SYSTEM SAFETY OF THE ORDINARY AND EMERGENCY FLIGHT DATA DISPLAY ON THE GRIPEN COLOR DISPLAYS

Jan Palmqvist (Jan.Palmqvist@saab.se), Rolf Santesson, (Rolf.Santesson@saab.se)
Saab AB

Keywords: *Flight Data, Integrity Monitoring, Stand-by Instruments, Gripen*

Abstract

The Saab-BAe multi-role fighter aircraft Gripen has a continuos development program to incorporate new technology. Current important cockpit changes are the replacement of the three 5´´x6´´ monochrome CRT displays by three 6´´x8´´ Color Multi-Function Displays (CMFD), and the removal of the traditional and dedicated electromechanical stand-by flight data instruments.

One important aim of introducing the new 6"x8" CMFDs in the Gripen aircraft is to use them all for full screen presentation of tactical information. The size of the displays disables the use of self-contained stand-by instruments, why these instruments will be deleted. As a consequence a new concept for displaying flight data has been developed. The concept comprises of automated flight data monitoring and functions for immediate head down presentation of flight data when necessary.

To achieve this, system safety considerations must be a vital part of all steps in the design and partly new principles has been used to ensure system safety and the performance of the supervision functionality for cross comparing the ordinary to stand-by flight data.

Figure 1.1: The fourth generation multi-role combat aircraft Gripen.

1 Introduction

The Saab-BAe Gripen is a fourth generation multi-role combat aircraft, as shown in figure 1.1. The Gripen is already in operational service with the Swedish Airforce, as the first fourth generation fighter aircraft in the world. As a fourth generation aircraft Gripen has an integrated avionics system with a very high degree of software control, communications, flexibility and growth potential. Even so, further development is needed to reduce pilot workload and enhance mission efficiency.

Current important cockpit changes are the replacement of the three 5´´ x 6´´ head-down monochrome CRT displays by three 6.2´´ x

8.3´´ Color Multi-Function Displays (CMFD), and the removal of the traditional standby flight instruments.

The introduction of the larger CMFD in the Gripen cockpit disables the use of stand-by instruments. A new functionality has been developed where the CMFD consist of both the ordinary and an emergency display system, The later utilizing a back-up display processor in each CMFD. The emergency flight data display system is a separate system that will be used when the ordinary system is malfunctioning.

In all known aircraft designs yet the ordinary and stand-by presentation have been displayed concurrently and the safety objectives for ensuring that no misleading information is being used by the pilot has been managed by the pilot cross comparison of the ordinary and stand-by presentation prior to and during flying under Instrument Flight Rules (IFR) conditions.

2. Gripen Cockpit

The present Gripen, lot 1 and 2, has a cockpit with a Head-Up Display (HUD), four electromechanical stand-by flight data instruments and three monochrome Cathode Ray Tube (CRT) multi-function displays, as shown in figure 2.1.

The head-down displays are named according to their original use: Flight Data Display (FDD), Horizontal Situation Display (HSD) and Multisensor Display (MSD). The Flight Data Display presents all flight information needed for flying and landing the aircraft. Pilots can also select to display sensor images here. The tactical situation and a digital electronic map are presented on the Horizontal Situation Display. The Multi-Sensor Display provides sensor information in different modes and the man-machine interface for all recording functions.

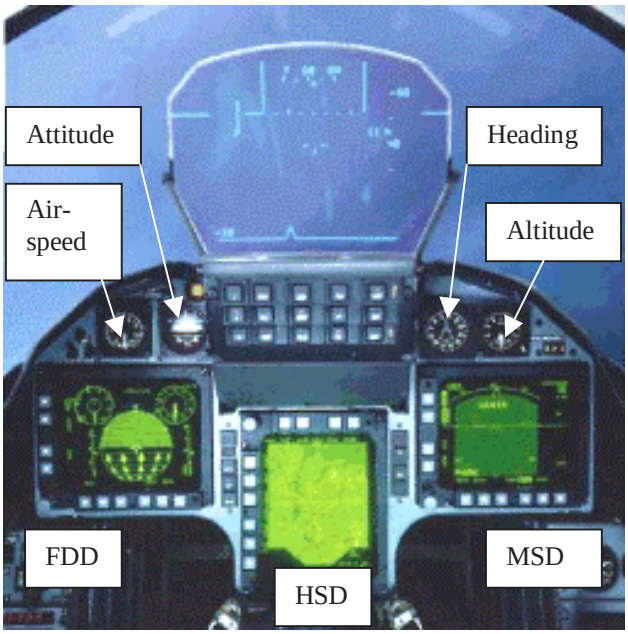

Figure 2.1: Current Gripen cockpit.

