Military Aviation Authority

MAA

SYSTEM INTEGRITY HANDBOOK (SYSI HB)

GUIDANCE DOCUMENT IN SUPPORT OF RA 5721

Cover photo shows zonal contamination due to fluid leakage surrounding electrical terminal blocks.

FOREWORD

This handbook has been produced to support Regulatory Article (RA) 5721. It provides a background to the need for System Integrity (SysI) Management and additional guidance material, amplifying what is included in RA 5721. It also highlights the relationship between RA 5721 and other areas of the Military Aviation Authority Regulatory Publications (MRPs).

It is offered in the understanding that the MRP retains primacy and where any differences are observed between documents, compliance is expected as required by the extant regulation.

This handbook will:

a. Introduce the need for and the goals of SysI, as well as where it sits in relation to the rest of the MRP and where SysI sits in relation to the MAA.

b. Expand on the threats to SysI, how they might be manifest on a platform and how they might be countered.

c. Explain how SysI is supported by other RAs and processes, how these RAs counter the threats to SysI and are applied within Establish, Sustain, Validate, Recover, Exploit (ESVRE) principals.

Suggestions for improvement may be sent by e-mail to:

MAA-Cert-ES1-Group@mod.uk

Or by post to:

MAA Certification Electronic Systems Team

Military Aviation Authority

Neighbourhood 5

Juniper, Level 1, Wing 4

#5104

MOD Abbey Wood North

BS34 8QW

Table of Contents

List of Figures

List of Tables

DEFINITIONS

1. MAA 02: - MAA Master Glossary, should be the primary point of reference for abbreviations and definitions of common terminology however the information below provides a ready reference for definitions and abbreviations used in this Handbook.

System

2. MAA 02 gives the definition of System as:

> *"A combination of physical components, procedures and human resources organised to achieve a function."*

3. This definition meets the requirements for System Integrity (SysI) Management and identifies that management of SysI is an organizational activity relating to the physical components of an aircraft.

4. In addition to the definition in MAA 02, RA 5721 also defines a system as:

> *"A set of connected devices and interconnecting elements, encompassing hardware, firmware and software that, when functioning correctly, results in a desired outcome. This includes all avionic and mechanical systems, including actuating and dynamic components; it specifically excludes aircraft structure, structural attachment fittings and core Engine Change Unit (ECU)."*

5. This definition is limited to defining the aircraft systems in physical terms, for Integrity Management. It also states that the devices are connected and that the interconnecting elements of a systems are worthy of consideration in their own right. The definition also highlights that System Integrity Management has boundaries with other areas of Integrity Management. These boundaries need to be defined and managed to ensure that no aspects of the aircraft's design are left unmanaged.

6. The RA 5721 definition of a system relates directly to the definition of System Integrity.

System Integrity

7. RA 5721 and MAA 02 gives the definition of SysI as:

> *"The ability of an aircraft system, designed, certified and maintained to defined standards, to retain, at an appropriate level of safety, its function, within defined limits and without undue frequency of failure or adverse effect on other systems, throughout the aircraft's service life while operating to the Aircraft Document Set."*

8. The crux of the definition is "The ability of an aircraft system to retain its function throughout the aircraft's service life". Incorporated into the definition are constraints against which System Integrity has to be assessed in order to demonstrate that the aim of System Integrity Management has been satisfied.

List of Abbreviations

AAA	Ageing Aircraft Audit
AAMC	Acceptable Alternative Means of Compliance
AAR	Air-to-Air Refuelling
AD	Accidental Damage
ADS	Aircraft Document Set
AEDIT	Aircraft Engineering, Development & Investigation Team
ALARP	As Low as Reasonably Practicable
AMG	Airworthiness Management Group
AOA	Aircraft Operating Authority
CAA	Civil Aviation Authority
CADMID	Concept, Assessment, Demonstration, Manufacture, In-Service, Disposal
CAMO	Continuing Airworthiness Management Organizations
CC	Configuration Control
CoD	Certificate of Design
DAOS	Design Approved Organization Scheme
DASOR	Defence Air Safety Occurrence Report
DAT	DE&S Airworthiness Team
DH	Duty Holder
DLOD	Defence Lines of Development
DMA	Data Management Agency
DO	Design Organisation
DRACAS	Data Reporting Analysis and Corrective Action System
ED	Environmental Deterioration
ESVRE	Establish, Sustain, Validate, Recover, Exploit
EWIS	Electrical Wiring Interconnect System
FLC	Front Line Command
FMECA	Failure Modes Effects Criticality Analysis

FRACAS	Failure Reporting, Analysis and Corrective Action System
FSI	Functionally Significant Item
HF	Human Factors
IBA	Internal Business Agreement
LEP	Life Extension Plan
LoAA	Letter of Airworthiness Authority
LoD	Letter of Delegation
MAA	Military Aviation Authority
MDs	Maintenance Data System
MOD	Ministry of Defence
MRP	Military Aviation Authority Regulatory Publications
MSG3	Maintenance Steering Group 3
OEM	Original Equipment Manufacturer
OSD	Out of Service Date
PIWG	Propulsion Integrity Working Group
PSP	Project Safety Panel
PT	Project Team
PTL	Project Team Leader
RA	Regulatory Article
RAF	Royal Air Force
RCM	Reliability Centred Maintenance
RN	Royal Navy
RTS	Release to Service
RTSA	Release To Service Authority
SEMP	Safety and Environmental Management Panel
SIWG	Structural Integrity Working Group
SLA	Service Level Agreement
SME	Subject Matter Expert
SOI	Statement of Operating Intent
SOIU	Statement of Operating Intent and Usage

SPC	Sortie Profile Code
SQEP	Suitably Qualified and Experienced Personnel
SysARCS	System Airworthiness Regulatory Compliance Scorecard
SysCC	System Configuration Control
SysI	System Integrity
SysIWG	System Integrity Working Group
TAA	Type Airworthiness Authority
TI	Technical Information
TLMP	Through Life Management Plan

SECTION 1 – SYSTEM INTEGRITY BACKGROUND

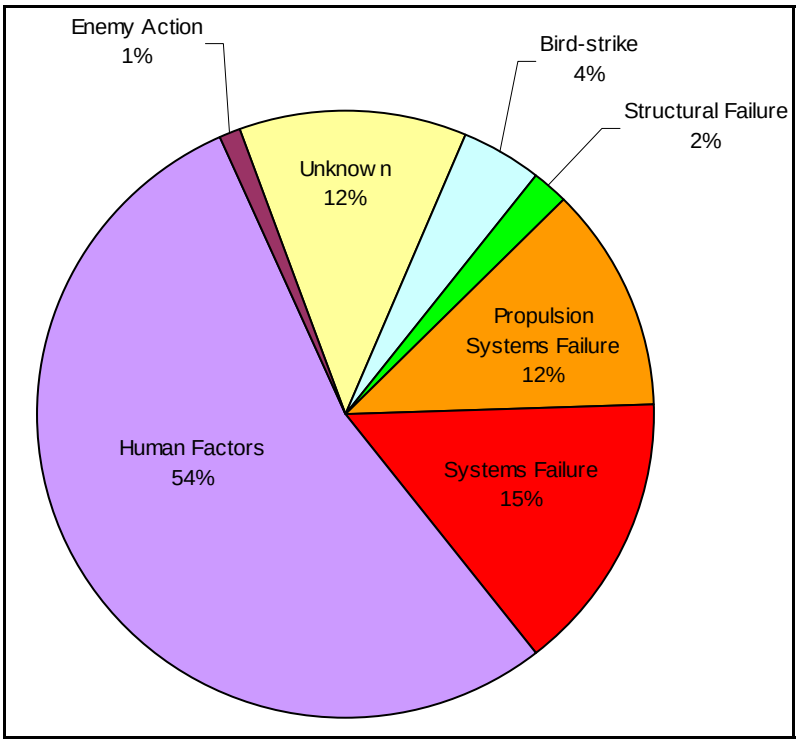
1.1 - The Need for System Integrity

1. During the pioneering days of powered flight early aircraft were, by their nature, very simple with little in the way of what we would today describe as a system. Historically, it was structural failure that was often the root cause of aircraft related accidents and incidents. However, as aircraft grew increasingly complex and the underlying aerodynamic characteristics became better understood, more emphasis was placed upon the systems incorporated into the design of the aircraft. Indeed, modern combat aircraft are successfully and consistently designed to withstand incredible loads, often only restricted by the human element of the system. Conversely systems have been developing at ever increasing rates with platform capability becoming ever more dependent upon the safer operation and interoperability of complex systems. Therefore, given the proliferation of on-board systems and through analysis of Air Incident Reports and other data, it has been determined that systems failures are responsible for far more accidents/incidents, missed sorties and unserviceable aircraft than structure or propulsion systems.

2. Modern aircraft, such as the Typhoon, are built aerodynamically unstable to improve combat capability, requiring many systems to enable them to fly. This places a large emphasis on the continuing reliability of the on-board systems, since failure could result in loss of aircraft and crew. Moreover, integrated systems are becoming increasingly complex, which further increases the potential for a system to fail. Therefore, the subject of Systems Integrity and the potentially catastrophic consequences associated with it should not be underestimated.

3. The extent of systems failures is illustrated in Figure 1, which shows the causal factors of UK military aircraft accidents from 1979 to 2007. As you will see from this, the majority of aircraft accidents over this period have been attributed to Human Factors errors. However, approximately 15% were as a consequence of a systems failure. This figure may actually be higher since the cause of 12% of the accidents remains unknown owing to insufficient evidence being available during the accident investigation. By contrast, a structural failure caused only 2%. Therefore, the probability of a systems failure causing an accident is over seven times greater than that for a structural failure. Since all platform PTs have recognised the importance of Structural Integrity by the inclusion of a Structural Plan, Structural Integrity Working Group and Strategy Document within their TLMPs, it follows that SysI must also be considered as a through-life activity given the potential consequences associated with it.

Figure 1 - Breakdown of Military Aircraft Accidents (1979 – 2007)



1.2 - Impact of Loss of Systems Integrity

4. There is an obvious cost in terms of lives and aircraft lost in accidents. However, the cost of putting things right even when there hasn't been an accident is also very high. A number of high profile civil and military accidents have highlighted the potential impact systems failure can have, and serves to demonstrate why SysI is so important.

