowledgements

This work was financed by Saab Aeronautics.

I want to thank all my colleagues from Saab Aeronautics, Division of System Safety and Reliability, especially Johan Karström and Lars Holmlund, for their involvement and work with ZSA, as well as for the field experience and feedback provided during the analysis.

References

[1] IEC 60300-3-1:2003 "*Dependability management, Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*", International Standard, 2003

[2] SAE ARP4761, "*Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment"*, International Standard, 1996

[3] C. Johansson, "*On system safety and reliability methods in early design phases. Cost focused optimization, applied on aircraft systems"*, Linköping Studies in Science and Technology, Thesis No. 1600, 2013, Linköping