Figure 2.2: Forthcoming Gripen cockpit.

In lot 3 the Gripen cockpit is upgraded with three 6.2´´ x 8.3´´ full-color Active Matrix Liquid Crystal Display (AMLCD) multi-function displays, as shown in figure 2.2.

The size of the displays was chosen with the objective of achieving an all-glass cockpit. The display area has been expanded by approximately a factor of two which improves the opportunity to display information very clearly.

To make it possible to install the new and larger displays the electromechanical standby instruments had to be removed. Furthermore the AMLCD was required to have an additional graphics generator built-in for presenting stand-by flight data information in case of failure in the ordinary Display Processor (DP12).

The CMFDs receive flight data from two independent flight data sensor systems, one primary (ordinary) and one secondary (stand-by). All CMFDs have the ability to be switched over to display of back-up flight data from the secondary sensors.

3 System Design Overview

The CMFDs (FDD, HSD, MSD) are integrated in the Avionics System as indicated in figure 3.1. The normal display of flight data on the HUD and the FDD is controlled by the System Computer (SC) and generated by the Display Processor which is divided into two redundant parts DP1 and DP2. If this fails, the CMFDs´ internal back-up function generates a display of flight data from the secondary sensors transmitted over RS 485 Serial Links.

The Flight Control System (FCS) includes an integrity monitor functionality which compares primary and secondary flight data sensor output. Detected deviations, faults etc in the flight data display functionality are reported to the pilot by the function monitoring system (caution panel warning and information on the CMFD).

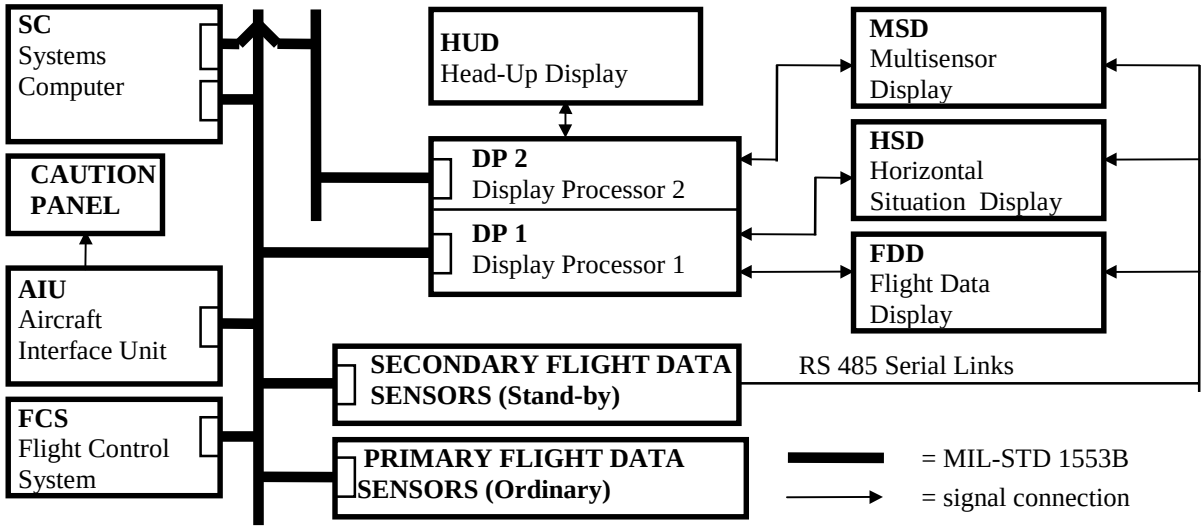

Figure 3.1: Gripen flight data and CMFD integration principle.

