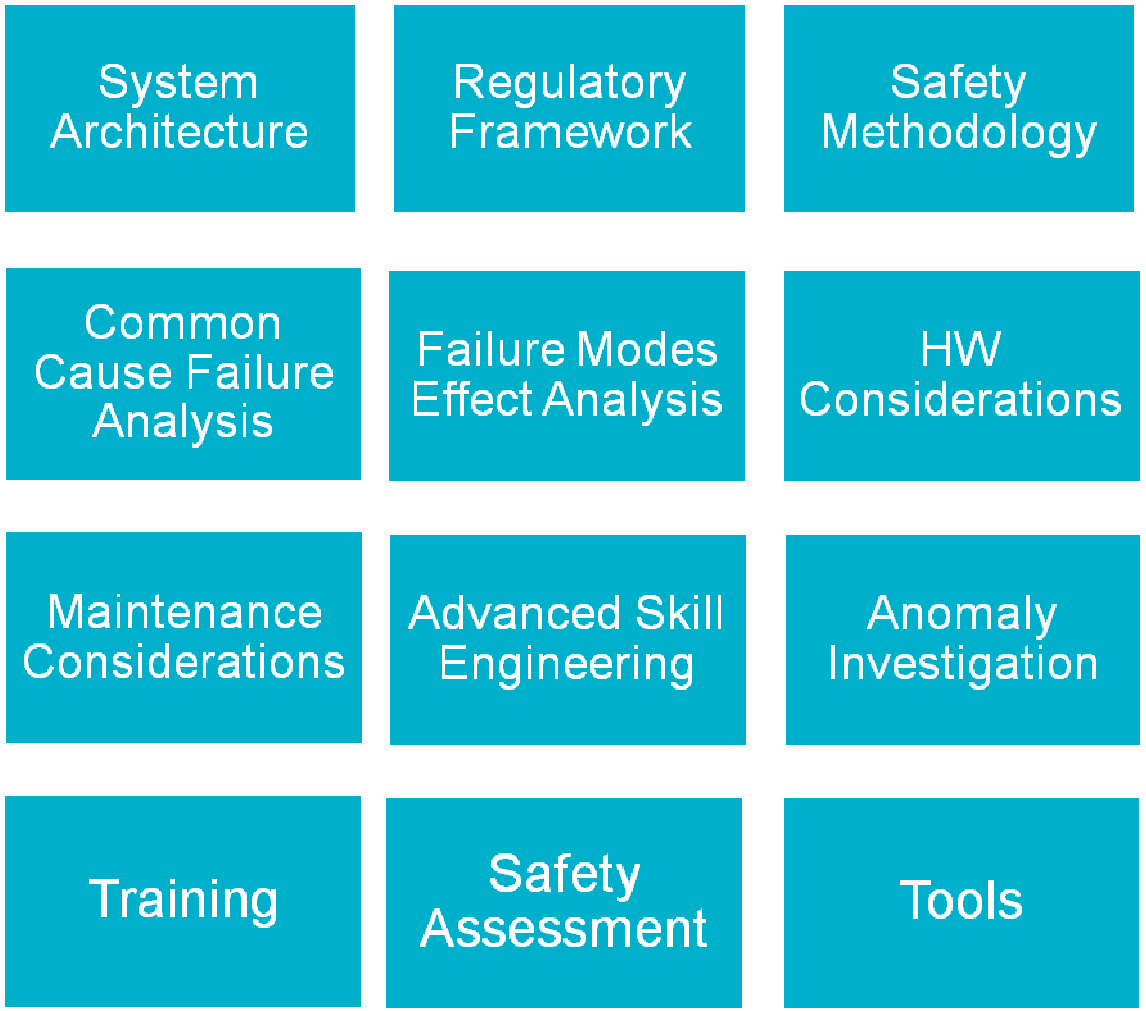
SOFTWARE SAFETY ASSURANCE SYSTEMS & DEGRADED MODES OF OPERATIONS in New FDPS

Bled, September 21st-22nd , 2011

INDEX


System Architecture
Regulatory Framework
Safety Methodology
Common Cause Failure Analysis
Failure Modes Effect Analysis
HW Considerations
Maintenance Considerations
Advanced Skill Engineering
Anomaly Investigation
Training
Safety Assessment
Tools

New FDPS “New Flight Data Processing System”

- Indra developed the New FDPS for Eurocontrol Maastricht.
- Project was executed from 2003 to 2008 in accordance with the contract.
- New FDPS is operational since 12th Dec 2008.
- One of the key aspects for the success of the project was the establishment of a close collaborative approach between Customer and Supplier.

Safety considerations in New FDPS

- This collaborative approach took place also in the safety-related aspects of the project.
- The safety aspects were taken into account from the very beginning of the project.
- The New FDPS specifications were developed including different types of requirements related to degraded modes of operation:
  - Safety
  - Operational Modes
  - Specific Recovery Mechanism
  - Graceful Degradation

Collaboration Service Provider/Supplier

- Eurocontrol and Indra adopted a pro-active and collaborative approach for the safety management in the development of the New FDPS.
- Collaborative approach between Eurocontrol and Indra was a key for reducing the safety risks associated with New FDPS.
- The safety analysis and assessment activities were performed together, considering all the supplier and user viewpoints, sometimes with initially different views.
- A realistic approach was applied when considering the safety requirements versus the reasonable practicable mitigations.

