Development of integrated functional monitoring and warnings system for Saab 39 Gripen.

Carina Birgersdotter[1] and Torbjörn Fransson[2]

[1,2]*Saab Aeronautics, Linköping, S-581 88, Sweden*
carina.birgersdotter@saabgroup.com
torbjorn.fransson@saabgroup.com

ABSTRACT

As the requirements of a modern air vehicle changes during development and use, requirements and design of test and recording functions have to be continuously updated. To achieve control over functional monitoring, pilot warnings and health management in a tightly integrated avionics system with several configuration variants and frequent updates, powerful tools are needed, especially when requirements on cost reduction and a small staff are considered. Traditionally the work has been divided among several departments, with own processes and tools, leading to redundant work and inconsistency, despite tremendous inspection efforts.

This paper describes how the workflow to define pilot warnings are integrated in order to reduce development time and reuse data. There are over 500 failure modes defined for the Gripen Aircraft.
The impact of a failure is depending on equipment configuration and thus will the required pilot actions differ between the variants. In complex failure situations it is also important to find the primary fault and filter faults that can be considered as consequences of the primary fault. The presentation will show how primary failures are distinguished from secondaries or consequences.

Experience has shown that the recommended pilot actions often need to be revised after that operational experience has been achieved by the users. As changes in a delivered product are costly, the method of separately loadable databases for flight manuals and warnings information will significantly reduce the cost of an update and also enable an incremental development. This paper will also describe how field loadable databases can be used in aircraft.

Figure 1. Gripen Dual Seat

The paper will have the following disposition

Introduction: A brief overview over the Gripen project and development of Monitoring and Warning functions.

Current Design: A description of the design concept for the warnings system in Gripen. This chapter will explain some acronyms and describe how failures are presented as warnings in different modes of operation.

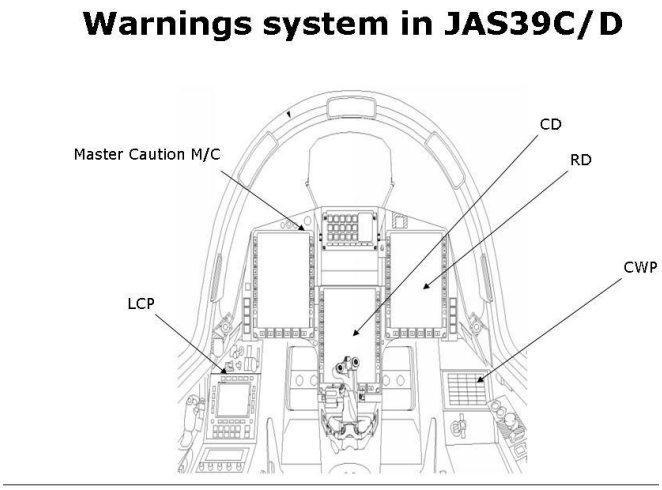

Figure 2. Cabin layout

Problems: This section will list some important design drivers which in this case are derived from customer requirements and needs for cost reduction.
Approach: This section describes how the problems are analyzed and taken care of.
Conclusions: Experience from both Saab and Swedish Air force.

1. INTRODUCTION

When the Gripen, see
Figure 1, development started in 1982, Test and Monitoring requirements were not the first thing in our focus. The product specification was very detailed on weapon functionality, while embedded test functions was covered in a few sentences. Test and monitoring was by then not neglected, they were just treated like something obvious. The maintenance concept for the predecessor, JA37 Viggen, was a success and thus requirements like "Performance better or equal of that for JA37" could be found. Despite the lack of detailed requirements, experienced personnel were allowed to develop the monitoring functions from the beginning.

Embedded test, monitoring and recording functions were developed in parallel with tactical functions in the aircraft. With three processors, one MB of code memory and three Mil-STD 1553B data buses, the systems computer was well equipped for the task. As always, the requirements for new functions grew faster than hardware upgrades permitted. Limited computer capacity pushed the development towards highly optimized designs and approaches.

Many tools were developed for various purposes, tools that had great importance for further development but little integration with other tools. To avoid further diversification, common processes were defined for the company.