4 System Safety of Flight Data

4.1 Introduction

The commonly used method for expressing the required flight data capabilities has been, and is still, to require a mandatory carriage of certain equipment. This method constrains the optimum application of modern airborne equipment and the use of new types of instrumentation, such as large displays that disables the possibility to use self-contained stand-by instruments. Instead a concept were a set of required performances are defined will here be applied to the flight data display and specifically to set the requirements for the monitoring functionality.

The work to achieve the system safety of the new flight data presentation has forced a partly new design of the whole flight data system. The concept of disabling the continuous stand-by presentation also forced a new monitoring concept replacing the pilot cross comparison. This meant that a partly new concept of stating the system requirements was needed and that the system safety has been ensured by a deep investigation of all parts of the system.

The required system safety has been achieved by designing a system where the ordinary and emergency flight data system are totally independent except for the display surfaces.

The monitoring functionality is distributed both locally and central to ensure that no misleading flight data is presented to the pilot.

4.2 Hazards

The most hazardous situations regarding the display of flight data are

1. Total Loss of Display,
2. Hazardously misleading information, displayed without warning,

for the following entities:

- Airspeed
- Altitude
- Attitude
- Heading

Both situations are categorized to be catastrophic according to ref [3] for the first three entities. This categorization is assuming Instrumental Meteorological Conditions (IMC).

A hazardous situation does not necessarily lead to a loss of aircraft accident; it increases the exposure to an accident. The risk that an incident leads to an accident must be estimated as a conditional probability, that we call the accident-to-incident ratio. A catastrophic situation has a accident-to-incident ratio of 1:1 to 1:10.

The system safety work has to deal with the two different hazardous situations in two different ways:

1. The total loss of data must be prohibited by ensuring that the probability of losing both systems is very small.
2. The display of misleading information without warning must be prohibited by cross monitoring with a high level of confidence.

4.3 Traditional Requirements by Procedure

The monitoring of flight data is today depending on mandatory pilot cross monitoring. It can to a certain extent rely on continuous pilot cross monitoring of the electronic display of flight data on the HUD and the FDD against the following objects of comparison:

- electromechanical stand-by instruments.
- outside world when possible (i.e. VMC-Visual Meteorological Conditions) and relevant.

In this situation it is the pilot who has the main responsibility to discover if the ordinary system gives deviating flight data to what is stated above, or a fault has been flagged. The monitoring function according to this principle puts great disciplinary requirements on the pilot´s ability (human factor) to continuously check that the displayed flight data mirror the actual flight situation.

4.4 New Concept for Expressing Requirements

To set the requirements for the displayed flight data, including the monitor the same basic method as is used for navigation systems [1] and [2], i.e. Required Navigation Performance (RNP), will be used. The performance of the displayed flight data is then defined by three parameters - accuracy, continuity and integrity.

- *Accuracy* is the degree of conformance between the estimated or measured attitude, heading, airspeed or altitude and the true value.
- *Continuity* of a system is the capability of the total system to perform a function without interruptions.
- *Integrity* is a measure of the trust which can be placed in the correctness of the information supplied by the total system. Integrity includes the ability of the system to provide timely and valid warnings to the user when the system must not be used.

The accuracy requirement depends on the intended usage of the aircraft. It is important also to understand that the intended usage of the aircraft depends on the availability of the most accurate information. There are three levels of system degradation and the pilots possibility to accomplish a mission is decreased accordingly:

- *Ordinary* - Full system performance
- *Degraded* - Progressive degradation to limited mission performance
- *Emergency* - Capability for the flight safety and safe return to base.

Lowest level of performance requirement is to achieve a safe flight back to the nearest airfield and to land the aircraft.

The situations that must be prohibited with the highest level of confidence is the occurrence of a hazardous or catastrophic situation which may end in a loss of aircraft. The two most important situations that contributes to the risk of such a situation is a total loss of an important parameter and the presentation of hazardously misleading information without any warning to the pilot. The continuity requirement shall ensure a small likelihood of a total loss and the integrity requirement a small likelihood of a presentation of hazardously misleading information.

5 Fault Detection

In the design of complex systems there has been an increasing demand on reliability and safety as many applications are safety or economy critical and the interest in automatic *Fault Detection and Isolation* (FDI) has received a growing attention during the last decades.