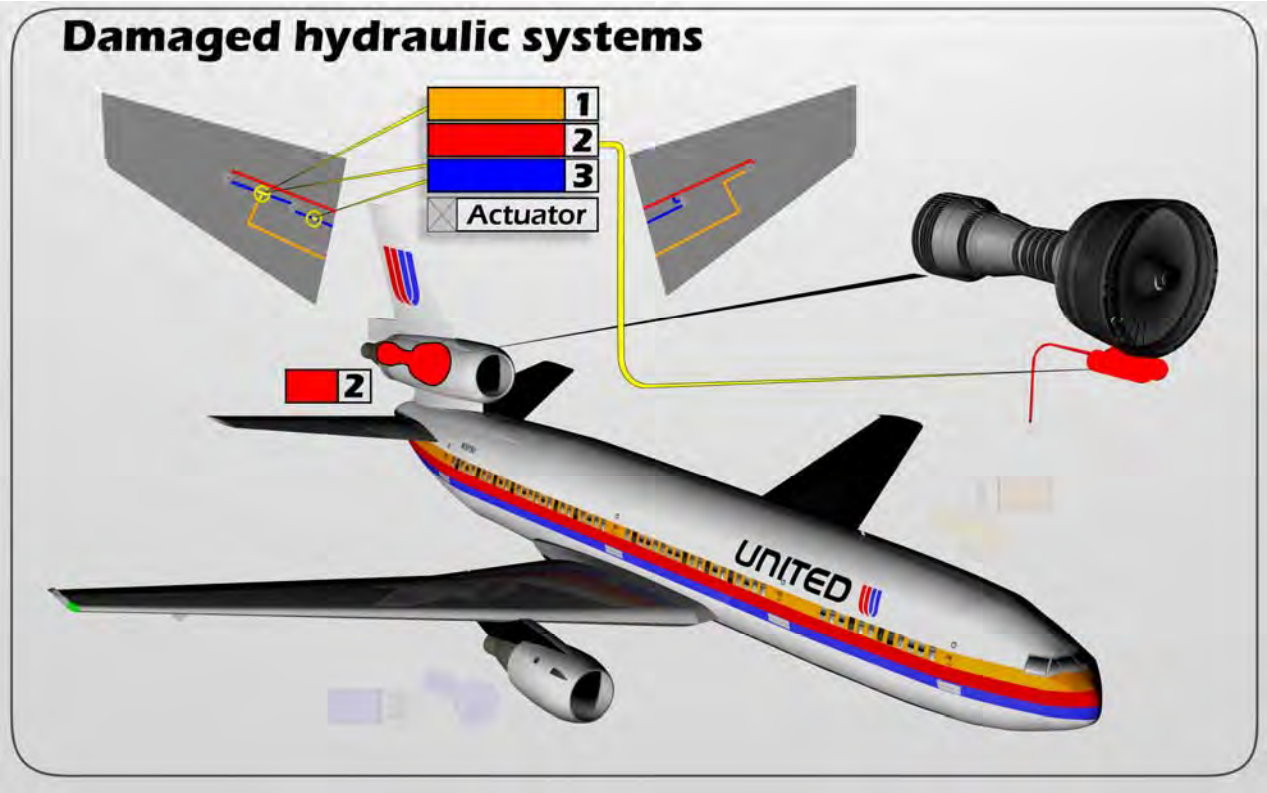
5. Between 1997 and 2006 there were at least seven military occurrences that have been attributed to a systems failure and have resulted in either the loss of the aircraft and either major or minor injuries to the operator, shown in Table 1 - High Profile Military Air Accidents .

Table 1 - High Profile Military Air Accidents

Year	Type	Details
1997	Bulldog	Float detached
1997	Harrier	Dry soldered joint
1998	Hawk	Loose battery causing aileron jam
1999	Jaguar	Hydraulic pipes cross-connected leading to hydraulic fluid leak
2002	Tornado	Faulty fuel coupling leading to a fire
2004	Tornado	Dislodged locking pin – loose article
2006	Nimrod	Fuel seal failure, fuel leak, fire, explosion

6. Civilian operators have also learnt the hard way the importance of systems integrity, illustrated by the loss of United Airlines flight 232 in 1989 where the Douglas DC-10 suffered an uncontained failure of its number 2 engine which destroyed all three of the aircraft's hydraulic systems, Figure 2. With no controls working except the thrust levers of the two remaining engines, the aircraft broke up during an emergency landing on the runway at Sioux City, Iowa, killing 110 of its 285 passengers and one of the 11 crew members. The disaster is famous within the aviation community as a textbook example of successful Crew Resource Management, due to the effective use of all the resources available aboard the plane for help during the emergency.

Figure 2 - UA flight 232 Hydraulic System Damage



7. Investigation attributed the cause of the fracture of the fan disk to a failure of United Airlines maintenance processes to detect an existing fatigue crack. Post-crash analysis of the crack surfaces showed the presence of the penetrating fluorescent dye used to detect cracks during maintenance, indicating that the crack was present and should have been detected at a prior inspection. The detection failure arose from poor attention to human factors in United Airlines' specification of maintenance processes. The investigation also revealed several other fan disks already in service from the same batch of ingots which had started to exhibit the initial cracking symptoms of part failure.

8. The odds of all three hydraulic systems failing simultaneously had previously been calculated as high as $1*10^{-9}$. Yet, in 1981, and eight years before the Sioux City crash, an Eastern Airlines L-1011 (also a 3-engine airliner) suffered a similar kind of massive failure of its number two engine. The shrapnel from that engine inflicted damage on all four of its hydraulic systems, which were also close together in the tail structure. However, fluid was lost in only 3 of the 4 systems. While the fourth hydraulic system was impacted with shrapnel too, it was not punctured. The hydraulic pressure remaining in that fourth system

enabled the captain to land the plane safely with some limited use of the outboard spoilers, the inboard ailerons and the horizontal stabilizer, plus differential engine power of the remaining two engines.

9. These occurrences highlighted the fact that the initial assumptions over probability of failure were wrong. Had timely SysI Management procedures been put in place after the Eastern Airlines flight then 111 people may not have lost their lives at Sioux City. As a consequence of the Sioux City accident, newer aircraft designs such as the MD-11 have incorporated hydraulic fuses to isolate a punctured section and prevent a total loss of hydraulic fluid; this was also partially implemented on DC-10 models after the accident.

1.3 - The MAA – The Regulator

10. Part of the Ministry of Defence (MOD), the MAA is an independent and autonomous organization responsible for the regulation, surveillance, inspection and assurance of the Defence Air Operating and Technical domains. It ensures the safe design and use of military air systems.

11. The MAA was established in response to the recommendations made by Mr Justice Haddon-Cave in his Nimrod Review, which called for a radical overhaul of military airworthiness regulation.

12. As the single regulatory authority responsible for regulating all aspects of Air Safety across Defence, the MAA has full oversight of all Defence aviation activity. Through independent audit and continuous surveillance of military aviation, the MAA aims to provide the Secretary of State (SofS) for Defence, through the Permanent Under Secretary (PUS) of State for Defence, the necessary assurance that appropriate standards of Air Safety are maintained in delivering operational capability.

13. The MAA draws the authority to discharge its regulatory role from a Charter signed by SofS. The Charter also specifies the MAA's high level governance arrangements and broad responsibilities.

14. The MAA, which is located at MOD Abbey Wood (North), Bristol, is led by a 3* Director General (DG) who is based in Level 6, Zone L, MOD Main Building, Whitehall, London, SW1A 2HB.

15. DG MAA is supported by two 2*s, Director (Operations) and Director (Technical), who collectively form the MAA Executive.

16. The organization consists of a number of key areas:

a. Regulatory Services Delivery Groups deliver end-to-end Regulations and Certification, and Oversight and Approvals across the Defence Air Environment.

b. A Strategy and Policy Group develops and sets MAA policy and conducts strategic planning with a 5 year horizon.

c. A centralised Analysis and Planning Group uses evidence to develop and resource a risk-based, operational delivery plan, which is informed by a number of activities such as audits and inspections.

d. The Enabling Services function provides a range of support services to the MAA. It comprises a number of smaller, interlinked teams: Business Plans and Finance; Secretariat and Communications; Legal Services; and Skills, Training and Talent Sustainment (who support the governance and outputs of the MAA).

e. The Military Air Accident Investigation Branch (MilAAIB), based in Farnborough, undertakes military air accident investigations in support of Service Inquiries convened by the DG.

f. Of particular importance to SysI management are the MAA Certification Electronic Systems (MAA Cert ES) and Mechanical & Propulsion Systems (MAA Cert MPS) Teams. Their role is to:

i. Carry out certification of: new aircraft on the military register; major changes to aircraft on the military register; and UORs, as required by MAA RA 1500.

ii. Develop System Integrity regulation under RA 5721.

iii. Support Project Team's System Integrity activities through the System Integrity Working Groups.

iv. Provide advice and guidance to PTs on airworthiness regulation.

v. Provide assurance to the Airworthiness Management Groups on matters relating to System Integrity.

vi. Support the development of Ageing Aircraft Audit regulation and Life Extension Programme regulations.

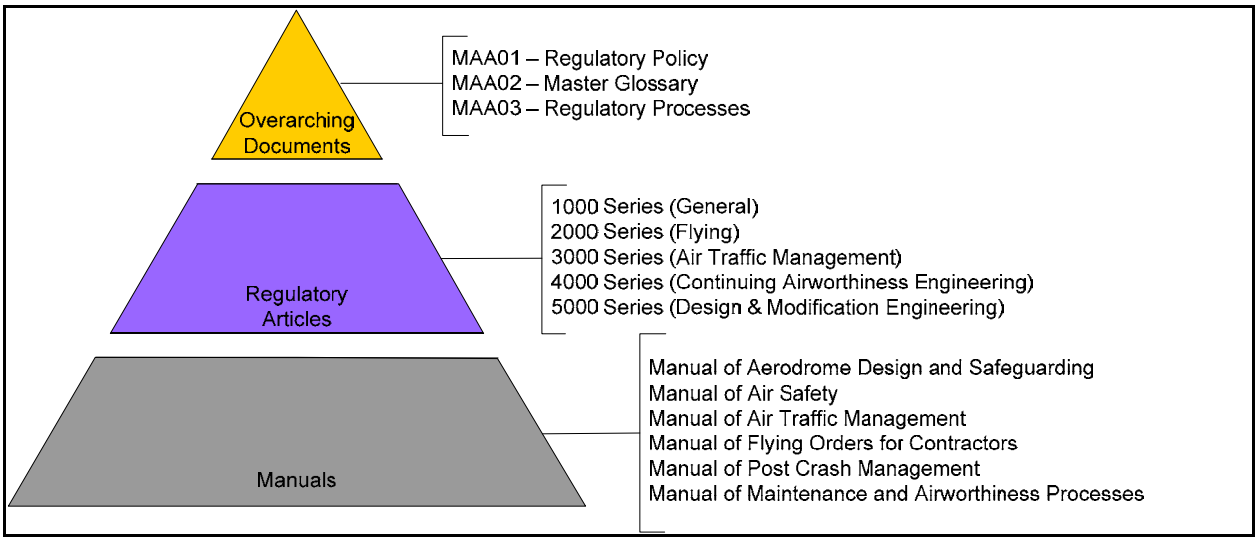
1.4 - The MRP – The Regulations

17. The overarching document, MAA 01 – Regulatory Policy, states that:

> *"The Regulatory Articles within the MRP (also referred to as the Regulations) are Orders within the meaning of the Armed Forces Act".*

18. With the exception of Queen's Regulations and MAA Regulatory Notifications, the MRP has primacy over all other military aviation orders or instructions. The MAA Regulatory Framework is represented in Figure 3:

Figure 3 - MAA Regulatory Framework



1.5 - RA 5721 – System Integrity Management

19. RA 5721, System Integrity Management forms part of the 5000 series regulations, Design and Modification Engineering, of the MRP. It provides regulation for SysI and the management of SysI, which are Type Airworthiness Authority responsibilities, as defined in RA 1015. RA 1015 – Type Airworthiness Authority (TAA) – Airworthiness Responsibilities, states:

> *"The TAA shall be responsible for the Type Airworthiness of an air system throughout its life from development to disposal."*

20. To satisfy the AMC for RA 1015, the guidance material states:

> *"The TAA is responsible for maintaining the Structural, Propulsion and Systems Integrity of the platform type through life including regular review of the actual usage and in-service experience against the design assumptions."*

21. RA 5721 provides the regulation for the management of SysI. The regulation comprises 5 aspects: Establish, Sustain, Validate, Recover and Exploit (ESVRE). RA 5721(1) – System Integrity Management, states:

> *"The Type Airworthiness Authority (TAA) shall be responsible for System Integrity Management, for all aircraft within their area of responsibility, to ensure an acceptable and demonstrable level of System Integrity."*

22. SysI is a physical attribute of a system. Systems are developed and supported by processes and organizations, both civil and military, across all Defence Lines of Development (DLOD). The threats to SysI are physical, process driven and organizational; they are pan-DLOD and are present throughout the CADMID cycle. Countering the threats to SysI is a whole-life, pan-DLOD activity, which encompasses aspects of type design assurance and continuing airworthiness. SysI Management is dependant on the effective application of the 1000, 4000 and 5000 series MRPs.

1.5.1 - System Integrity – Introduction

23. RA5721 highlights the threats to SysI, which fall into nine distinct categories, given as: ageing components, change of usage, procedural error, fatigue, overload, accidental damage / environmental deterioration, lack of configuration control, obsolescence, legislation change, or any number of the threats working in combination.

