Failure Modes and Effects Analysis (FMEA) and Systematic Design

J. Murdoch, J.A. McDermid; High Integrity Systems Engineering Group;
University of York, York, YO10 5DD UK
P.Wilkinson; Rolls Royce plc; PO Box 31, Derby,
DE24 8BJ UK

Keywords: FMEA, safety, design for safety

Abstract

The paper describes recent work to improve the safety process for aero-engine controllers. The role of FMEA is discussed in the context of the safety and certification processes, with reference to ARP 4754 and ARP 4761. Whilst the ARPs' emphasis on top-down hazard-driven approaches is valuable, it is concluded that the role of FMEA should not be down-played. Instead it should be recognized that FMEA is complementary, and offers a way of managing other sorts of risk, including project risk. In particular the role of "Potential FMEA" from the automotive industry in managing failure mode risk is discussed. Practical implications of the approach are discussed, although details of its application are not given.

Introduction

The safety assessment process for complex aerospace systems involves co-ordination of different organizations, as well as technical activities. The control system integrator works at a middle tier of system integration, providing links between suppliers and “customers” at the engine and aircraft levels. The control system integrator has to “flow down” hazard related information to suppliers, and to integrate and “flow up” failure mode related information. This role is not really reflected in current regulations.

Control system applications involve a range of implementation technologies, such as:

- Electro-mechanical hardware, including actuators, sensors, and cabling & packaging;
- Fluidic systems, including hydraulics, fueldraulics and thermal systems;
- Electronic hardware, including micro-processors, PLDs, ASICs, and power electronics;
- Software including “applications”, device drivers and real time operating systems.

The work reported here focuses on civil aircraft systems, especially engine controllers, which are subject to regulatory flight worthiness approval against JAR Parts 25 & E, or FAR Parts 25 & 33. The system development and safety processes are undertaken against guidelines including ARP 4754 (ref. 1) and ARP 4761 (ref. 2) at system level, DO-254 (ref. 3) for electronic hardware, and DO-178B (ref. 4) for software.

The motivation for the work was to improve co-ordination in the supply chain, and thus to reduce the number of issues which arise late in the process, and to improve the quality and value of information provided by the FMEAs. All the improvements must comply with the relevant guidelines. We discussed limitations in the PSSA process in an earlier paper (ref. 5), focusing on the top-down, hazard-directed aspects of the safety process. The work here is complementary, as it considers bottom-up, failure-mode directed aspects of the process based on FMEAs.

FMEA is a mature technique (with several variants) and is well described in the literature (refs. 6, 7). The method plays a foundational role in many standards (refs. 8, 9) including the ARPs and DO-254. Our concern here is the concurrent application of FMEA at all assembly levels of system development and its relationship with design assurance processes.

The paper has three main parts: (1) identification of four issues which have arisen in efforts to comply with the ARPs; (2) discussion of possible responses to these issues; (3) suggestion of an extended role for a ‘generalised’ FMEA as a key element of the safety process. The paper then considers application of FMEA to *repeat* and *novel* design situations, and the integration of FMEA results between levels in the system hierarchy. The closing section identifies some practical implications of making these process improvements.