In the literature there is a distinction between *failures* and *faults* as follows:

Failure - The term failure suggests a complete breakdown of a system component or function.

Fault -The term fault is used to indicate any kind of malfunction which may be serious or tolerable. These are sometimes denoted soft failures.

Typically, the risk of deterministic failures or faults, i.e. latent design errors in the hardware or software which repeat when the same (unanticipated) signal input condition is present, resulting in a hazardous situation is mitigated by using a highly structured development, and verification process

In practice, the most frequently used approach for fault detection is limit or trend checking of individual system variables. This approach is very simple but has a number of serious drawbacks, namely:

- In a dynamic system there is always noise present which means that either there will be a high rate of false alarms or the check thresholds have to be set quite conservatively due to large variations in the system variables.
- A single fault may cause a number of measurable variables to change and to exceed their limits making fault isolation very difficult.

Reliability and fault-tolerance in dynamic systems are traditionally achieved through hardware redundancy, meaning that there is redundancy in hardware elements, e.g. sensors, actuators. The use of redundant equipment

however has the drawback of extra cost, weight and size and this approach is mainly used in situations were redundancy is needed for maintaining the functionality after a failure. You can partially overcome this by using less accurate and less expensive second sources.

Both to overcome the problems with hardware redundancy and to improve the overall system reliability, analytical redundancy can be utilized. Analytic redundancy utilizes analytical models of the dynamic systems to generate redundant information of the parameters of interest. There might be a direct redundancy if there are multiple measurements that are analytically connected, or if not, there is always temporal redundancy if a dynamic model of the system is available. The term analytical redundancy is used for all methods based on some mathematical model of the underlying system.

Most diagnostic algorithms utilizing analytical redundancy consist of two parts:

- **Residual generator**

  The residual generator takes the observed input and output and transforms them into a sequence of residuals. These generators are designed in order to reflect possible changes of interest in the analyzed signal or system. They are typically close to zero under a no fault condition and their mean or spectral properties change when a fault occurs.

- **Decision maker**

  The decision maker uses a set of decision rules based upon the residuals to decide if and when a fault occurs. Thus the task is to design a convenient detector for detecting the changes in the residuals. Thereby the term ``change'' detection.

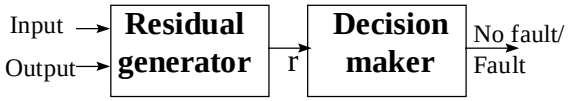

Figure 5.1. Two stage structure of an FDI process

For a dynamic system, the residual generator may be constructed by a number of different techniques with the main objective to design the residuals to be insensitive to noise or disturbances and to change significantly on a fault.

When the residuals have been generated, the next step is to check them for significant changes. The decision, whether a change has occurred in the residuals, has to be based on testing the residual or some test statistics of the residuals against a predetermined threshold.

Some indices of performance, that are often used for setting the requirement and for evaluation of detection algorithms are the following ones.

- Probability of false alarm
- Probability of missed detection.
- Maxim error before the fault is detected.
- Mean delay for detection.

The final step in an FDI scheme is to isolate the faulty part when a fault has been detected. To do this an additional set of data is needed. Since that is not the case in the system considered this part has to be performed by the pilot by cross comparing with the horizon.

6 Requirements and Design Concept

In this chapter the basic requirements and design principles for the system and the integrity monitor are discussed.

6.1 Basic Requirements

As stated in chapter 4.4 we will express the requirements in terms of accuracy, continuity and integrity.

The accuracy requirement will not be discussed further. From a safety stand point it will ensure safe return to base.

The continuity requirement shall ensure a small likelihood of a total loss of any flight data information and the integrity requirement shall ensure a small likelihood of a presentation of hazardously misleading information.

This means that we can form two fault trees;

1. Total Loss of Display,
2. Hazardously misleading information, displayed without warning,

for each entity:

- Airspeed
- Altitude
- Attitude
- Heading

The fault tree for the total loss of display of information will show that the continuity requirement is met.

$$P(\text{Loss of Stand-by}) * P(\text{Loss of Ordinary}) \quad (1)$$

That is valid if the ordinary and stand-by systems are design to be independent.