System Architecture

- The most important safety considerations were taken into account for the New FDPS system architecture and have been applied through different design principles, both, at system and SW level.
- The main safety related aspects of system architecture were:
  - Decoupling
  - Redundancy
  - Partitioning
    - Separation
    - Isolation
  - Modularity
  - Common Failure Analysis (ß factor)
  - Performance
  - Graceful Degradation
  - Reliability & Availability
  - Maintenance

Regulatory Framework

- The safety standard applicable was IEC 61508, which describes the safety integrity level (SIL) concept. Its application was a key element to provide evidence for ESARR2 compliance.
- Eurocontrol and Indra worked together efficiently, performing all the IEC 61508 processes and activities required for SIL 2.
- The assurance evidence obtained due to the application of IEC 61508 is at the same level of rigor as the one requested by ED-109 (AL4) or ED-153 (SWAL3). Some relevant assurance information obtained was:
  - Code Inspections Reports
  - Traceability Analysis
  - Unit Test evidence
  - Dormant Idle Code Study
  - COTS assurance reports
  - Control and Data coupling
  - Sensitivity Analysis, etc

Safety Methodology

- The complete Safety Assessment Methodology (SAM) was applied.
  - Functional Hazard Analysis (FHA)
  - Preliminary System Safety Assessment (PSSA)
  - System Safety Assessment (SSA)

- Early assessment performed by Eurocontrol and Indra allowed an early detection of the potentially unsafe cases, that is, assessing the risk before the recovery action were needed.

- The complete implementation of SAM and the promotion of safety culture improved some processes and activities already applied. Safety is for all and by all.

Failure Modes and Effect Analysis

- Specific Failure Modes and Effect Analysis (FMEA) activities were performed during New FDPS development.
- The FMEA encompassed the whole system:
  - HW
  - SW
  - Procedures and people (staff)
- System engineering of both sides participated in the FMEA.
- FMEA covered system state transitions and degradation modes.
- The FMEA conclusions were reflected in the project requirements, and ad-hoc system tests were performed to verify the FMEA results.
- Close collaboration between Eurocontrol and Indra allowed the detailed analysis of:
  - Paths leading to failure.
  - Recovery actions recommended.

CCF - Advance Skill Engineering

- Specific Common Cause Failure Analysis (CCF) activities were performed during New FDPS development.
  - Beta factor Estimation (ß factor)

- The results of the Common Cause Failure analysis were considered in:
  - Safety assessment activities:
    - Fault Tree Analysis
    - Reliability Block Diagrams
  - The analysis of the common resources usage for both, HW and SW.

- Participation of system engineers with high experience in ATM systems, made possible the early detection of safety issues and the identification of the system recovery means to be put in place.

HW & Maintenance Considerations

- Safety analysis was applied to the selection of appropriate HW equipment.
- The performed safety and assurance activities provided valuable inputs to maintenance process, such as:
  - Reliability, Maintainability and Availability Studies.
  - Data for spare equipment estimation.
- Specific sensitivity analysis was performed to identify potential problem areas related to HW.
- Maintenance activities were considered.
- Project team has been maintained after the system commissioning.

Anomaly investigation

- The verification of the tests which were obtained from the safety activities (FMEA, safety requirements,…) was useful to obtain reliable recovery mechanisms and contingency plans.