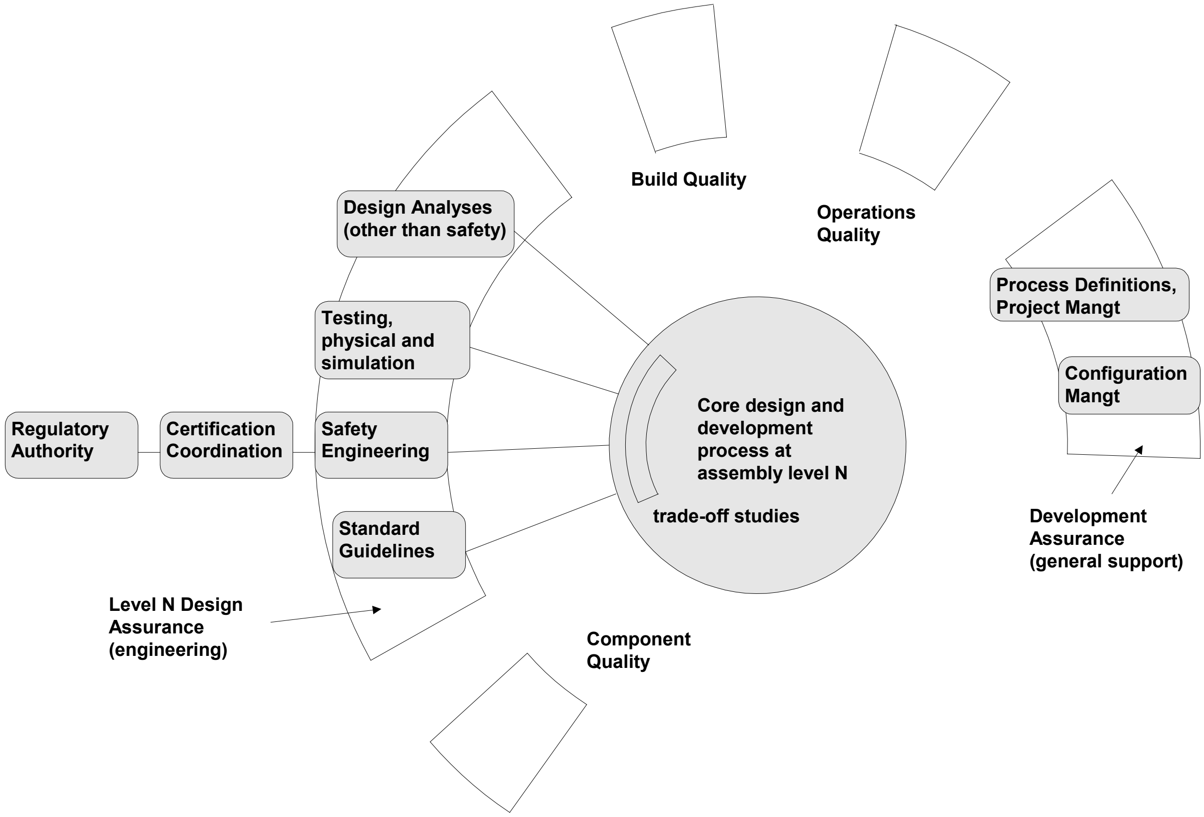
Build Quality
Operations Quality
Design Analyses (other than safety)
Process Definitions, Project Mangt
Testing, physical and simulation
Configuration Mangt
Core design and development process at assembly level N
Regulatory Authority
Certification Coordination
Safety Engineering
trade-off studies
Standard Guidelines
Development Assurance (general support)
Level N Design Assurance (engineering)
Component Quality

Figure 1 – General Process Concept showing Separation of Design, Safety and Certification Concerns

Four Issues Arising from the ARPs

The regulatory guidelines are written, at least in part, from the point of view of system certification. However, manufacturers wishing to comply with the guidelines have to integrate certification activity into wider product development processes. In our experience this raises a number of issues, four of which are addressed in this paper:

1. Safety certification is not the only concern of safety engineering. In particular, safety engineering has to support system design decision-making, for example trade-offs against other system properties;
2. A top-down, hazard-driven approach is adopted by the ARPs in order to organize certification data. However, practical system development is rarely conducted "purely" top-down. In practice there is both a bottom-up element to design, and frequent iteration;
3. In the interests of generality, the guidelines purposely do not address role/responsibility aspects of safety process design. However this is an important issue in projects and organizations;
4. *Complex* systems are defined as those for which deterministic testing cannot establish correct operation to the required confidence level; the guidelines introduce the concept of *Development Assurance Levels* (DALs) for such systems. However, for manufacturers, quality and development assurance is a wider issue than safety.

None of these issues are perceived as showing that the ARPs are "flawed", but simply indicate that they do not address all the issues needed to establish an effective safety process.

Responses to the Issues

Issue 1, Certification Coordination: Figure 1 summarizes the general organizational approach adopted in response the first issue. ARP 4754 identifies Certification *Coordination* as a support process, but does not amplify on the role. In our view it is useful to distinguish this role from that of *Safety Engineering*. The *Certification Coordination* process exerts considerable influence on *Safety Engineering* but having a separate safety process makes clear the