The fault tree for the hazardously misleading information, displayed without warning will set the basic requirements on the integrity monitor, i.e. the maximum probability for a missed detection.

$$P(\text{Misleading Ordinary}) * P(\text{Detection} \mid \text{Misleading ordinary}) \quad (2)$$

This means that given the probability for the ordinary system to output misleading data without warning the requirements on the monitor is given as one minus the conditional probability for a detection.

6.2 Requirements on CMFD Back-up Function

The CMFD´s back-up function shall permit safe return to base, at comfortable altitude and airspeed, and landing also after total loss of other avionics and or MIL-STD 1553B data bus communication.

For safety reasons the back-up shall be automatically activated:

- when the main MIL-STD 1553B data bus fails;
- when DP1-part of the DP12 malfunctions and makes transfer of flight data to the FDD impossible;
- when loss of AC power to the FDD occurs (for instance engine stop);

Furthermore, the pilot shall be able to manually activate the emergency display on any CMFD at any time.

The back-up function shall be available for all power supply modes, including battery level.

6.3 Requirements on Integrity Monitoring

Based on the basic requirements in section 6.1 the maximum probability for a missed detection is specified.

But to set the requirements on a integrity monitor the following must also be specified:

1. Maximum false alarm rate. What are the acceptable false alarm rate for the pilot to trust in the integrity monitor.
2. Maximum error before the fault is detected. There is a must to specify what the maximum acceptable error without a warning is, or in another word when is the error considered misleading.
3. Mean delay for detection. There will always be a delay in the detection and notification of the pilot. The acceptable time must be stated.

6.4 Basic Design Philosophy for Flight Data Integrity Monitoring

The removal of the old stand-by instruments, and the introduction of the new back-up system, also raises a need to define new design principles for pilot monitoring of flight data.

This is being dealt with in two ways. First, a special display mode is created to make it possible for the pilot to visually perform traditional cross monitoring between independent sources. Second, in order to make maximal tactical use of the CMFDs´ surfaces, automated (hidden) integrity monitoring is being used. These two monitoring concepts are described below.

6.4.1 Design Philosophy for Visual Cross-Monitoring

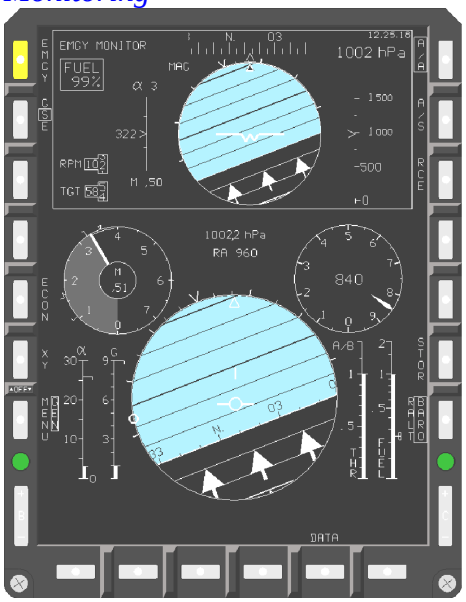

Figure 6.1. Information disposition of FDD display surface.

The basic flight data displays are the HUD and the FDD. The FDD is divided into two main image areas A and B according to figure 6.1. The figure also states what type of information can be displayed on each FDD image area. The most important prerequisite is the introduction of an "Secondary Sensor Monitor Mode" on (A). This mode enables cross-reading against the HUD, or against the "Standard Flight Data Mode" on (B).

The functionality of the "Secondary Sensor Monitor Mode" is illustrated in figure 6.2:

This functional design has two important qualities:

- The secondary sensor data used for creating the Secondary Sensor Monitor Mode is kept within the electronic display system which avoids using the Systems Computer (SC) in the actual image generation of this mode. The only SC impact is a command to Display Processor 1 (DP1) for activating display of the Secondary Sensor Monitor Mode on the FDD.