Today (2016), there are three Gripen versions in service, Single seat 39C, Dual seat 39B and 39D. Customer specific variants and upgrades exist for both serial aircraft and test aircraft. New variants are under development and new functions are delivered for flight test each month. Processes for systems and software development are now working as intended and roles and responsibilities have been clarified. For monitoring, test and recording, all responsibilities have been allocated to one department with the result that methods and tools have been standardized and are better integrated. Meanwhile, the defense budgets have decreased drastically the last decade and there is no longer room for any major redesign unless cost reduction can be proved in a short term. The issue will then be to improve the performance on legacy systems without expensive updates.

2. TERMS AND DEFINITIONS

2.1. Central Functional Monitoring

Central Functional Monitoring provides the aircraft system with the following functionality:

- Functional monitoring of the aircraft system including logic for primary and secondary failure warnings.

- Failure warning generation

- Display of failure warnings on panels and text displays. See Figure 2

- Display of flight manuals.

2.2. Local Functional Monitoring

Local Functional Monitoring at subsystem level handles fault detection. In non-degraded modes, all detected failures are passed to central functional monitoring where further processing is done.

3. PROBLEMS

3.1. Complexity

A main difference compared to older systems was that in the old federated architectures, all systems had their own failure modes and typically one or a couple of warning lamps connected to that system. A problem with that was that a failure warning in a supply system could cause so many side effects that the real failure warning would be obscured by a myriad of flashing warning lights, see Figure 3. The problem to solve was how in a complex failure warning pattern pick out the primary fault and display that in a way that would give the best help to the pilot.

Having over 500 distinguishable failure modes, no pilot would keep all required actions in mind. A flight manual

mode was developed early in the project and is now for 39C complete in the meaning that there is one specific flight manual for each failure warning.

Figure 3. Conventional Warning System

In an integrated system, there are easier ways to control the warnings displays.

The first effort to be done in 39A was to distinguish between primary faults and secondary faults. A suppression function on the caution and warning panel blocked the lamps for systems secondarily affected and the text info on the head down displays differed between primaries and secondaries for all flight critical failures. In 39C this function was extended to cover also failure warnings in the tactical system that would impact on mission capability.

3.2. Development cycle

Another problem was the time required to develop a new warning, as it required a great effort of integration and verification. To keep information in aircraft consistent with flight manuals and maintenance documentation with paper documentation and manual inspections was extremely time consuming.

It was early decided that we had to use tools to support the development. With all information stored in a database, the same source could be used to generate documentation and data for the avionics computers. In a later step, functionality to support integration between subsystems was added.

3.3. Time to customer

With embedded functions, new releases to customers are very expensive as the entire software has to be certified. By making the warnings system parametric driven, it is now possible to separate the warnings and flight manual data from the resident software and instead having it field loadable in a separate file system.

4. APPROACH

How do you get a good partitioning of a complex functionality involving several organizations?

A systematic approach to get maintainable software architecture led to the so called Warning Triangle.

In the Warning Triangle there are clearly distinguished layers that interact with clearly defined interfaces.

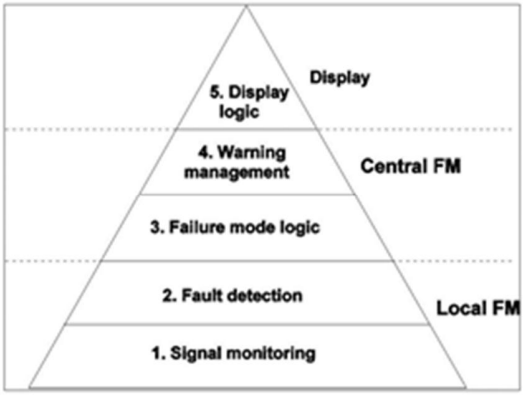

Figure 4. “The Warning Triangle”, principle layout for functional monitoring

Figure 4 illustrates the different layers in functional monitoring:

• Functional level 1, in the bottom is signal monitoring. That is the most basic function that with a very minimum of involved functionality indicates a state that can serve as a warning. Typical examples are lamp indications that are connected to a basic sensor, like fire warning and heat sensor or low fuel warnings. A very important aspect is to monitor unexpected states that are not considered faults, like “gear not out at landing approach”. The signal monitoring is also used to cover the most critical failure warnings to make the failure mode presentation available even in case of a computer fault.