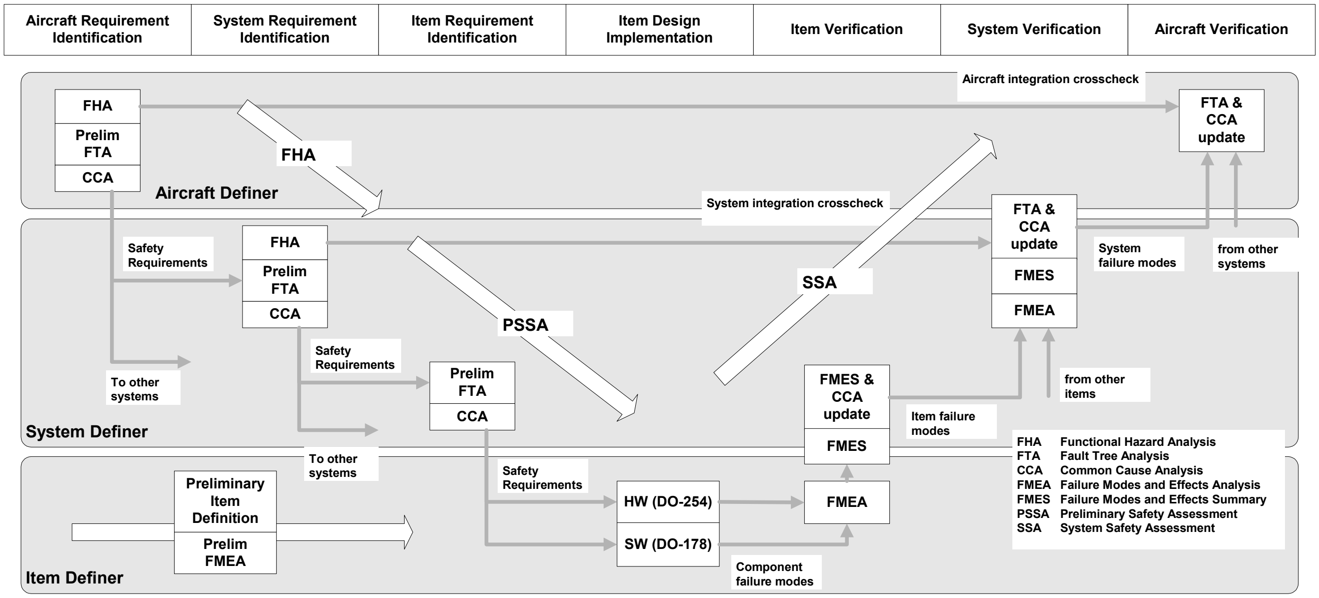

Figure 2 – Concurrent Development View of the System Safety Assessment Process

ownership of safety work not directed at certification.

Safety Engineering is viewed as one component of design assurance (see below). Both *Safety Engineering* and *Certification* are distinguished from a *Core Design and Development* process, where the design decisions are made. The core development, at system integrator level, is viewed as a S*ystems Engineering* process (ref. 10.). This is fundamentally an *engineering design* process, comprising the following general tasks:

a. Development of control system requirements derived from design processes undertaken by customers working at higher levels of system assembly (whole engine and aircraft levels);
b. Development of system architectural design alternatives in response to requirements, viewed as a multi-disciplinary effort. *Technical Performance Measures* (TPMs) (ref. 11), or effectiveness measures, would be used to enable design alternatives to be compared and the most promising selected for further development. The process would support the assessment of design proposals from several different views, necessary to support assessment of each TPM;
c. Development of requirements to be placed on item (subsystem, unit or component/ item) developers working at lower assembly levels;
d. Management of the development and/or procurement of items, involving teams internal to the company and/or suppliers;
e. Integration and test of the control system prior to delivery to customer processes.

Bell and Reinert (ref. 12) have considered the development of safety-critical systems as a process of risk management. More generally, an *opportunity/risk management* approach is typically adopted to support design decision-making, where *technical risk* is viewed as the potential for not meeting requirements associated with a TPM. Safety-related TPMs are assessed by Safety Engineering, which can be seen as evaluating *hazard* risk. It is shown below that safety engineering can contribute by managing *failure mode* risk, concurrently with *hazard* risk management, using Potential FMEAs. This enables it to fill a broader role in opportunity/ risk management.

The process organization described in Figure 1 does not ensure that safety is considered in trade-offs – but it helps to identify this broader role.