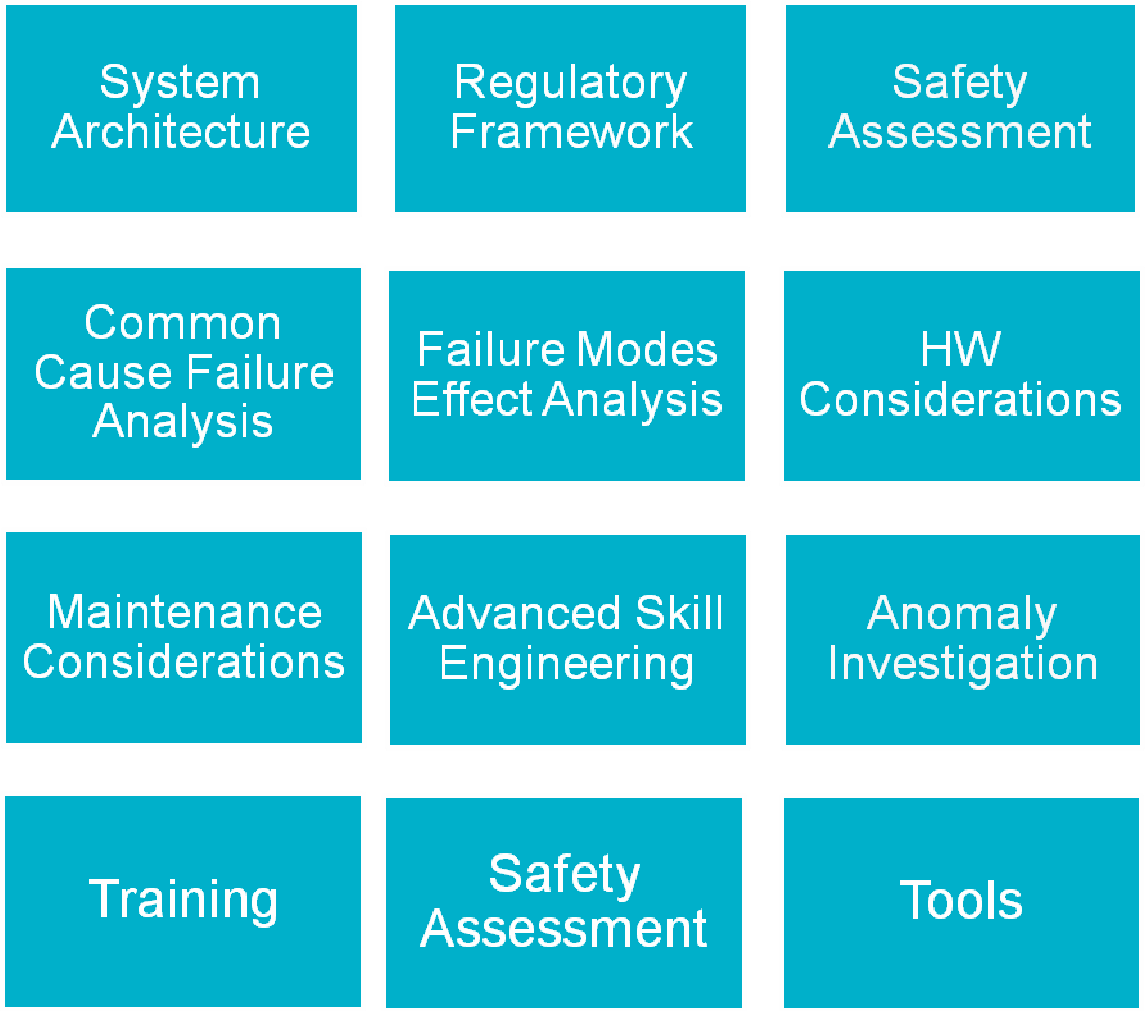
- The analysis and study of the system anomalies helped service provider and supplier understand the dangers of the degraded modes of operation.

Tool & Training

- Tools that were used for safety and assurance activities were assessed to ensure:
  - There were available people with experience in the use of the tools.
  - The availability and maintainability of the tool in the future.
  - The outputs obtained by the tool can be “easily” maintained.
- To give support in assessing the degraded modes and risks.

- Training was performed in order to continuously improve the product safety.
  - Operational staff received operational training.
  - Engineering staff received technical training.
  - Specific training sessions on safety and assurance issues were provided to all staff.

Software Safety Assurance System & Degraded Modes of Operations



INDEX

Lessons Learned (I)

- Close collaboration between System Provider and Supplier was a key element in the success of the project.
  - It allowed to reach a common understanding of safety implications.
  - A clear commitment with safety was present on both parties at all levels and in all teams.
- The safety assessment outcomes provided added value being used as inputs to other project activities:
  - System Engineering: New requirements were obtained.
  - System Verification and Validation: Ad-hoc tests were performed.
  - System Maintenance: Useful input information was provided.
- The safety analysis performed during New FDPS allowed:
  - Understand the paths leading to failure.
  - Assess the risk before the recovery action was needed.
  - Identify the required recovery means.
  - Recognize single points of failure.

Lessons Learned (II)

- The identification of balance of synchronisation between primary and redundant system was a key point in the safety analysis activities.
  - Synchronisation strategies must be adapted to system needs.
    - High data coupling increase common cause of failure.
    - Low data synchronisation leads to “poor” back-up system.
  - The propagation of failures must be tackled in design.
- The redundant system should be of lower complexity but at the same time should provide adequate functionality and services to be operationally usable.
- Application of SW assurance activities was another key point in the success of the project, providing real added value to system implementation.
  - The quality of the requirements improved.
  - The integrity of SW implementation increased.
  - Test procedures were more detailed and efficient.

INDEX

The Future

- Improve the risk assessment methodology to be less “heavy”.
  - Perform a quicker risk assessment:
    - Identify a more productive way to integrate safety assessment in system development.
- The consideration of the degraded modes in the safety assessment activities should be maintained for future projects.
- The identification of the failure and recovery paths was a key element in the success of the project and it is being maintained for the next projects.
- Keep working together (service provider and supplier) in the same collaborative way.

Thank your for your attention

Any Questions?

Indra Sistemas S.A.
Ctra. de Loeches, 9
28850 Torrejón de Ardoz
Madrid, Spain
T +34 916 271 159
F +34 916 271 005
www.indra.es