• Functional level 2, Fault detection is distributed and shall be done as close to the source as possible, uses combinations of the monitored signals to detect abnormal conditions or faults.

• Functional level 3, Failure mode logic is a central function that determines what is primary and secondary. It evaluates abnormal conditions or faults, detected by local functions, to see if it shall be considered a system level failure mode. Transients are not considered as failures.

• Functional level 4, Warnings management, is the core of central functional monitoring functions. It determines when failure warnings shall be given for reported failures and when warnings shall be deactivated. It also supplies data to display, I e Flight manuals.

• Functional level 5, Display logic is a special entity as there are several ways to display the information and the mode selection on the text displays are unsynchronized with how the warnings appears and disappears.

The responsibility of Central FM covers layer 3, 4 and 5. Local FM, on equipment or subsystem level covers the bottom two layers.

5. CURRENT DESIGN

5.1. Overview

The Gripen warnings system, according to Figure 5 consist of

- Two master caution lamps with acknowledgment button.
- Audio warning
- Caution and Warning Panel, CWP
- Displays
- Local monitoring functions
- Central functional monitoring
- FM-database (Field loadable)

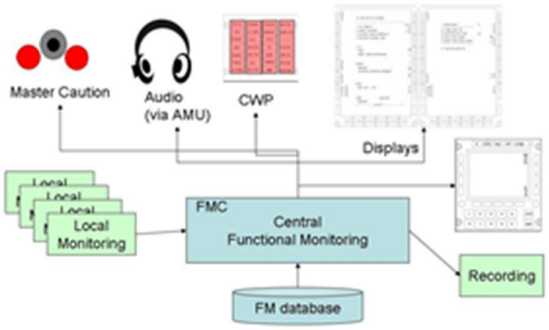

Figure 5. Overview

These components ensure that failure warnings are presented, first with alert (audio and light) to capture attention. A system oriented CWP lamp points out the problem area and the text displays gives further information and decision support.

Redundant displays and distributed logic ensures that no single fault in the central function can prevent failure warnings to be displayed. For more detailed description about the design drivers, see [2].

5.2. Workflow

With shared responsibility between local and central functionality, the subsystem experts will focus on the fault detection and system behavior. The detection capability is implemented as Continuous Built in Test, CBIT, functions in the subsystems. Normally the detection function is limited to one subsystem or line replaceable unit, LRU, for each warning, but when a subsystem has several LRUs interacting, there might also be local failure mode logic, between level 2 and level 3 according to Figure 4.

The technical manager for the central functions will together with subsystem managers and the test pilot assign a name for the corresponding failure warning. This can sometimes be a bit tricky as the name has to be limited in size and clearly interpretable at a short glance. The failure warning shall primarily identify the affected functionality.

The flight manuals that are shown on the displays are authored by a team including technical manager for central functions, subsystem managers and pilots.

The information regarding failure warnings are continuously entered in a database. When the work is complete a specification is automatically generated from the FM-tool, see Figure 6. One specification is issued for each affected system. These specifications will then be inspected and finally approved. When all specifications are approved, software for the aircraft is generated from the same source as the specifications.

The generated software is field loadable to the aircraft to enable the flight manuals to be updated at a very short notice.

As the software is generated from the same source as the specifications, no further inspections of the software is necessary but the consistency between code and specification has to be verified. This is done by another tool, which is developed independent of the FM-tool, and is described in section 5.4.

5.3. FM tool

As all development is tool supported, new and altered failure warnings are easily administered using the by Saab Aeronautics developed FM-tool.

In the FM-tool, several parallel configurations and systems can be handled.

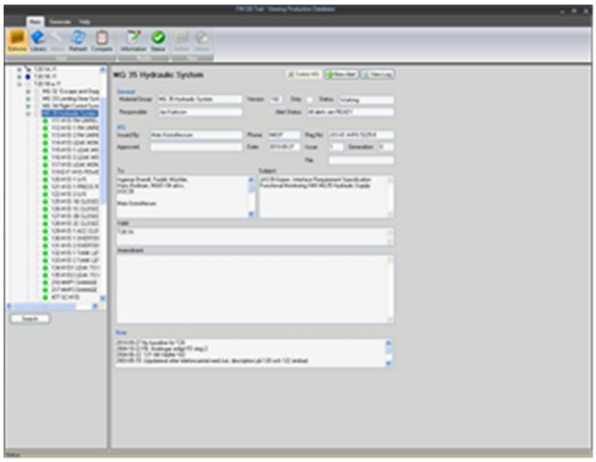

Figure 6. FM tool system view

Warnings are defined per system and the system structure is similar to the ATA chapters, see Figure 7.