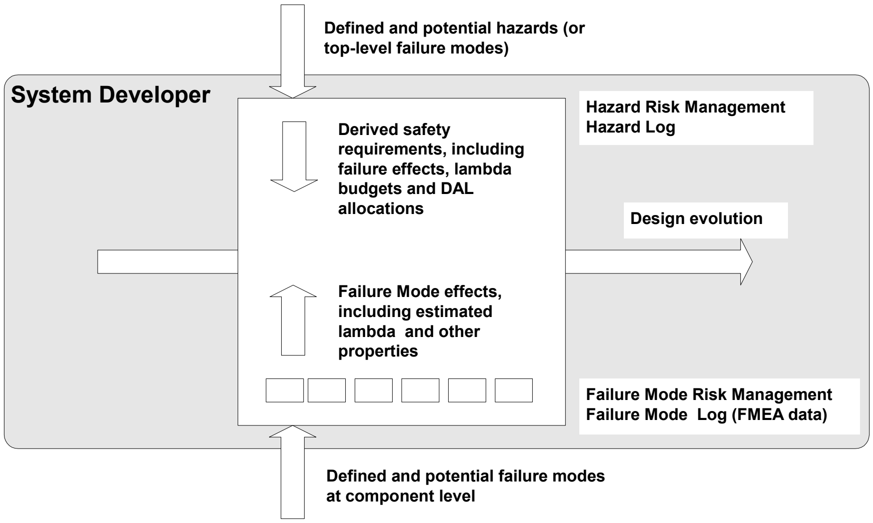
Defined and potential hazards (or top-level failure modes)
System Developer
Derived safety requirements, including failure effects, lambda budgets and DAL allocations
Hazard Risk Management
Hazard Log
Design evolution
Failure Mode effects, including estimated lambda and other properties
Failure Mode Risk Management
Failure Mode Log (FMEA data)
Defined and potential failure modes at component level

Figure 3 – Top-Down and Bottom-Up Safety Assessment at a Particular Assembly Level

Issue 2, Top-down, and bottom-up safety assessment: ARP 4761 includes a process chart similar to Figure 2 (our modifications are described in the following paragraph). It is noted that the ARP takes a hazard-driven, *requirements management* approach to the development and gathering of certification data. The main recommended safety assessment technique (FTA) is top-down, and driven by top-level functional hazard assessment. The focus is on defining and decomposing safety requirements to be placed on item developers. Interestingly, the development activities (the top row) in Figure 2 also imply that design happens at *Item* level rather than at *System* level.

Figure 2 has been modified from the ARP in two ways. The roles of *Aircraft Definer*, *System Definer* and *Item Definer* have been super-imposed on the V-process, to show that the development and associated safety activities are undertaken concurrently at each level. Also, a *Preliminary Item Definition* task has been added to indicate concurrent development at item level, prior to definition of derived safety requirements.

The view is taken that *Safety Engineering* is fundamentally concerned with the assessment of product designs, at all assembly levels. It also supports the management of safety requirements and verification against them, which are the main concerns of *Certification*. Following the systems engineering approach, development at all assembly levels is treated as involving design, integration and operations design activity.

The safety process strategy adopted here is 'dual track'; to manage *failure mode* risk concurrently with *hazard* (safety) risk. Failure mode risk management is conducted independently of hazard concerns, at least in the earlier stages of a project. This dual-track approach provides a balanced top-down and bottom-up assessment, and is associated with each design team involved in a project. In terms of Figure 2, the dual track approach would be applied at each assembly level, supporting concurrent development. The bottom-up assessment supports the assessment and trade-off between design alternatives, something not supported by top-down requirements allocation. Figure 3 summarizes this approach at a particular assembly level.

Design assessment at a particular assembly level considers the smallest components in terms of which the design is expressed, at that level. Design validation is part of an organization's quality effort, discussed further below.

FMEA provides a key approach for failure mode risk management, as developed in the following sections. Failure mode risk management also supports other failure-mode related specialties. FMEA has been included with the *Preliminary Item Definition* task in Figure 2.

Issue 3, Role/responsibility assignment: The separation of responsibilities between assembly levels and different items raises difficulties for safety assessment. Although the ARPs are mute on this, it is possible to make useful generalizations. The left half of Figure 4 shows an iterative design activity linking a *Customer* and a *Supplier* role under conditions of perfect communication. Design at system level is accompanied by safety assessment work yielding derived safety requirements placed on the item. Item development results in an item design and an assessment of failure modes presented to the system. The effects of item failure modes on the system are assessed. In the general case, system design and derived safety requirements are modified for a further iteration.