24. Unless managed any of the listed threats can break down the defence barriers and eventually lead to an incident or accident. Furthermore, the presence concurrently of more than one threat will serve to exacerbate the situation and introduce added complication. SysI Management uses the ESVRE approach to IM which is a common approach across Systems, Structures and Propulsion systems.

1.5.2 - System Integrity Management – Rationale

25. The rationale for SysI Management is given in RA 5721 as:

> *"The aim of System Integrity Management is to counter the threats to System Integrity throughout the life of the aircraft or system, across organisational, process and responsibility boundaries; ensuring risks to airworthiness are Tolerable and As Low As Reasonable Practicable (ALARP). System Integrity Management requires a planned programme of measures."*

26. This stated aim for SysI intimates that SysI Management is carried out in a complex environment of technical, organizational and social contexts which may result in emergent system properties that are difficult to predict but which may threaten System Integrity. This complexity requires that the root causes of the threats are addressed and this requires management across technical and organizational boundaries by a broad stakeholder community.

27. Successful implementation of SysI Management is dependant on the appropriate application of other areas of the MRP and consideration of the interactions between these items of regulation and their outputs and effects.

28. Aircraft systems are usually designed using failsafe design techniques. Functionally Significant Items (FSI) are identified during design and where preventative maintenance is appropriate will be included in the maintenance schedule using Maintenance Steering Group 3 (MSG3) logic. FSIs with a critical failure mode should be identified to the Project Team by the Design Organization (DO) as critical components and will be candidates for lifing. Ongoing maintenance schedule reviews, using RCM analysis will validate design assumptions and change the scheduled maintenance appropriately. For system elements where preventative maintenance is not appropriate, fault trending, Failure Reporting Analysis and Corrective Action System / Data Reporting Analysis and Corrective Action System (FRACAS/DRACAS) and other occurrence reporting will help validate the design assumptions.

29. Aircraft and aircraft systems should be designed to appropriate specifications and standards. For aircraft and system integration the MOD's certification specification for design and airworthiness is Def Stan 00-970. For individual systems there are a variety of standards that can be applied. All standards and specifications should be identified and agreed by the PT as they will form the Type Certification Basis (TCB) for the aircraft or

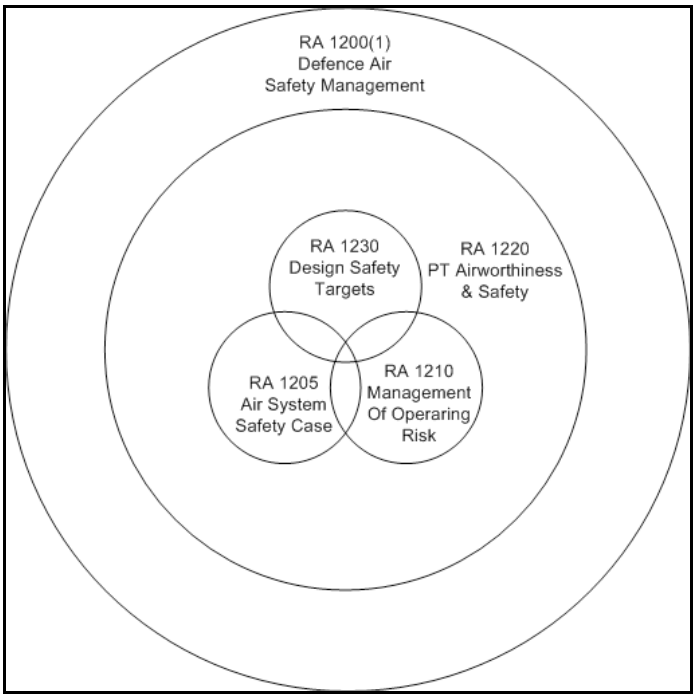
system. Any intention to deviate from Def Stan 00-970 should be agreed with the MAA. System design should also be carried out by approved organizations, operating within the scope of their approval.

30. Certification of new aircraft and Major modifications will be assured by the MAA, against the TCB. Regulation for certification is contained within RA 1500. Changes to the air system that are not classified as Major will still be required to follow the process as outlined within RA 1500 but will not be subject to MAA assurance. All other elements of the MRP apply to changes to type design and contribute to Continued Airworthiness and as such fall within the overall responsibilities of the TAA.

31. As part of the design process, approved data should be used in the development of the Aircraft Document Set (ADS), which has a prime airworthiness function for the aircraft type. The ADS will be managed, updated and controlled throughout the service life of the platform through the activities of a variety of organizations in accordance with regulations and processes. Included as part of the ADS will be the technical publications to which the aircraft will be maintained. This maintenance activity will also be supported by a number of Policy documents. Maintenance will also depend on training and the application of skills by suitably qualified and experienced personnel, in accordance with approved standards.

32. As part of the PTs Airworthiness Strategy (RA 1220(1)), SysI should be managed within an acceptable Air Safety Management System (RA 1200). Systems will be designed with cognisance of the Design Safety Target (RA 1230). Throughout the air-systems life the design safety target must be maintained and the associated RtL managed to at least Tolerable and ALARP. The relationship between the Design Safety Target and some other areas of regulation is shown in Figure 4.

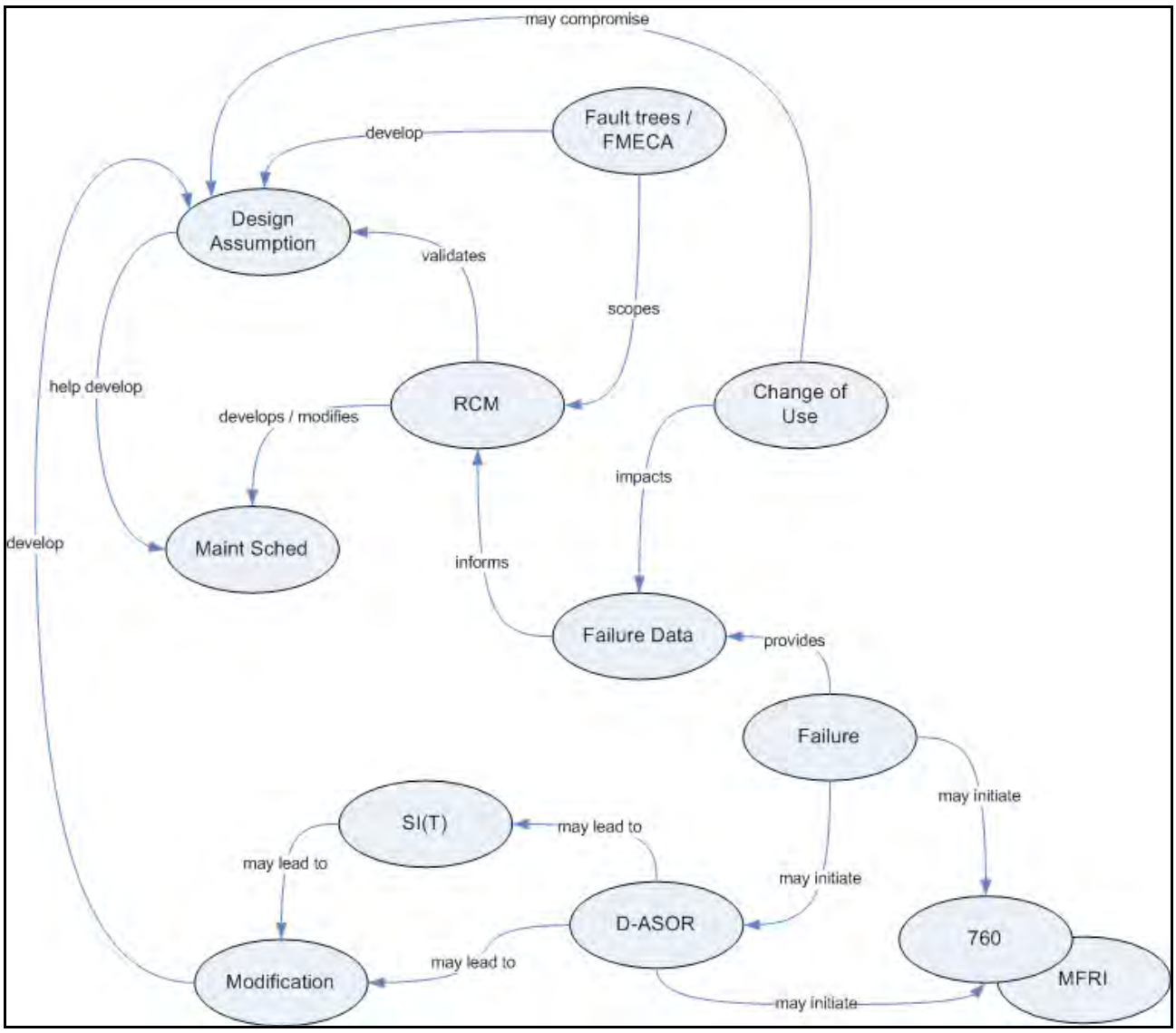
Figure 4 - Defence Air Safety Management



33. Certification evidence, generated through validation and verification activities, will ensure the systems meet the functional requirements for design and that the systems operate within the defined design limits. Once in-service, the defined limits for aircraft systems, as expressed in the ADS, will be verified by testing systems to the ADS. A system's failure to retain its function within defined limits might indicate a system fault to be rectified as part of normal maintenance. It may also indicate the impact of one of the threats to System Integrity and require deeper investigation. A diagram of the interactions to validate design assumptions is shown at Figure 5.

34. When an aircraft or system is designed there are a number of design assumptions made. Amongst these assumptions are the reliability predictions for the parts that make up the as designed system, which together meet a system level probability of failure. For catastrophic hazards this must meet the technical system safety target. Data exploitation, including fault trending and analysis as part of a wider FRACAS programme is essential to validate design assumptions against undue frequency of failure.

Figure 5 - Validating Design Assumptions



35. All systems should be designed so that there is no adverse effect on any other systems even during failure modes. Zonal Hazard Analysis and consideration of common cause failures will validate the design for potential undesirable system interactions based on system composition within a zone and/ or adjacent zone. Zonal Inspections, identified during Reliability Centred Maintenance (RCM) analysis and carried out as part of scheduled maintenance, may also indicate zonal effects that may be compromising SysI.

36. The ADS contains the documents that have prime airworthiness function for each air system type and it is essential that detail from the Release to Service (RTS) is carried forward into supporting aircrew and engineering publications.

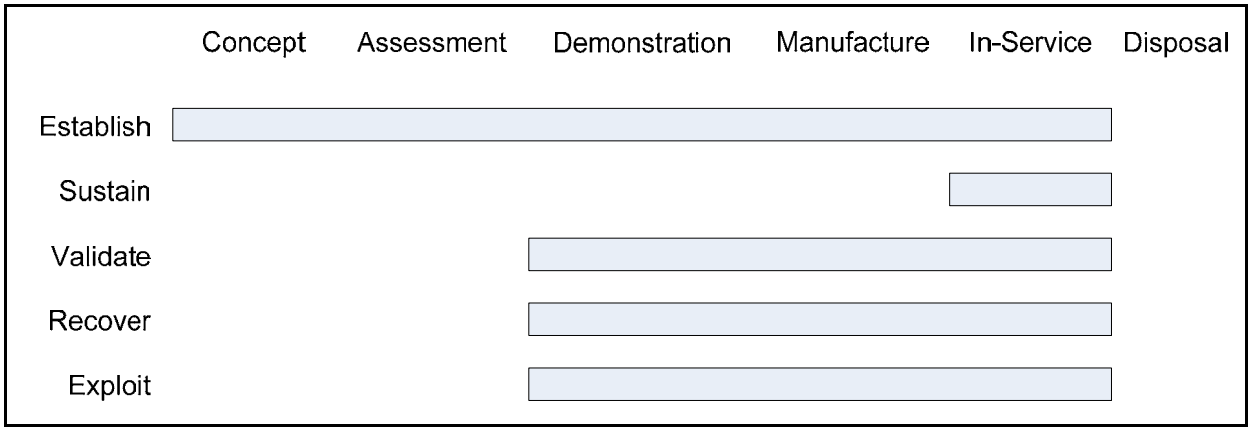
1.6 - System Integrity Regulation (RA5721) and the ESVRE Framework

37. RA 5721 comprises six sub-regulations covering the ESVRE approach to SysI Management. This common approach is applied by Systems, Structural and Propulsion Integrity Management regulations, giving a consistent approach to Integrity Management across all disciplines.