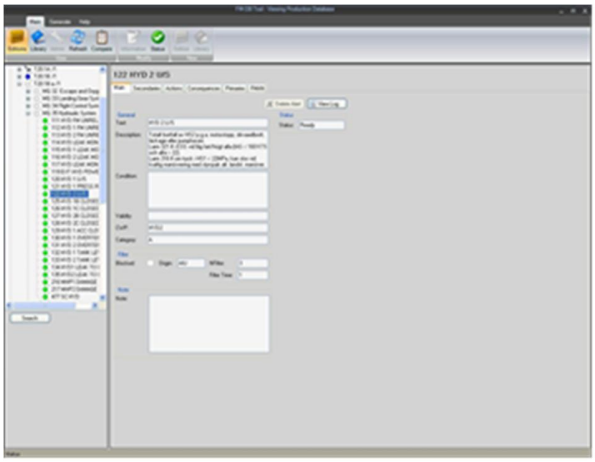

Figure 7. Main view

For each warning, primaries and/or secondaries are defined. Based on all warnings, complete fault trees are generated and displayed in the tool, see Figure 8.

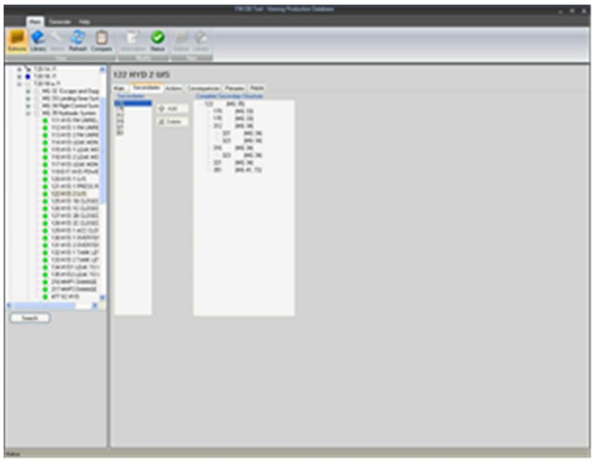

Figure 8. Fault tree view

Flight manuals consist of a list of recommended pilot actions and a list of consequences. Each failure has its set of actions and consequences but the final display is a synthesis of actions and consequences for the actual fault in combination with secondary failure warnings see Figure 9 and Figure 10.