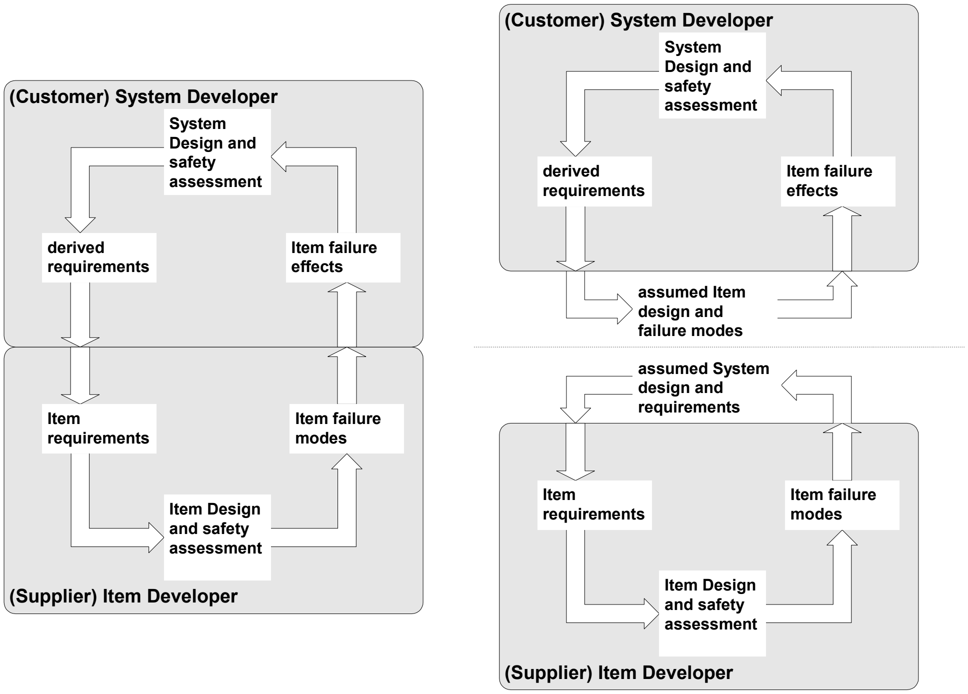
(Customer) System Developer
System Design and safety assessment
derived requirements
Item failure effects
Item requirements
Item failure modes
Item Design and safety assessment
(Supplier) Item Developer
(Customer) System Developer
System Design and safety assessment
derived requirements
Item failure effects
assumed Item design and failure modes
assumed System design and requirements
Item requirements
Item failure modes
Item Design and safety assessment
(Supplier) Item Developer

Figure 4 – Iterative Development between *Customer* and *Supplier* Roles in Conditions of (a) Perfect Communication and (b) Imperfect Communication, Involving the Making of Assumptions

The right hand chart in Figure 4 shows the situation where communication between the roles is imperfect. This can arise because of relative time shifts between the activities at different levels, contractual constraints or disparate technical fields. Under these circumstances, independent design and assessment may proceed under assumptions about the designs and failure modes and effects of the other level. Any assumptions will eventually have to be checked and validated.

A purely top-down approach is not appropriate for safety requirements because they are usually *negative* in character; meaning that a system requires an item *not* to fail in any way which endangers the system. The openness of negative requirements requires more interaction between *Customer* and *Supplier* roles than do positive functional requirements. Typical mis-understandings include the *Customer* not expressing a requirement on an item because the possibility of some behavior was not known. Similarly, the item *Supplier* may not identify a failure mode due to being unaware of a sensitivity at system level.

In the following, the FMEA technique is applied to the assessment of as-designed systems and also to anticipated designs owned by other roles and not yet communicated.

<u>Issue 4, Development Assurance:</u> Figure 1 identifies development assurance activities of various kinds at each assembly level. It seems helpful to distinguish *general* support processes, such as outline process definitions, project management, configuration management etc. which provide housekeeping functions, from *engineering* validation effort. Under the second heading, the literature typically identifies *design*, *component*, *build* and *operational* quality. Component quality maps onto quality processes at the next level down. Design quality, the main concern in this paper, comprises guidelines for

good practice, including definition of systematic design methods, as described below, and design validation activity.

Safety engineering is one component of design validation, but there are others including physical prototype testing, simulation and design analyses not specific to safety, but supportive of it (e.g. *Worst Case Analyses*). We view safety engineering as being undertaken within an environment which includes general design validation effort. A general quality and design validation context is a necessary platform for safety engineering activity.

An Extended Role for FMEA

FMEA is treated as a key element in design validation at each assembly level. Top-down methods (such as FTA) are efficient in that they focus on particular areas of safety and certification concern, but do not provide general validation support.

FMEA is arguably the fundamental technique for identifying and managing single point failure modes, applied traditionally to piece-part and functional descriptions (ref. 6). We are concerned here with FMEA applied to all assembly levels, including architectural levels. Several techniques similar to FMEA, including HAZOP (ref. 13) and software HAZOP, share the property that they are concerned directly with assessment of system designs. We consider these techniques as variants of FMEA which share a bottom-up approach applied 'locally' within an assembly level.

A system may generally fail in one of two ways; (1) as a result of a component failure or (2) as a result of unintended functioning when all components are behaving to specification. Each of these may be caused by either (1) a fault intrinsic to the component or system or (2) by an external disturbance. In this paper we include consideration of all these types of failure under a generalised FMEA heading, applied at each assembly level. It is recognised that techniques have been developed in particular domains to support parts of this assessment (e.g. *Sneak Path Analysis* in the electronics domain).