38. In many respects, the ESVRE approach to SysI should not introduce anything fundamentally different from the established processes and practices already being adhered to. However, what it does introduce is a formalised management process in which SysI issues can be identified and managed accordingly.

39. The ESVRE framework is applied until the Disposal phase of the CADMID cycle but does not mirror the CADMID cycle, as shown in Figure 6. It is a repetitive, cyclical framework shown by the application of Establishing activity throughout all parts of the CADMID cycle.

Figure 6 - ESVRE Within CADMID



1.7 - Threats to System Integrity

40. The threats to SysI must be countered throughout the life of the aircraft, over all phases of the CADMID cycle. The threats to SysI are physical, process driven and organizational; they are also pan DLOD and are present throughout the CADMID cycle. Countering the threats to SysI is also therefore whole life, pan DLOD activity. Threats to System Integrity are given as:

a. Ageing components.

b. Change of usage.

c. Fatigue.

d. Overload.

e. Lack of configuration control. Accidental Damage (AD) / Environmental Deterioration (ED).

f. Procedural (design and manufacturing, maintenance or supply) error.

g. Obsolescence.

h. Legislation change.

i. A combination of two or more of the threats.

41. There may be simultaneous threats to SysI further increasing the risk and complicating the management of SysI.

1.7.1 - Ageing Components

42. Over time, components are subject to degradation, which ultimately impacts on their ability to perform their required function. Such degradation may manifest itself as either avionic or mechanical wear.

43. Avionic wear is the undesired cumulative degradation caused by electronic components drifting outside their specified tolerance due to usage, age and AD/ED. This degradation is often gradual in nature and therefore difficult to identify in its early stages.

44. Mechanical wear is the undesired cumulative change in dimensions brought about by the gradual removal of discrete particles from contacting surfaces in motion, usually sliding, predominantly as a result of mechanical action. Wear is not a single process but a number of different processes that can take place independently or in combination, resulting in material removal from contacting surfaces through a complex combination of local shearing, ploughing, gouging, welding, tearing or other actions. The consequence of this may be the lack of load-carrying ability of the material, play in moving components, or the inability to complete the expected movement cycle.

1.7.2 - Countering the Threat of Ageing Components

45. The ageing threat to SysI is countered by the application of a number of processes which are applied at various stages of the air system’s life to validate the design assumptions and as part of continuing airworthiness:

a. Preventative Maintenance. The application of preventive maintenance ensures that the systems, where preventative maintenance is appropriate, are maintained in a manner that supports the design life of the system components.

b. Schedule Maintenance Reviews. The RCM analysis associated with maintenance schedule reviews validates system design assumptions and provides the opportunity to adjust preventative maintenance periods in response to system failure rates.

c. Fault Trending. Fault trending may indicate an increase in the failure rates of system elements. This increasing trend may indicate that the threat from ageing is having an effect which requires recovery action. The presence of changing environmental factors, in conjunction with the passage of time, is often responsible for the ageing of components and this may be identified by fault trending. This would then indicate the need for recovery action, but might also indicate a change of use that has not been identified and which may compromise one or more design assumptions.

d. Sampling. Sampling is a physical check of system elements which verifies that they continue to perform to the design specification. Sampling tests a proportion of the population of a system element, with a view to extrapolating the results to the whole population. Sampling should be carried out once a system has gained enough usage for any degradation in performance to be measurable. Sampling can be carried out using the following 3 approaches:

i. **Planned sampling**. Planned sampling may be carried out concurrently with scheduled maintenance, where the penalty of equipment removal, refit and testing is mitigated by the requirements of scheduled maintenance activity.

ii. **Opportunity sampling**. There are 2 types of opportunity sampling: off and on aircraft.

(1) Off aircraft: where equipment is returned to Depth for maintenance, sampling may be carried out. Some items of equipment have periodic bay maintenance or repair, giving an opportunity to gain information.

(2) On aircraft: when normally inaccessible equipment is exposed by other maintenance activities such as modification programmes or extensive repairs, the access can be exploited for sampling.

iii. **Teardown sampling**. System teardown is a progressive, detailed, controlled and destructive examination of elements of an aircraft system. Teardown is normally carried out on a service aircraft that has reached the end of its useful life. Preserving evidence is key to the validity of any data gathered, therefore careful planning of any teardown activity is essential in order to maximise the benefit.

46. **Ageing Aircraft Audit (AAA) (RA 5723)**. The systems' elements of an AAA provide assurance that the SysI hence the airworthiness risks of a fleet's aircraft are being managed appropriately from the perspective of ageing. It is a periodic, independent assessment of the effectiveness and applicability of procedures, management processes, technical information and documentation, established to assure a fleet's systems' airworthiness is maintained throughout its life. It is conducted to give confidence that airworthiness risks are at least tolerable and As Low As Reasonably Possible (ALARP), as the fleet ages and regulatory requirements evolve.

47. Ageing Aircraft Audits are carried out at mid life of the aircraft or the 15 year point, whichever is earliest, and then every 10 years subsequently. As part of the AAA a condition survey should be carried out. This should give an indication of how system elements, identified as being within scope for the survey, are ageing. It should also

identify any ongoing recovery work that should be carried out and give the PT an indication of whether the system elements are likely to meet their required life.

48. An AAA also reviews the physical condition of the aircraft, to ensure it is consistent with the management processes that have been applied to it, rationalising the as-designed, as-maintained and as-flown conditions for the aircraft against the requirements of the ADS.

49. These AAA activities give an indication of how well the aircraft has been managed through its life and what impact long term exposure to the threats to SysI is having on the air system and its processes. Analysis of AAA reports may also give an early indication of any system or adverse process interactions that may be at play.

1.7.3 - Change of Usage

50. Any change in use of a platform or system may affect SysI. These changes may include the following:

a. Adding new functionality or using a system's capability differently (noting that modifying or upgrading systems, including hardware, firmware or software changes, may affect another system's integrity).

b. Change of sortie profiles.

c. Differing environments.

d. Increased loads.

e. New working practices or changes to maintenance regimes.

51. The introduction of system usage within a phase of flight, not originally intended, may bring with it unexpected results. Also sustained use within a narrow region of the air system's flight envelope may compromise design assumptions.

52. The Statement of Operating Intent (SOI) and, once in service, the Statement of Operating Intent and Usage (SOIU) are documents that articulate to the designer how the aircraft will be or is operated; the SOIU is updated on an annual basis. This document mainly satisfies the needs of structural integrity, but there is the opportunity to expand it to cover systems usage. Documents that give information on usage from the systems perspective, that are available to the PT, are Use Studies, Concept of Use and Concept of Operation. The weakness with these documents is that there is not necessarily a requirement to update them as usage changes. Although focused on Structural Integrity, the information contained within the SOI / SOIU is still relevant to systems designers.

53. As an example, it might be the case that there is a design assumption that flights will typically be of 8 hours duration. Life of undercarriage components might be measured in landings but this measure may be converted to flying hours in a conservative manner to simplify the maintenance programme. If the average sortie length then decreases to 4 hours then this might compromise the design assumptions and doubles the number of landings that will occur between maintenance. This may mean that undercarriage components are then being used outside their anticipated design life if the change in usage and its impact are not identified and addressed.

1.7.4 - Countering the Threat Change of Usage

54. Any change of use should be considered potentially damaging to SysI until contra evidence is presented. RCM, ZHA, SOIU reviews and DO information all have their part to play in aiding the TAA to retain SysI.

1.7.5 - Fatigue

55. Fatigue is a process of progressive, permanent change occurring in a material that is subject to fluctuating loads below the static yield strength of the material. This may affect systems such as:

a. Load-bearing structures.

b. Electrical Wiring Interconnect System (EWIS).

c. Pipework and hoses.

d. Mechanical control cables.

56. In the extreme, fatigue can destroy SysI, which may impact the airworthiness of an air system. Therefore consideration needs to be given to fatigue as a threat to SysI.

57. The impact of fatigue may be exacerbated by environmental factors, ageing and accidental damage, particularly where there is a presumption that the system elements are fitted for the life of the aircraft.

1.7.6 - Overload

58. Overload may occur in any mechanical or avionic system when an item or system exceeds one or more of its designed parameters. The consequence of overload may result in the deformation or degradation of an item or system; these overload effects may be temporary or permanent. Therefore overload must be considered a threat to SysI.

59. For electrical systems the overload may be due to external influence or unintended system interaction, such as High Intensity Radiated Field or Electro-Magnetic Compatibility effects. These effects will also be influenced by environmental and other change of use threats.

1.7.7 - Lack of Configuration Control

60. Inter-system as well as intra-system Configuration Control (CC) is necessary to support the aircraft Safety Case and to inform airworthiness decision-making, which will assist in ensuring confidence in SysI. DOs may make life extension, modification and repair recommendations based on presumed configuration that does not match the as-flown configuration as a result of a lack of Sys CC. Therefore Sys CC is essential to maintaining SysI particularly for hazards resulting from interaction between systems.

61. Failure to manage the configuration of the air system, its design records and ADS can also lead to the inadvertent de-modification of aircraft or the fitting of inappropriate system components during maintenance activities.

1.7.8 - Countering the Threat of Lack of Configuration Control

62. The loss of CC is countered, for type airworthiness, by processes which are particularly relevant during the design and any subsequent modification of the aircraft. Ensuring that changes are approved correctly, resourced through procurement of items and equipment, and updating the ADS to reflect the changes are fundamental to retaining CC. This requires processes that are appropriate to the task, robust, auditable and understood by all users. If Sys CC is lost, or it is in doubt, the immediate actions should already be established and documented as part of the Configuration Control Plan. This enables the appropriate actions, whether the issuance of a Technical Instruction or other investigative or mitigation to be initiated appropriately.

1.7.9 - Accidental Damage (AD)/ Environmental Damage (ED)

63. **Accidental Damage (AD)**. AD is the physical alteration of an item caused by any unintentional influence, contact or impact on a system or component. This damage may be caused by external factors, such as the presence of debris, or spilled material. It may also be caused by human error, which can occur during manufacture, operation or maintenance of the systems but which may not constitute maintenance error. AD/ED to systems may also occur when items of equipment are not fitted to the aircraft. Battle damage or sabotage, although not strictly accidental, may also be considered within this category, as the effects are comparable.

64. **Environmental Damage (ED)**. ED is the physical degradation of material properties as a result of their interaction with the climate or localised environment. Chemical interaction, erosion, fluid/gas absorption, thermal cycling or radiations are typical causes of ED. ED may manifest itself as corrosion, loss of surface finish, including electrical insulation or softening of composite materials and other component degradation. ED is affected by the amount and duration (calendar time or equipment use) of exposure to the environmental effect, although this may not be in a predictable manner. Identification of ED in one physical location may be an indicator that the effect is occurring elsewhere, possibly in less inspectable areas of the aircraft, where the degree and duration of exposure may be different. AD and ED of system elements will occur while equipment is not in use.

65. Both AD and ED will also be affected by changes in system use and changes in geographical area of operation. AD and ED can represent common-cause failure modes, defeating fail safe design philosophies, so should be countered and addressed in a timely manner.