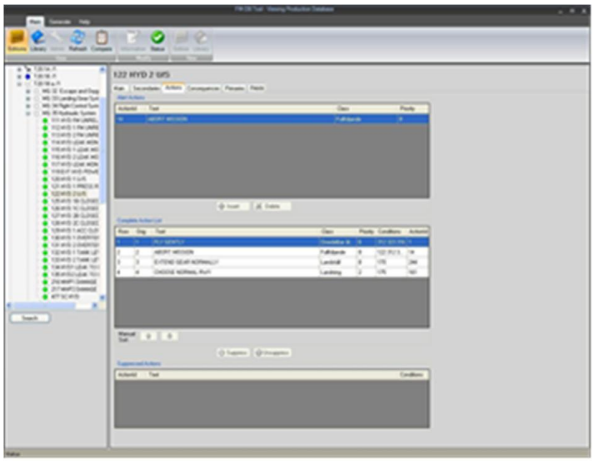

Figure 9. Action view

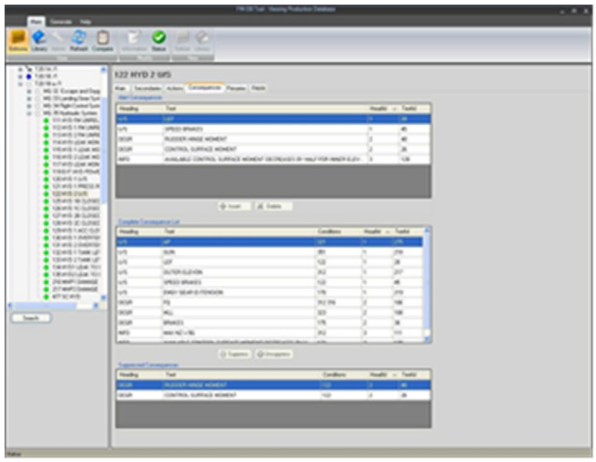

Figure 10. Consequences view

In some cases the sum of all actions and consequences gives more information than can be displayed on a screen page or it is just too much for the pilot to cope with. There is a priority function in the tool that enables the user to manually sort out the most important information. The result can then be viewed exactly as it is shown in the cockpit, see Figure 11.

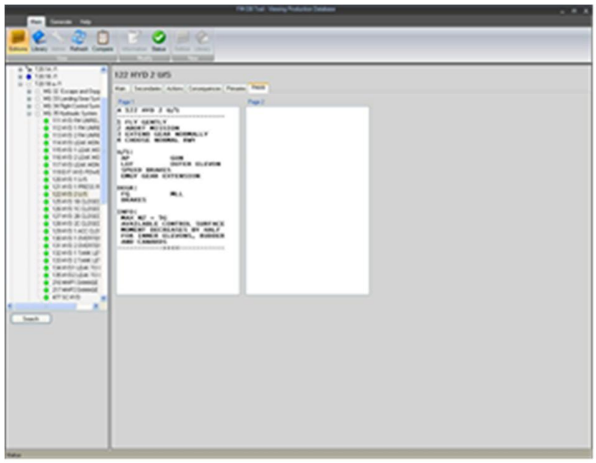

Figure 11. Flight Manual view

5.4. FM Verifier

As manual code inspection and testing can be very time consuming, the FM-Verifier was developed to ensure consistency between software and documents.

The FM-Verifier converts specifications to code and compares this code with the field loadable data generated from the FM-tool. To pass the verifier, the data from the two data sets has to be identical.

As one specification is issued for each subsystem, there will be about 30 documents that have to be checked against the code. As only documents affected by the last changes are reissued, the complete set of document dates can vary much in between. It is therefore important to verify that the "old" documents still are valid.

5.5. FM Viewer

The Flight manual view is useful but it does not give the proper dynamic behavior.

FM-Viewer is developed by Saab Aeronautics to display the behavior of the failure warnings from the pilot point of view.

It is used during development and modifications to view the warning pattern and failure warning presentation for critical and complex failure modes. Pilots and system engineers work together to develop the proper set of display and emergency flight manuals.

The tool will at startup ask for a software configuration. Then a field loadable file, exactly the file that is used in aircraft, is loaded. Figure 12 shows the three displays as they can be seen in the cockpit. In the FM-viewer several warnings can be set in the same time and the displays will show how the failure pattern change as warnings are added or removed.

Figure 12. FM Viewer

By default only primaries are displayed, as the central display in Figure 12 shows. The complete list of failure warnings, including all suppressed secondaries, see the left display above, can be manually selected by the pilot.

A recent update makes it also possible to use the viewer as a tool to identify failure modes in emergency mode, when textual presentation is lost.

6. CONCLUSION

The tool supported process has been a great success. First of all, manual errors in the process that earlier resulted in discrepancies between documentation and displayed information has been eliminated, which has significantly increased the pilot confidence in the warnings system.

The visualization of fault trees has resulted in a better understanding of complex failure modes.

The FM-Viewer has been used as a simple desktop trainer for the pilots. It has also been used by technical staff when analyzing certain fault event.

Another important aspect is that the toolset significantly reduced development time and cost.

Our experience tells us that we are on the right track and we are following this method by introducing similar tools also for recording and test functions.

REFERENCES

Fransson T., (2006). Integrating development- and support tools for PHM in Saab 39 Gripen. *IEEE Aerospace Conference 2006.*

Andersson S., Peterson M., (2003). Att skapa uppmärksamhet vid presentation av central funktionsövervakning, Thesis Malardalens Hogskola FLYG/2003/137/10/FS-Av/O