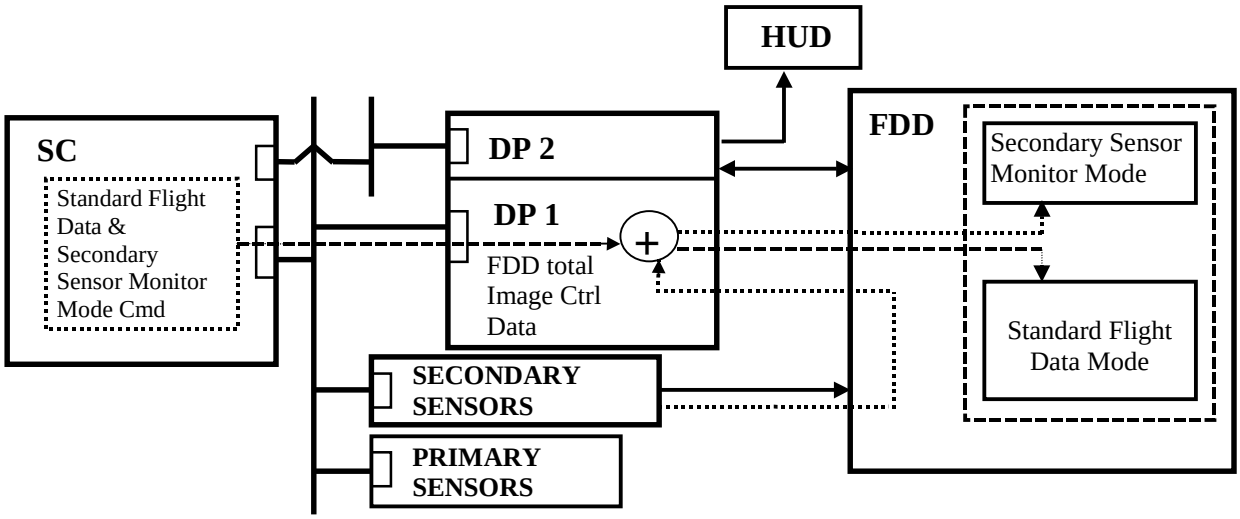

Figure 6.2. Secondary Sensor Monitor Mode

- The generation of HUD flight data image uses Display Processor 2 (DP2), while generation of FDD images uses DP1. Thus a great deal of functional independence is achieved between the HUD and the Secondary Sensor Monitor Mode.

6.4.2 Design Philosophy for Sensor Data Monitoring

An advanced monitoring function which operates automatically (hidden) has been introduced. The design goal is that the pilot shall be able to fully rely on this monitoring function, and thus be off-loaded from the visual procedure described in Section 4.3. Instead the pilot can concentrate on cross-monitoring HUD flight data to the outside world. If something fails with the Secondary Sensors or the CMFD built-in back-up function, the pilot will be given a computer generated warning.

The design philosophy and the structure of the sensor data monitoring is illustrated in figure 6.3.

Each computer in the Avionics Computer System (ACS) has a monitoring function organized in three basic parts:

- Internal (I): monitor the equipment's own functional status;
- External (E): monitor the quality of incoming data (parity, ability, range, checksum);
- Administrative (A): compiles data from external (E) and internal (I) monitoring for:
  - transfer to other systems;
  - initiation of fault handling in the equipment itself.