Figure 5 illustrates the assessment of a system at some midpoint in its design definition, at some assembly level. There are three main sources of information to support an assessment: (1) the results of assessment at an earlier stage of the project, e.g. list of safety issues; (2) the current design definition and (3) anticipated future design and implementation, based on knowledge of similar products.

The basic approach is to link FMEA application as closely as possible with design methods and data. Concurrent application of FMEA to different assembly levels implies that assumptions have to be made (Figure 4(b)). This involves a risk management approach to support the making of assumptions. FMEA used in a predictive manner is proposed for this, an approach affected by the level of precedence in the design situation. Concurrent application also raises the issue of eventual coordination between levels.

Novel Design FMEA

Engineering design domains develop systematic design methods in order to reduce development risk. Definition of reference processes would be contained in the Standards/ Guidelines element of Figure 1. Perhaps the classic approaches are those due to Pahl and Beitz (ref. 14) in the mechanical engineering domain and methods enshrined in the VDI standards in Germany. The steps of *functional modeling*, *identification and selection of physical solution principles*, *concept design generation and selection*, *architectural* and *detailed design* are recommended. Analogous processes have been developed in the real time systems and software domains. Computer-based systems methods are more concerned with behavioural properties and timing than embodiment and structural issues. Functional modelling appears in most methods. The discussion of system development above draws from systematic design principles in the systems engineering domain (ref. 10).

In novel design situations (and in the novel areas of variant design) there is little prior knowledge of the as-operated form of the product. FMEA application necessarily is based on systematic design methods and the *current* design definition. The fundamental approach is that the FMEA is a sceptical assessment of all design descriptions available, forming a search for potential (or actual) departures from design intent. Emphasis is placed on the product models that are available - as complete a picture of the design as possible is needed. This is in

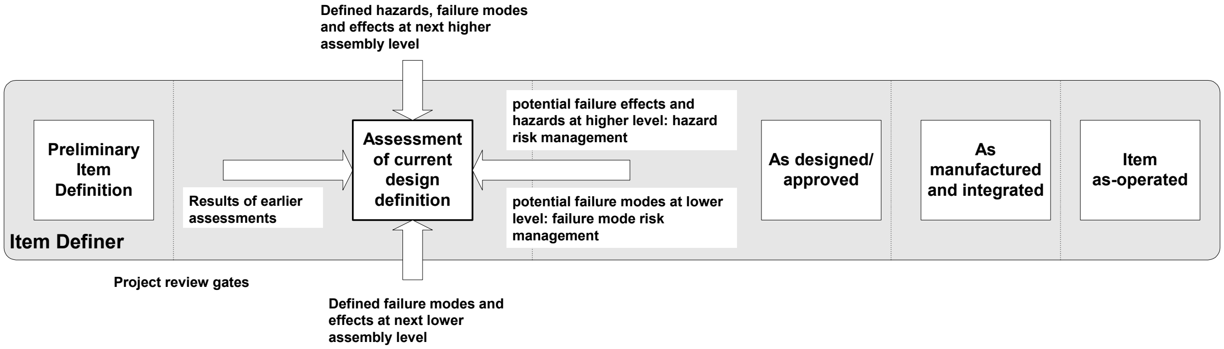
Defined hazards, failure modes and effects at next higher assembly level
Preliminary Item Definition
Results of earlier assessments
Assessment of current design definition
potential failure effects and hazards at higher level: hazard risk management
potential failure modes at lower level: failure mode risk management
As designed/ approved
As manufactured and integrated
Item as-operated
Item Definer
Project review gates
Defined failure modes and effects at next lower assembly level

Figure 5 - Evolution of a Design during a Project, Illustrating Three Aspects of Safety Assessment Based respectively on (a) Previous Assessment, (b) Current Design Data and (c) Design Expectation.

accord with the model-based approach to systems engineering.

The character of the FMEA technique varies according to the nature of the design description to which it is applied. Hardware systems are the traditional application domain; electronic hardware approaches, because of the distributed circuit nature of the designs, emphasise functional paths and failure paths (ref. 3). Functional FMEA (F-FMEA) has been applied to all domains, including software.

Different models will be assessed in different ways. Function structures can be subject to F-FMEA and the related HAZOP technique as applied to architectural block diagrams (ref. 13). Physical solution principles can be assessed with regard to their susceptibility to interference within the planned operational context etc. Preliminary layout diagrams may be subject to preliminary Zonal Analyses.