1.7.10 - Countering the Threat of Accidental and Environmental Damage

66. Accidental damage can be countered through the application of procedures to reduce the likelihood of inadvertent contact occurring between aircraft systems and other items of equipment. As an example, marshalling of ground equipment and the use of chocks when in the proximity of aircraft is a procedural approach to countering the threat. Accidental damage can also occur to equipment in store and transit but can be countered by application of supply procedures and the use of appropriate packaging. Occurrence reporting gives a mechanism for monitoring accidental damage.

67. Scheduled maintenance and maintenance schedule reviews, including lifing and sampling of components help counter ED. As part of this, ED can also be countered by

considering the operating environment of an aircraft. For changes in environment the application of additional preventive maintenance in periods of abnormal usage will limit the impact of environmental effects. Environmental damage can also occur while equipment is in store. This can be countered by ensuring that equipment has appropriate storage instructions and that it is stored in an appropriate environment. Anti-deterioration maintenance can be carried out on equipment that is held in store for extended periods and it is also important to manage stock holdings at a level that allows a level of stock rotation to minimise the impact of ED. This is particularly relevant during periods of fleet size reduction.

68. **AD / ED**. Zonal inspections, local procedures, training and educational campaigns are also among the measures that might be employed to counter the AD and ED threat to SysI.

1.7.11 - Procedural (Design and Manufacturing, Maintenance or Supply) Error

69. Procedural errors can be the result of design, manufacturing, maintenance or supply error.

70. **Design error.** Design error describes the result of failure to adhere to recognized design standards, design best practice and qualification evidence methodology. Examples of design error include:

a. Failure to generate sufficient evidence of material properties.

b. Potential for incorrect assembly.

c. Specifying inappropriate material and manufacturing processes.

d. Failure to design an assembly so that it can correctly perform its required functions.

e. Failure to produce error-free software.

f. Failure to take account of user requirements.

g. Failure to identify and accommodate system interactions in complex systems.

71. As well as errors in the design of the system, designers are also subject to all the problems associated with project management, quality assurance and configuration control. There is also the potential for problems to arise due to failures in communication, both internally to the DO and externally with the customers, manufacturers and other sub-contracted organizations.

72. **Manufacturing error.** Manufacturing error describes the outcome or the performance of a system or component that fails to meet the design specification. Factors leading to manufacturing error include:

a. Failure to adhere to manufacturing drawing requirements and processes, such as:

i. Use of incorrect material.

ii. Application of an incorrect process or loss of process control.

iii. Use of incorrect parts or components.

b. Use of unauthorized jigs, fixtures and tooling.

c. Incorrect routing or assembly of components, cable ducts, pipes or looms.

73. These manufacturing errors are often driven by the same things that threaten SysI and can be the result of issues arising from inadequate quality control, insufficient information from the designer on the provided drawings, use of inappropriate standards, or the failure to adhere to standards to name but a few.

74. Manufacturing error can be particularly critical as it can constitute the prime source of common mode failures, which may then defeat the designer's achievement of a safety target through the application of redundancy in the system design. Also, any manufacturing error that affects critical components can have a serious impact on the airworthiness of the aircraft.

75. **Maintenance error.** Maintenance error describes the unsatisfactory outcome or performance of a maintenance process on an aircraft system. Factors leading to maintenance errors that threaten SysI may include:

a. Inadequate instruction, training or supervision.

b. Sub-optimal resources.

c. Incorrect technical information.

d. Use of unauthorized jigs, fixtures and tooling.

e. Human factors.

76. **Supply error.** Supply error describes the supply of a component or product that does not meet the current specification and therefore does not satisfy the aircraft's airworthiness requirements. Factors leading to supply errors may include:

a. Non-conforming components, products or software.

b. Those items from an unknown pedigree.

c. Those items from unapproved suppliers.

d. Those products that are incorrectly identified and/or codified.

1.7.12 - Countering the Threat of Procedural Error

77. **Countering the threat of Design Error**. Design Error can be introduced by the PT or the DO. Design error can be countered by application of RA 1500 and by consideration of the following:

a. Defence procurement is a systems engineering discipline; it is described in detail in the Acquisition Operating Framework (AOF). From a systems engineering perspective, the development of user requirements and system requirements are part of the design process. This gives the PT the opportunity to minimise design error throughout the procurement cycle by application of the principles as discussed in the AOF. Validation and verification activities are critical in the design process and should be articulated in an agreed test and evaluation plan.

b. From a type, or continued, airworthiness perspective the TAA must agree the certification basis for the aircraft or system with the DO and the MAA. The TCB will contain the airworthiness requirements for the air system and will be carried forward into the Certification Plan, which will direct how compliance is to be demonstrated. Finally, submission of the Type Certification Exposition (TCE) will provide evidence that will support verification of the design against those airworthiness requirements as stipulated in the TCB.

c. PTs should only contract competent organizations and for DOs this competence is assessed under the Design Approved Organization Scheme (DAOS) which awards an approval for a defined range of products and services, which are articulated in the approval scope. Once the approval has been granted annual surveillance audits are carried out to ensure continued compliance. The approval via DAOS also imposes the responsibility for work carried out by any of the DO's subcontractors.

d. A Certificate of Design (CofD) is required to identify the extent to which the requirements of the specification have been achieved. It includes the following:

i. A Configuration Status Record (CSR) or equivalent drawing list appropriate to the materiel.

ii. A list of reports on all tests conducted to show compliance with the specification.

iii. A list of subsidiary certificates of design agreed by the DO for materiel designed and developed by other DOs and incorporated in the Design. For Government Furnished Articles certificates should be provided by the PTL.

iv. Specific evidence of Structural Integrity (SI).

v. A system safety case, in accordance with Def Stan 00-56 that demonstrates that the certified design is tolerably safe for the intended purpose.

e. The System Safety Argument forms part of the Air Safety Case (RA1205) and as such details all the risks and mitigations that ensure the platform remains within the tolerable and ALARP argument. This living document should be revised and amended as new, or changes to established, risks are discovered. It should also be under continuous review to ensure the risks and mitigations documented remain appropriate and effective.

78. **Countering the threat of manufacturing error**. The TAA has no direct means to counter manufacturing error. The only potential counter to manufacturing error is through the DOs subcontracts with equipment suppliers. The TAA can only identify that manufacturing errors might have occurred through analysis of fault data and equipment test. If manufacturing error is suspected F760 action is required as part of the investigation, leading to recovery action.

79. **Countering the threat of maintenance error**. Maintenance error can be countered by ensuring that: all personnel are trained to an appropriate level, they hold appropriate authorizations and that supervisory procedures are in place and are effective. To support the maintenance effort the ADS should be up-to-date, correct and appropriate for the activities carried out. The ADS should be supported by timely F765 activities, which may require the application of contracts, IBAs and SLAs with other IM stakeholders. Ensuring

that the necessary support equipment is calibrated and available to those carrying out the maintenance will help to reduce the likelihood of maintenance error, as will ensuring that only authorised tools are used. Application of human factors principles will help support maintainers by ensuring they are working in an appropriate environment and an appropriate frame of mind. The use of a maintenance error management system will give the PT an indication of where there might be a requirement for recovery action. Much can be done to minimise the risk of maintenance error though the application of design principles that incorporate simplicity as part of the design.

80. **Countering the threat of supply error**. Some TAAs now have Performance Based Logistics (PBL) or 'hole in the wall' type supply systems where input from the PT is minimal and great reliance is placed on the contract holder to procure the correct components. This requires a thorough understanding of the contract requirements before it is let and effective management during the period of contract. Others rely on MOD provided components that are procured against stated demand and IAW JSP 886. In both cases it is imperative that changes in the ADS, and therefore the requirements, are implemented in the supply chain and that there is a system of assurance that only the correct items are available.

1.7.13 - Obsolescence

81. Obsolescence, as defined in the International Standard IEC 62402:2007 is:

> *"The transition from availability from the original manufacturer to unavailability"*

and Obsolescence Management is

> *"The co-ordinated activities to direct and control an organization with regard to obsolescence".*

82. Failure to manage the obsolescence risks of equipment will impact life cycle costs, product performance, product availability, maintainability, safety and legislation. Some of the ways that failure to manage obsolescence can threaten SysI are:

a. Causing the use of alternate parts and/or suppliers.

b. Permitting parts of uncertain provenance into the supply chain.

c. Increasing aircraft cannibalisations and increasing wear in systems.

d. Forcing change in use through limited availability of capable aircraft.

1.7.14 - Countering the Threat of Obsolescence

83. JSP 886 states a mandatory requirement that "projects will implement a proactive obsolescence management strategy unless it is clearly not cost effective to do so". JSP 886, Volume 7 (Supportability Engineering), Part 8.13 (Obsolescence Management) contains the MOD policy, process and procedures for the management of obsolescence. Chief Defence Materiel mandates use of the Support Solutions Envelope (SSE) by PTs and the SSE cites JSP 886, Volume 7, Part 8.13 as underpinning policy.

1.7.15 - Legislation Change

84. Throughout the life of an air system legislation changes may impact SysI. PTs must ensure that the effects of legislation changes are addressed for their aircraft and systems. Currently, legislation changes relating to the use of materials considered to pose an environmental, or health hazard, are causing engineering challenges which have an impact on SysI. As the use of such substances is banned through legislation alternatives must be found. Any deviation in the properties of the alternative materials, from those originally required by the designer, may compromise design assumptions.

85. This threat may also generate an obsolescence threat. It may also lead to issues over Sys CC and any number of the threats associated with Procedural error. Restriction of Hazardous Substances is an example of legislation change acting as a threat to SysI via a number of other threats.

1.7.16 - Countering the Threat of Legislation Change

86. Legislation change is likely to be outside the direct control of the MOD. To counter the threat from legislation change the PT should attempt to research prospective areas of legislation change. In some cases the MOD can be exempted from changes in legislation, however these exemptions cannot be relied on, or guaranteed, to persist. Recovery action in response to legislation change will have to address the cause indirectly and may require activity in areas such as; obsolescence management, configurations control, redesign of system elements and changes to maintenance activities. Addressing the consequences of legislation change early and effectively will reduce the impact they have when the change is realised.

SECTION 2 - RA 5721 - SYSTEM INTEGRITY MANAGEMENT

2.1 - RA5721 (1): System Integrity Management

87. RA 5721(1) assigns applicability and responsibility for System Integrity and states the requirement for the threats to System Integrity to be countered:

> *"The Type Airworthiness Authority shall be responsible for System Integrity Management, for all aircraft within their area of responsibility, to ensure an acceptable and demonstrable level of System Integrity."*

2.2 - RA5721 (2): Establishing System Integrity

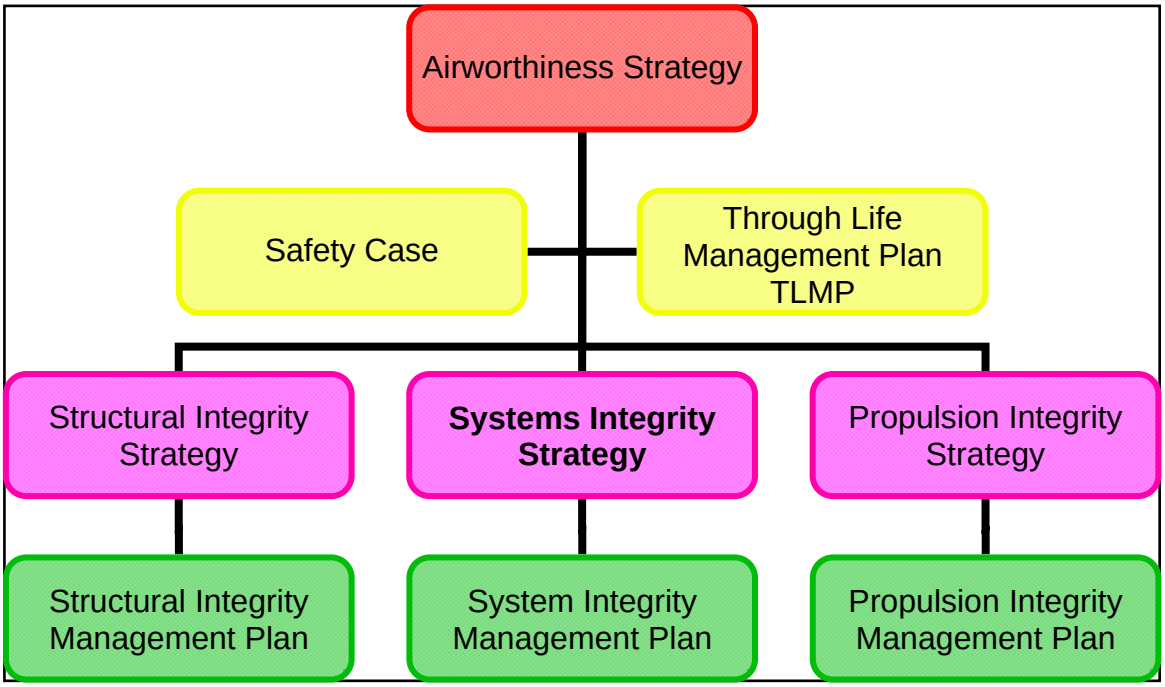
88. Furthermore RA 5721(1) outlines the establishing of SysI through the use of DO evidence, and also identifying and implementing the organizational relationships, processes, documents and meeting structure that supports SysI.