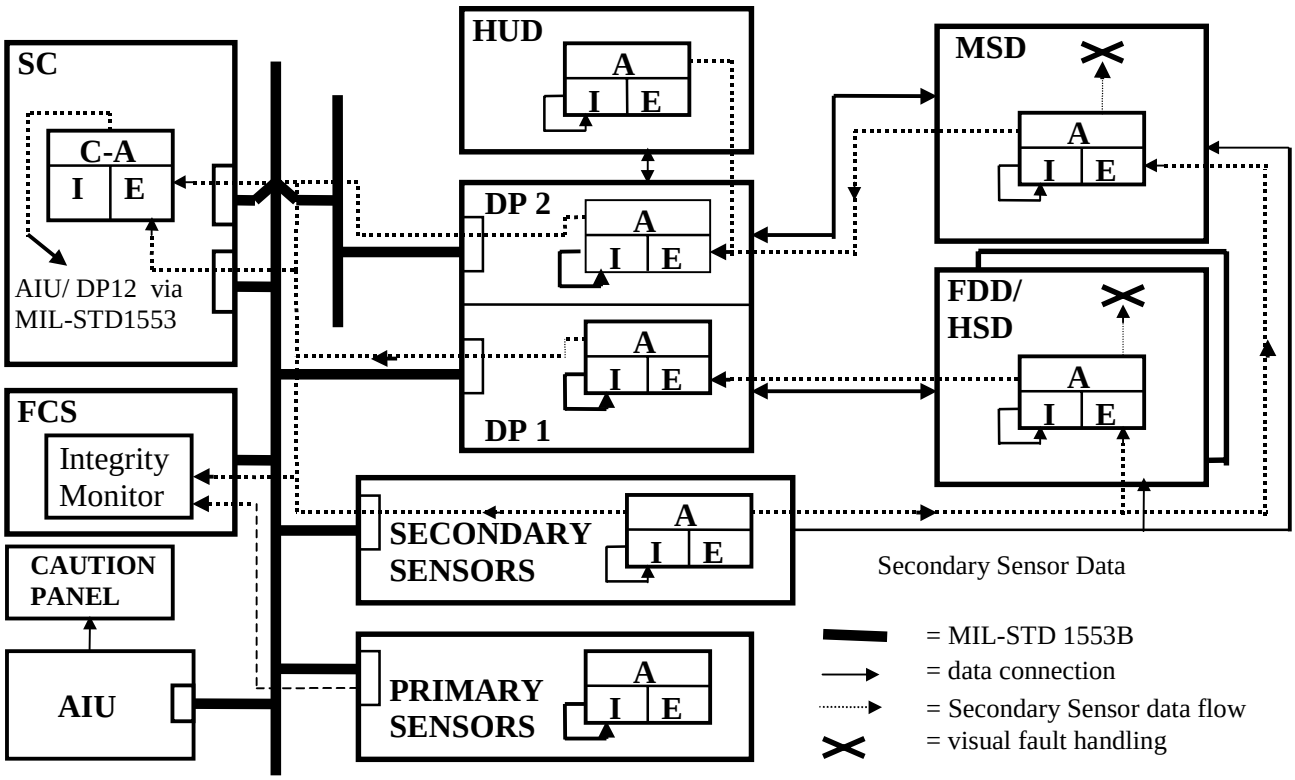

Figure 6.3. General structure of the new monitoring system.

As the data flows from the Secondary Sensors (for airspeed, altitude, attitude & heading), each receiving equipment processes the data first in the External Monitor part (E), adding data from the Internal Monitor part (I). Thereafter the Administrative Monitoring part (A) on basis of the result from (E) and (I) prepares refined monitoring data for transfer to the next receiving equipment ''downstream" in which the process is repeated. The Administrative part (A) also activates internal fault handling in the equipment concerned. This has for the new concept special implications for the CMFDs´ (FDD, HSD, MSD) in which the Administrative Monitor (A) has to decide if received flight data shall be displayed to the pilot or not.

The successively refined secondary sensor monitoring data finally ends up in the Central Administrative Monitoring function (C-A) situated in the SC, and in the Flight Control System (FCS) where the sensor data integrity monitor is located. The integrity monitor has access to primary and secondary sensor data transmitted directly from the sensors on the MIL-STD 1553B data bus, and constitutes the heart of the new flight data monitoring system.

7 Conclusions

With the introduction of the new 6''x8'' Color Multi Functional Displays in the Gripen aircraft the stand-by instrumentation will be deleted and a new concept for display of flight data has been developed

In this paper a new concept for ensuring system safety of the flight data display has been presented.

One of the aims of introducing the new larger displays is to use full screen and only presentation of ordinary flight data. Furthermore, a way to replace traditional mandatory pilot cross monitoring of flight data instrumentation with an automated monitoring functionality has been presented.

Finally, a way of defining the required performance of the displayed flight data by three parameters - accuracy, continuity and integrity - has been proposed.

8 References

[1] Kelly, R.J. and Davis, J.M. Required Navigation Performance (RNP) for Precision Approach and Landing with GNSS Application., *Journal of the Institute of Navigation*, Vol 41, No 1,pp 1-30, 1994

[2] *Draft Manual on Required Navigation Performance (RNP) for Approach, Landing and Departure Operations*., Appendix to ICAO All Weather Operations Panel paper AWOP-WP/721.

[3] MIL-STD-882C *System Safety Program Requirements.*