Behavioural descriptions are also amenable to sceptical investigation. Use cases and message sequence charts have been used in this way (ref. 15). Checklists of possible departures from design intent can be built up for each design representation, similarly to the guidewords in HAZOP.

Assessment of early and evolving designs results in the raising of safety concerns, which can be flagged for later analysis and review. This amounts to an approach to managing the risk of introducing failure modes into a new design at a particular assembly level. Assumptions will probably have to be made about the failure modes of components, the effects of failure modes at the higher assembly levels and about environmental conditions.

Repeat Design FMEA

In the case of repeat (or near-repeat) design, there is much advanced knowledge about the item or system in its as-operated form. An extension to support the identification of *potential* failure modes in proposed designs, called *Potential FMEA*, was developed in the automotive industry in the 1990's (ref. 16). A Potential FMEA is conducted early in the design process, raising safety concerns, based on knowledge of the performance of similar systems. These concerns are recorded and tracked in a similar fashion to failure modes identified in standard FMEA. Effectively, it is a form of risk management, with design and safety activity being directed by the issues raised. Safety concerns can be input to subsequent design reviews, with the objective of designing out the potential failure modes or otherwise demonstrating how they are to be contained.

This approach provides a means of bringing component, build and product service data to bear on design decision-making. It is not required initially that the failure modes be traced to top-level system hazards. The approach is therefore a conservative one, aimed at general quality improvement in design. As the top-down system design and safety assessment progresses, attention can be progressively focussed on the more critical failure modes.

Coordination between Levels

Analyses conducted independently at different assembly levels will eventually have to be coordinated. All assumptions made by each level about the others have to be checked. This is achieved by the integration of FMEA data between levels, when failure modes identified at Item level are grouped into failure effects at the next higher level. The grouping of failure modes (sometimes called *tagging*) is an area where assumptions have to be made and checked. System integrators have to be aware that item failure modes may be equivalent from one point of view (e.g. BITE specification) but distinct from another view. Project design reviews provide the formal approval and oversight of this coordination.

Practical Implications

Some practical implications of the above discussion are sketched in the following paragraphs.

Safety Engineering is viewed as an element of design validation, with specific responsibility for managing hazard and failure mode risks in system development. Certification Coordination is treated as a separate area of responsibility.

Product development is viewed as evolving concurrently at several levels of assembly. Design validation, including safety assessment, is applied at each level. A design orientation is applied at system level just as much as at item level.

In order to progress concurrent development at each level, assumptions have to be made. This results in a risk management view at both the Customer (system) interface, in terms of hazards and sensitivities, and at the Supplier (component) interface, in terms of failure modes.

An FMEA task is introduced at each assembly level to support assessment of design proposals. Other design analyses are expected to be present as well, covering non-safety aspects of design validation (some of which will have safety implications). Top-down hazard identification and safety requirements decomposition as advised by the ARPs will also be undertaken; this activity will coordinate the certification data for the total product.

FMEA is used as a focus for bottom-up assessments of various kinds, including different views of a design e.g. layout, functional, behavioural (scenario, state).

The Potential FMEA method supports a predictive application for an item and is revised during development, culminating in the final FMEA delivered to the next higher assembly level, along with the tested and integrated item. The FMEA is effectively being used as a Failure Mode Log, analogous to a Hazard Log, supporting a bottom-up approach to safety assessment. Coordination between teams and organisations is generally achieved through phase gates and design reviews. The issues and concerns raised in the Potential FMEA will result in activity to be reviewed as part of the planned design reviews. Arrangements between customers and suppliers should be negotiated to accommodate the rolling plans implied by this approach.

The allocation of Development Assurance Levels is recommended in the ARPs for complex systems. The approach described in this paper implies that early DAL assumptions may have to be revised as a project unfolds. This raises difficulties if a DAL is made more severe part way through the development of an Item. This situation is similar to the COTS case, where development assurance data is not available. Negotiation with the Certification Authority would be required to establish acceptable substantiation. In the worst case, re-work may be necessary.

The assignment of role responsibilities is central to the approach discussed here. The safety assessment responsibility allocation mirrors design authority allocation. In many cases, this will reflect the architecture of the product and the responsibility assignments which have evolved historically in the domain.

Conclusions

The ARPs present a view of safety engineering which is, understandably, focussed on certification. This paper has argued that the top-down, hazard-driven view is rational for developing coherent safety arguments about a system but does not reflect the concurrent, distributed nature of system development.