> *"The TAA shall establish System Integrity to demonstrate that the aircraft systems are airworthy to operate under agreed conditions".*

2.2.1 - System Integrity Strategy and Management Plan

89. The System Integrity Strategy Document and Plan are documents which convey to the stakeholder community the TAA's approach to and application of SysI. The documents form part of a document hierarchy as depicted in Figure 7.

Figure 7 - Integrity Document Hierarchy



2.2.2 - System Integrity Strategy Document

90. A SysI Strategy Document (Strat Doc) is a complementary document to the Through Life Management Plan (TLMP) and as such it should be produced early in the CADMID

cycle for a new platform and updated regularly as the platform moves through its lifecycle. The strategy should change in response to; the external environment, the internal environment and any changing long, and short-term, requirements for the air system's IM. The Strat Doc should be available to all SysI stakeholders so they can remain informed about the TAA's strategy, as well as giving them an opportunity for comment and input. The Strat Doc can be compiled under the following headings:

91. **Direction**. From RA 5721: "*Describe the strategic direction for System Integrity, including long-term and short-term goals*".

a. A SysI Strat Doc will be produced to convey the strategic direction for SysI, including long-term and short-term aims and objectives. As the air system life cycle progresses and changes are introduced to the TLMP there is a requirement to maintain coherence between the TLMP and the Strat Doc and it should therefore be a living document that is under 6 monthly review. The plans to satisfy the SysI objectives and progress towards meeting them should be available to all integrity stakeholders through the SysI Management Plan.

92. **Scope**. From RA 5721: '*Describe which systems fall within scope for System Integrity Management and where, in general terms, the handover occurs to other areas of Integrity Management. Also, record where areas of Integrity Management are compliant via AAMC and any waivers or exemptions'*.

a. The Strat Doc should identify the systems that are covered by the SysIWG. It should identify where there are boundaries between SysI and other areas of IM within an air system. For example the dynamic actuating components of a system may be covered under SysI but the attachment points may be covered under Structural Integrity. The Core ECU will be covered at the Propulsion Integrity Working Group, but the associated fittings and harnesses might be covered at the SysIWG. APUs are nominally part of the SysIWG, however, the TAA may choose to manage them at the Propulsion Integrity Working Group due to the distribution of suitably qualified and experienced staff from within the stakeholder community. Clearly defining these boundaries in the Strat Doc will help the PT ensure that IM is applied to the whole air system and no areas are missed.

b. Where the PT does not comply with regulation through the AMC, they may choose to record details of the AAMC that have been endorsed by the MAA. The PT may also record any waivers or exemptions they have been granted for areas where they are non-compliant, having covered their move towards compliance or alternative longer-term goals under direction.

c. The Strat Doc might also make reference to the Plan, which can be used to articulate the management of the SysI strategies' objectives, as well as for the management of routine SysI activities and supporting processes, including a timeline.

93. **Period**. From RA 5721: *'Give the milestones associated with Integrity Management, including but not limited to, OSD, LEP, capability enhancement programmes and AAA'*.

94. The Strat Doc should highlight the major milestones in an air system's life. This will help ensure that funding and other resource are in place in a timely manner.

95. **Resources.** From RA 5721: 'Identify the processes that support System Integrity and their owners'.

a. A SysI strategy should identify the processes that have been identified as supporting SysI. It should also identify who the process owners are and what arrangements are in place for continued support, be that through contract, IBA, SLA and Terms of Reference.

96. **Environment**. From RA 5721: 'Describe the organizational relationships associated with System Integrity Management. Describe the SysIWG's position and role in the meeting hierarchy'.

a. The SysIWG sits in a hierarchy of meetings and the strategy document should show the relationship between the meetings that support System Integrity.

b. A system map or organizational chart showing the organizational environment in which the PT operates, including MOD and non-MOD organizations. The map /chart should show the lines of communication between the organizations and should encompass all those organizations that support SysI Management, and those that are impacted by the activities and outputs of the SysIWG.

97. **Stakeholders**. From RA 5721: 'Identify System Integrity stakeholders'.

a. The SysI strategy should identify the stakeholders for SysI. It should identify all the key stakeholders and additional stakeholders. As part of the stakeholder community those organisations / roles that own processes that support SysI should be identified as additional stakeholders, as should those that are impacted by the activities and outputs of the SysIWG.

b. From the list of identified stakeholders, all the key stakeholders should be in attendance at the SysIWG, and the additional stakeholders as required, although some of the additional stakeholders might reasonably be expected to attend the majority of the SysI WGs.

2.2.3 - Establishing SysI Evidence

98. Establishing activities demonstrate that the aircraft is safe to operate under agreed conditions. This demonstration is achieved through the certification process for new aircraft and major modifications; the certification evidence that is generated supports the safety case argument for the Military Aircraft Release / Release to Service.

99. To ensure that an Air System's design meets appropriate safety requirements Certification is carried out in accordance with Certification of UK Military Registered Air Systems (RA 1500), which is required for both new types of military registered Air Systems and for Major changes to existing designs. Certification consists of the following 6 phases:

a. Phase 1 – Identify the requirement for, and obtain, organizational approvals.

b. Phase 2 – Establish and agree the Type Certification Basis (TCB).

c. Phase 3 – Agree the Certification Programme.

d. Phase 4 – Demonstrate compliance with the TCB.

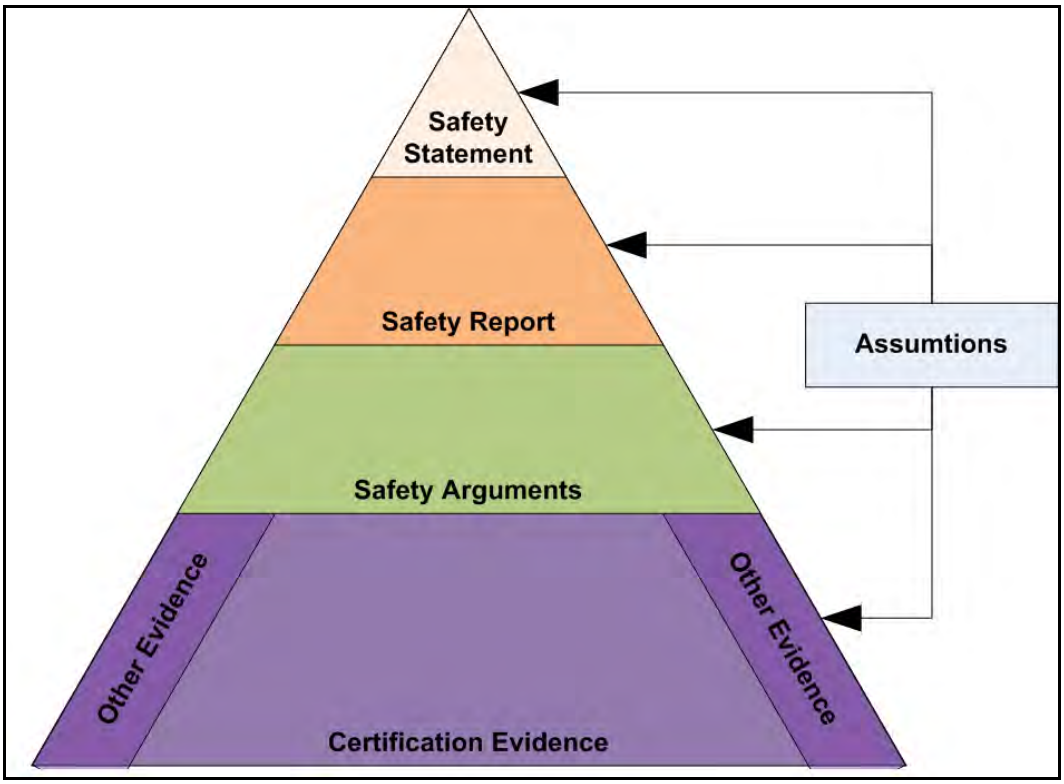
e. Phase 5 – Produce Final report and issue Certificate.

f. Phase 6 – Undertake post-Certification activities.

100. Ongoing System Integrity Management constitutes part of the Phase 6 post-Certification activity, requiring the PT to support the Certified Type design, modifications and updates of the Air System throughout its life.

101. As part of the design process, design assumptions are taken into consideration. Assumptions on usage are articulated in the SOI and also through the user requirements and other documents such as use studies, Concept of Operation and Concept of Use documents. These design assumptions must be recorded so that they can be used for later validation activities. Other design assumptions will be made by the designer at all stages of the design and should be recorded in the DO's documentation. Knowledge of the design assumptions is also of particular relevance when modifications are carried out on an aircraft, with the further complication that the modification might not be carried out by the original DO. Certification and the SysI evidence support the Safety Statement and RTS as shown in Figure 8.

Figure 8 - Certification Evidence and Assumptions



102. In addition to the certification process, the platform or system should also have a Certificate of Design, signed by the DO, which should be supported by, and have references to:

a. A configuration status record.

b. A list of reports on all tests conducted to show compliance with the specification.

c. A list of subsidiary Certificates of Design.

d. Specific evidence of systems integrity.

e. A System Safety Case, in accordance with Def Stan 00-56, demonstrating it is safe for its intended purpose.

103. For Platform, and therefore System, Integrity to be established a preventative maintenance programme with supporting evidence has to be in place before introduction of a new or modified air system. The Master Maintenance Schedule gives the maintenance requirements and activity and is an expression of some of the DO's design assumptions. The preventative maintenance programme development should be carried out using MSG3 logic during the RCM analysis.