It has been argued that additional application of bottom-up assessment techniques, especially the classic FMEA method, provides a balanced approach. The FMEA technique can be applied at each level of system development, to the complete set of design views and models available and in a predictive manner. Safety engineering is viewed as being part of design validation, with responsibilities for risk management of hazards and failure modes. Safety assessment techniques are considered side-by-side with other design analysis techniques, fostering an engineering approach to safety.

Acknowledgements

Thanks to colleagues at R-R Derby, especially Bob Knaggs and Ivan Edwards, and at York, especially Mark Nicholson.

References

1. ARP 4754 Certification considerations for highly-integrated or complex aircraft systems; SAE Systems Integration Requirements Task Group AS-1c, ASD, Society of Automotive Engineers Inc., December 1994.

2. ARP 4761 Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, SAE Committee S-18, Draft 13a, Society of Automotive Engineers Inc., August 1995.

3. DO-254/ED-80, Design Assurance Guidance for Airborne Electronic Hardware, RTCA/ EUROCAE, April 2000.

4. DO-178B/ED-12B, Software Considerations in Airborne Systems and Equipment Certification, RTCA/ EUROCAE, 1995.

5. Dawkins S., McDermid J. A., Murdoch J., Pumfrey D. J., Issues in the Conduct of PSSA, *17th International System Safety Conference*, 1999, Orlando.

6. MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis, US DoD, Washington D.C., 1984.

7. Failure Modes and Effects Analysis, A Special Bibliography from the NASA Scientific and Technical Information (STI) Program, February 2000.

8. International Standard IEC 1812, Analysis Techniques for System Reliability: Procedures for Failure Mode and Effects Analysis, Geneva, International Electromechanical Commission, 1985.

9. BS 5760 Part 5: Guide to Fault Mode and Effects and Criticality Analysis (FMEA and FMECA), BSI, UK, 1991. Also IEC, Draft International Standard 1508 Functional safety: Safety-related System, International Electrotechnical Commission, Geneva, 1995.

10. ISO/IEC 15288, Life Cycle Management - System Life Cycle Processes, ISO/IEC JTC 1/SC 7/ WG 7, 2000.

11. Blanchard B.S., System Engineering Management, Wiley, New York, 2nd edn., 1998.

12. Bell R., Reinert D., Risk and system integrity concepts for safety-related control systems, Microprocessors and Microsystems, 17(1), 3-15, 1993.

13. Murdoch, J., McDermid J.A., Astley K., Reid S., Wilkinson P., Applying HAZOP to functional system models, in *16th International System Safety Conference*, 1998, Seattle, Washington.

14. Pahl G., Beitz W., Engineering design: a systematic approach, Springer Verlag 1977, English translation, Design Council, London UK, 1984.

15. Allenby K., Kelly T., Deriving Safety Requirements Using Scenarios, Fifth IEEE International Symposium on Requirements Engineering (RE'01), Toronto, August 2001.

16. Potential Failure Mode and Effects Analysis: Reference Manual, Chrysler Corp., Ford Motor Company, General Motors Corp., developed under the auspices of the Automotive Division of the American Society for Quality Control (ASQC) and the Automotive Industry Action Group (AIAG), 2nd Edn, February 1995.

Biographies

John Murdoch, High Integrity Systems Engineering Group, University of York, York, YO10 5DD UK, telephone - (44) 190 443-3375, facsimile - (44) 190 443-2708, e-mail - murdoch@cs.york.ac.uk

John Murdoch has worked for over fifteen years in the aerospace industry, in a variety of specialist, systems engineering and R&D roles. Currently, with the Rolls-Royce University Technology Centre, he has interests in process and product modelling for high integrity systems.

John A. McDermid, High Integrity Systems Engineering Group, University of York, York, YO10 5DD UK, telephone - (44) 190 443-2726, facsimile - (44) 190 443-2708, e-mail - jam@cs.york.ac.uk

John McDermid is Professor of Software Engineering and Head of the High Integrity Systems Group within the Computer Science Department of the University of York, UK. He also heads the Rolls-Royce Systems and Software University Technology Centre at York. His research interests are in safety critical systems and software, especially in aerospace applications.

Philip Wilkinson, Rolls Royce plc, PO Box 31, Derby, DE24 8BJ UK, telephone - (44) 133 224-7935, facsimile - (44) 133 224-4225, e-mail - P.J.Wilkinson@rolls-royce.com

Phil Wilkinson has been with Rolls-Royce for 18 years. He has worked in a range of specialist safety, design and management roles in Control Systems and is currently Group Manager of the Systems, Safety and Reliability Group.