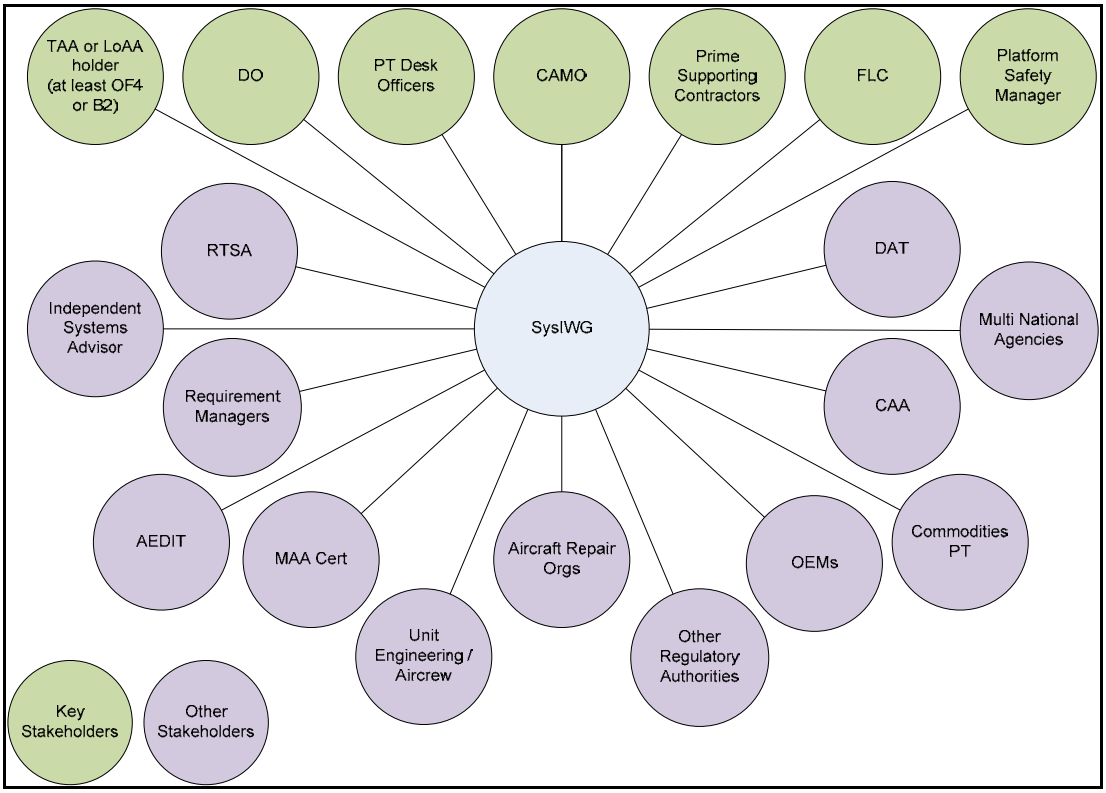
104. The system design should be based on fail-safe design principles such that no single failure should be catastrophic and that subsequent failures should be assumed. Coupled with this, the design should also meet the associated, relevant, safety targets. For example, some standards require that catastrophic failure conditions are extremely improbable, hazard failure conditions are extremely remote and major failure conditions are remote.

105. While the PT is carrying out Establishing activities the key stakeholders are Designers, Integrators, Suppliers, the Support Authority and Certification Authority.

2.2.4 - System Integrity Working Group (SysIWG)

106. The SysIWG should comprise a core membership of key and other stakeholders as shown in Figure 9 and should be held twice per year, although PTs are free to hold them more often if they feel there is benefit to the platform's Integrity.

Figure 9 - SysIWG Stakeholders



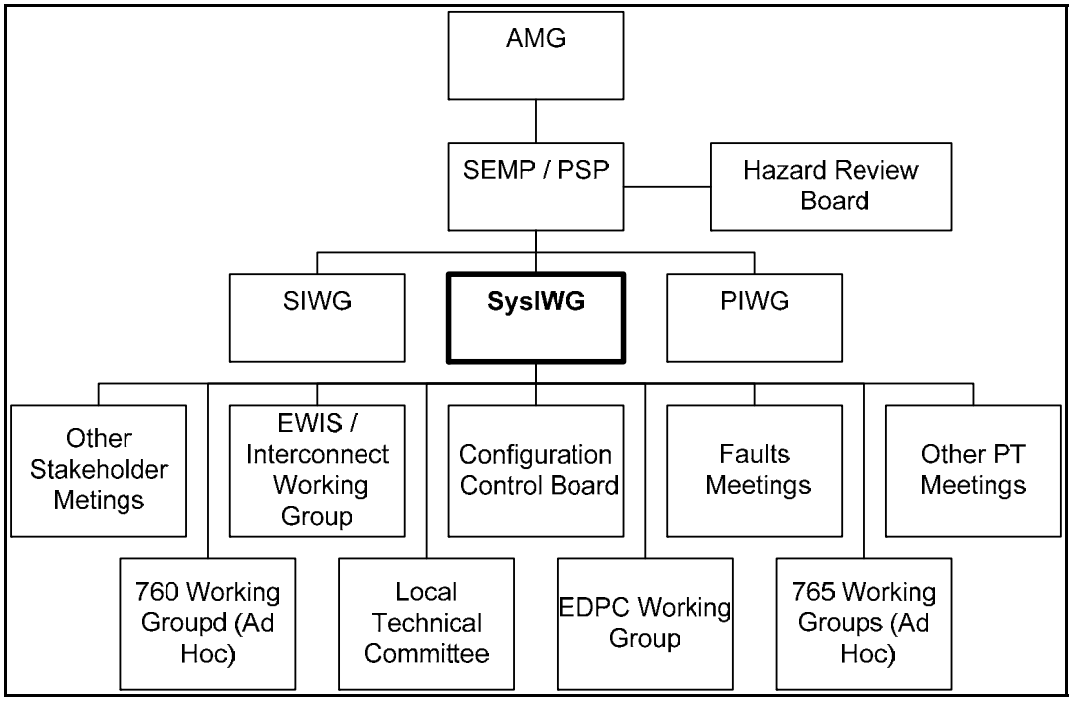
107. The SysI WG should be chaired by the TAA or the holder of a delegated LoAA (at least OF4 or B2), who is empowered to cover all systems discussed at the meeting. This

level of chairmanship is the same for all areas of IM. Set at this level it gives the OF4 / B2 a broad understanding of the IM status of the platform. Having a Chair at this level also ensures; that airworthiness decisions can be made at the meeting, without having to have them externally ratified, and that decisions that affect the whole platform can be made. It also ensures that resources can be committed should it be necessary and demonstrates to other key stakeholders the importance of SysI.

108. Because the threats to SysI operate across organizational, system and process boundaries, the SysIWG should have a broad membership base. This allows discussion of Integrity issues by all the relevant stakeholders and the development of recovery actions that address the root cause of the problem, employing engineering and process based activity. Given the range of threats that can exert an influence on SysI and the dynamic relationship between the threats, the additional stakeholder membership profile may change through the life of the air system.

109. The SysIWG should also sit in a hierarchy of airworthiness, safety and other meetings as shown in Figure 10. This is not a complete hierarchy and will depend on the PT and other Stakeholders' meeting hierarchies. Although the relationships between the meetings are shown in a hierarchy the information will flow in both directions, as will the requirement for SysI related activity.

Figure 10 - SysIWG Shown in a Meeting Hierarchy



2.2.5 - System Integrity Supporting Processes

110. As part of the Establishing SysI activities it is essential to identify and establish the processes that will support SysI throughout the life of the platform. Once the processes are identified, a process owner must also be identified. This process owner might not be part of the PT so there may need to be supporting contracts, SLAs or IBAs, depending on whether the process owner is MOD or contractor. For some of the process owners there

may be a requirement to ascertain that they hold appropriate approvals, such as DAOS and MAOS, and that they are operating within the scope of these approvals, as well as being subject to the awarding organizations audit and surveillance programme. All process owners should be considered for invitation to the SysIWG as a broad membership will support the identification of, and recovery from, Integrity issues which may be systemic and demonstrate undesirable emergent properties.

111. Some of the processes that support SysI may require the involvement of more than one stakeholder. The responsibility for, and implementation of, a process may be shared between organizations, be implemented in parallel by different organizations to meet differing requirements, or may transfer between organizations as the platform moves through the CADMID cycle. An example of this is configuration management, which impacts many of the SysI stakeholders in the same and differing contexts, to varying degrees and at various times, throughout the CADMID cycle.

112. The processes that support SysI are often the subject of RAs, Defence Standards and other regulations in their own right. The processes that support RA 5721 may include but are not limited to:

a. Implementation of strategy and plans
    i. Airworthiness Strategy
        (1) RA 1220(1) – Airworthiness Strategy
    ii. Configuration Management Plan
        (1) RA 5301 – Control of Designs
        (2) RA 5311 – Configuration Management – Project Team
    iii. Obsolescence Management Plan
        (1) JSP 886
    iv. Disposal Plan
        (1) JSP 886
b. Safety Management Systems
    i. RA 1015 - Type Airworthiness Authority (TAA) Airworthiness Responsibilities
    ii. RA 1020 – Roles and Responsibilities: Aviation Duty Holder (DH) and DH-Facing Organizations
    iii. RA 1200 – Defence Air Safety Management
    iv. MAA Manual of Air Safety
c. Certification
    i. RA 1015(1) – Type Airworthiness Management
    ii. RA 1500 – Certification of UK Military Registered Air Systems
    iii. RA 5203 – Requirement Specifications
d. Organizational approvals and monitoring

i. DAOS

(1) RA 1005 – Competent Organizations and Responsibilities

(2) RA 1014 – Design Organization - Airworthiness Responsibilities.

ii. MAOS

(1) RA 1005 – Competent Organizations and Responsibilities

iii. CAMO

(1) RA 1016 – Roles and responsibilities: Continuing Airworthiness Management Organizations (CAMOs)

e. Usage / SOI / SOIU / Use Study / CONUSE / CONOPS / CONEMP

i. RA 5720 – Structural Integrity Management

ii. JSP 886

f. Configuration management

i. 4900 Series RAs - Airworthiness Review (AR) Regulation

ii. 5300 Series RAs – Control of Design and Design Records

g. Development and maintenance of the Aircraft Document Set

i. RA 1310 – Aircraft Document Set

ii. RA 5401 – Provision of Service Technical Publications

h. Support policy

i. RA 4214 – Support Policy Statements

i. Preventative maintenance

i. RA 5320 – Aircraft Maintenance Programme – Design Guidelines

ii. RA 4200 – Maintenance Philosophy – General

iii. RA 4200(1) – Maintenance

iv. RA 4203 – Preventative Maintenance

v. RA 4351 – Production and Maintenance of Maintenance Schedules

j. Application of corrective maintenance

i. RA 4200 – Maintenance Philosophy – General

ii. RA 4200(1) – Maintenance

iii. RA 4205 – Corrective Maintenance

k. Airworthiness Directives and Special Instructions (Technical)

i. RA 1015(1) – Type Airworthiness Management

ii. RA 4457 – Special Instructions (Technical)

l. Modification process

i. 5300 Series RAs – Control of Design and Design Records

m. Fault and occurrence reporting, investigation and trending, including FRACAS

i. RA 1140 – Military Air System Technical Data Exploitation

ii. RA 1410 – Occurrence Reporting

iii. RA 4200(2) – Type Airworthiness

iv. RA 4814 – Occurrence Reporting (MRP.145.A.60)

n. Maintenance error management

i. RA 1410 – Occurrence Reporting

ii. RA 4814 – Occurrence Reporting (MRP.145.A.60)

iii. RA 4815 – Maintenance Procedures and Safety and Quality Policy (MRP.145.A.65)

o. Obsolescence management -

i. JSP 886

p. Training and authorization of personnel

i. RA 1440 – Air Safety Training Requirements

q. Ageing aircraft audit

i. RA 5723 – Ageing Aircraft Audit

r. Life extension programme

i. RA 5724 – Life Extension Programme

s. Out of Service Date Extension

i. RA 5725 - Out of Service Date Extension Programme

113. The regulatory references given in the above paragraph does not represent a full list of the regulations that must be complied with in satisfaction of process areas. The regulations highlighted are a selection of the top level applicable regulations, or regulation at a level that involves the PT.

114. SysI Management is primarily concerned with supporting Type Airworthiness and validating the design assumptions. As is obvious from the above list, some of the processes that support SysI Management are Continuing Airworthiness processes, but the application of these processes and analysis of their outputs is essential to supporting the Type Design.

115. SysI is supported by a variety of other regulations, policies, processes and procedures. These will either directly counter the threats to SysI, support SysI Management or allow SysI and the effectiveness of its management to be measured, either directly or indirectly.

116. Through application of the ESVRE framework, these supporting regulations, policies, processes and procedures should be given the following considerations:

a. Is there a policy, process or procedure in place to implement the regulation? (Establishing)(Recovering)

b. Is the policy, process or procedure in regulatory compliance, or subject to an AAMC, waiver or exemption? (Establishing)(Sustaining)(Recovering)

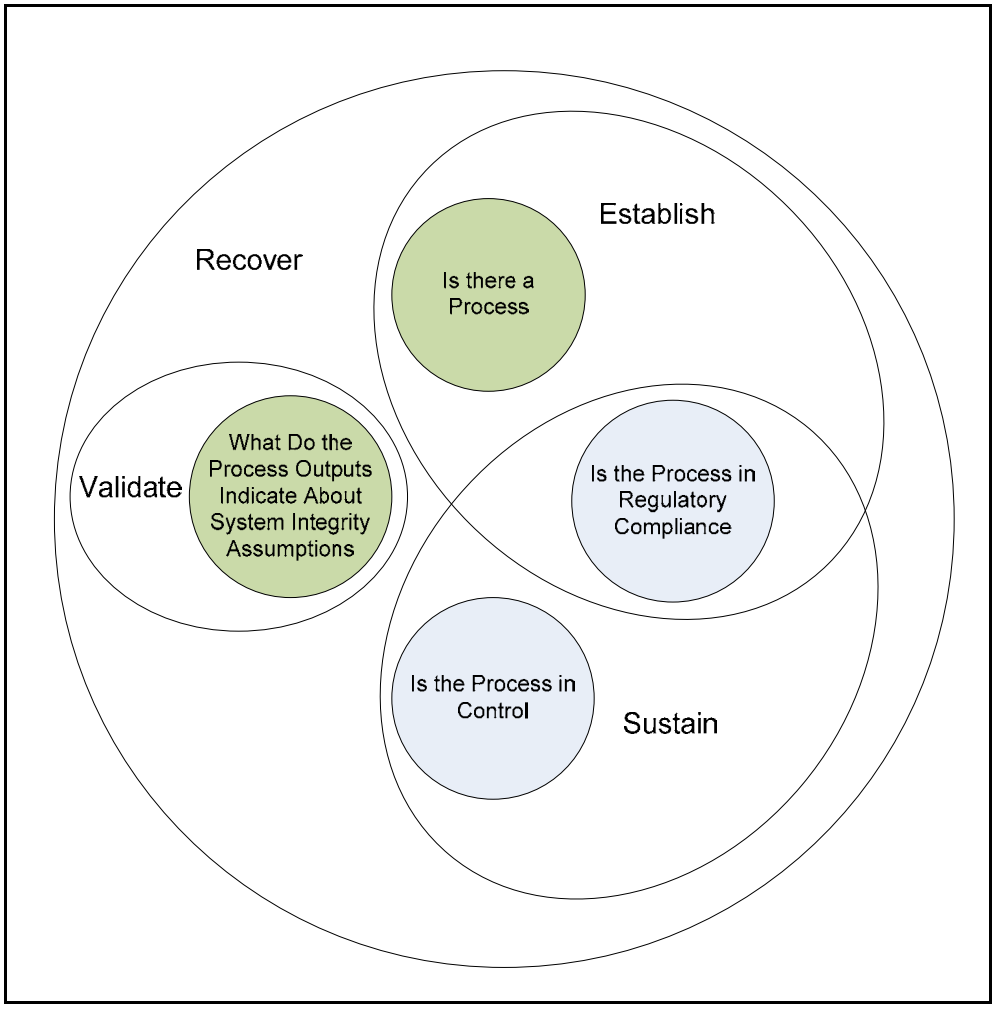
c. Is the policy, process or procedure in control? (Sustaining)(Recovering)

d. Does the output of the implementation of the policy, process or procedure indicate that there is a loss, or the potential for loss, of SysI? (Validating)(Recovering)

e. Has the policy, process or procedure gone out of control or regulatory compliance, or been identified as the cause of a loss, or the potential loss, of SysI? (Recovering)

117. The manner in which processes that support SysI relate to the ESVRE framework is shown in Figure 11. If a process is found to be not in regulatory compliance or is out of control then there is a requirement for recovery action for the process.

Figure 11 - SysI Supporting Process / ESVRE Relationship



118. If analysis of the outputs of a process, or a number of processes indicates that there may be a loss of integrity of the aircraft systems then there is a requirement for recovery action against the aircraft systems.

119. When considering what the output processes are telling you about System Integrity greater advantage can be gained if the outputs are considered in relation to each other, against the threats to System Integrity.

2.3 - RA5721 (3): Sustaining System Integrity

120. RA 5721(3) gives the requirement for the ongoing monitoring of System Integrity and the processes that support it, as well as onward reporting requirements.

> *'The TAA **shall** sustain SysI to continuously monitor and counter the threats to System Integrity'.*

It also outlines the ongoing requirement of the SysIWG.

2.3.1 - System Integrity Strategy

121. The SysI Strat Doc should be produced as part of the Establishing activity for SysI Management. As the PT moves onto Sustaining activities, the PT's strategies for SysI should be maintained, reviewed and updated. This ongoing strategy development should be articulated to all the SysI stakeholders through the SysI Strat Doc, which should be maintained as a living document as part of the platforms TLMP.

122. The strategy should be reviewed biannually, ensuring it is an up to date representation of the PT's strategy for SysI, covering long, medium and short-term aims, and objectives. It should be made available to SysIWG stakeholders prior to the SysIWG, giving them the opportunity to review the strategy and offer comment at the SysIWG, as an agenda item.

2.3.2 - System Integrity Plan

123. All PTs are required to produce a SysI Plan. The plan should articulate how the strategy will be implemented, as well as indicating the timeline for routine / scheduled activities in support of SysI. The Plan is to be integrated within the SysI Strat Doc and will cover implementation of the PT's SysI strategy.

124. The creation and maintenance of the plan is a continuous Sustaining SysI activity that ensures all SysI ESVRE related activities are captured and coordinated and that resource requirements are identified and allocated and actions are undertaken at the correct time in the platform's life cycle. This aspect is particularly important to inform decisions regarding life-extension activities in terms of costs and when to undertake activities. Hence SysI planning is a continuous activity and as such the Plan complements the TLMP. It will incorporate all the elements of the ESVRE framework, including: major modification and capability upgrade programmes, and changes in fleet disposition, fleet drawdown and OSD plans. Furthermore, the plan will also identify all planned SysI activities to achieve platform airworthiness until OSD.

125. The System Integrity Plan is to be reviewed at every SysIWG. Any proposed changes to the Plan are to be endorsed by the SysIWG members and authorised by the Project Engineer or equivalent person holding delegated airworthiness authority.

2.3.3 - SysIWG

126. The SysIWG is the working group for the management of SysI and its associated airworthiness impact. The focus of the meeting should be on Airworthiness and not the management of logistics and supportability issues, unless the logistics and supportability issues are manifesting as a threat to SysI, which can then have an impact on airworthiness.

127. The SysIWG requires a broad based stakeholder community of key stakeholders and other stakeholders, as identified in RA 5721. The list in RA 5721 is not meant to be an exhaustive list and the PT should consider inclusion of anyone who has an interest in the SysI of the platform, or manages equipment or processes which can have an impact on SysI. Broad stakeholder attendance ensures that:

a. Threats that cross organizational and process boundaries can be fully explored.

b. The elements of risk that reside in the organization or process boundaries and handovers can be identified and managed at the SysIWG.

c. A broad SQEP base is available to support decision making which might have an impact on airworthiness.

d. Recovery action can be discussed by the relevant stakeholders at the SysIWG, once a compromise, or the potential for compromise, has been identified.

e. All Integrity stakeholders have the opportunity to bring to the PT concerns over the threats to System Integrity that are identifiable from their area of responsibility.

128. As already shown at Figure 10 the SysIWG sits in a hierarchy of meetings with responsibility for onward reporting of any hazards resulting from a loss or the potential for a loss of SysI. The SysIWG might also initiate recovery action in mitigation of risks already being managed at the platform safety meetings. Similarly the SysIWG is also supported by the outputs of other the meetings and working groups shown in Figure 10Figure 9. It is important to maintain the information and activity flow in both directions between the SysIWG and these other meetings to ensure System Integrity is Sustained, Validated and Recovered.

129. Furthermore effective SysI Management requires a concerted effort and activity between SysI WGs, both in supporting the processes that support SysI, and in considering the outputs of the processes that support SysI to identify potential issues. The minutes of the SysIWG should act as a record of the SysI decisions made at the SysIWG and be used as a prompt for activity to ensure progression and closure of recommendations and actions between meetings.

2.3.4 - System Airworthiness Regulatory Compliance Scorecards (SARCS)

130. The DE&S requirement for onward reporting to the relevant AMG is achieved through application of the SysARCS. The SysARCS is the DE&S mandated scorecard that the PT uses to assess their MRP compliance with respect to SysI Regulation. It is a measure of regulatory compliance and not an indicator of RtL. It is owned by the DE&S Airworthiness Team but is used as part of the regulatory requirement so that the level of compliance can be onwards reported to the AMG.

2.3.5 - Sustaining the Process

131. Sustaining requires that the processes that were identified in Establishing are maintained in regulatory compliance and in control, as depicted in Figure 11, so that their effective application can help in the continuous countering of the threats to System Integrity. Many of the processes identified will have regulatory requirements of their own, which might be subject to audit and may not be owned by the PT. This highlights the need for a broad stakeholder community at the SysIWG, as well as the need for proactive management of SysI.

132. Maintaining the processes that support SysI on its own is not enough to counter the threats. There must also be mechanisms / processes in place to consider the outputs of the processes to evaluate what they are telling you about the state of SysI on the air system. Loss of SysI results in system failures through compromised design assumptions, either through initial error or subsequent modification in systems or use, either intentional or inadvertent. Managing the processes that support SysI and considering their outputs may lead to the identification of an incorrect design assumption, as part of Validation, before any associated threats are realised. This level of evaluation gives the PT the opportunity to intervene and introduce corrective action before a system failure can occur.

2.3.6 - Configuration Management A lack of Sys CC is one of the identified threats to SysI since without adequate control of the aircraft's configuration; there exists the possibility that the 'as-flown' configuration will not match the 'as-designed' and 'as-certified' configuration. Failure to maintain Sys CC may have adverse effects on SysI and Airworthiness. These deviations or changes to CC may affect functions, failure rates, system-to-system interactions, aircraft mass and balance as well as systems layouts. Moreover, without Sys CC there is a risk that the DO will make life extension, modification and repair recommendations based on presumed configuration that does not match the as-flown configuration.

2.3.7 - Obsolescence Management

135. Obsolescence is the loss or impending loss of the manufacturers or suppliers of items or shortages of raw materials and is one of the identified threats to system integrity. Failure to manage obsolescence may result in reduced availability of components, systems or aircraft and increased through-life costs. It is therefore necessary for PTs to maintain an Obsolescence Management plan as part of their TLMP aimed at ensuring that obsolescence is managed as an integral part of design, development, production and in-service support, in order to minimise its cost and impact throughout the product life cycle. Where necessary special requirements for qualification and certification are to be taken into account.

136. The Acquisition Operating Framework (AOF) website is an authoritative source of policy and best practice on Support Solution Envelope (SSE) aspects for all members of the MOD and Industry partners concerned.

2.3.8 - Support Policy Statement (SPS)

137. When an aircraft enters service, its systems may be the subject of an SPS. The SPS is an executive document and is one of the main subordinate documents of the air system ADS, which specifies all support arrangements for an aircraft or equipment throughout its service life. In particular, it contains details on the functionality and capability of the

system, details on how the system is to be maintained and any other system- specific information. The SPS will also contain the following information:

a. Aim.
b. Management responsibilities.
c. Security aspects.
d. Engineering and maintenance philosophy.
e. Personnel and training.
f. Test equipment and support.
g. Technical information.
h. Facilities.
i. IT resources.
j. Deployment plans.
k. Product support – Through Life Management Plan.
l. Supply support philosophy.

138. The initial SPS should be produced by the Integrated Logistics Support (ILS) Team in conjunction with the contractor. Furthermore, the SPS is promulgated as the first leaflet of either the 2(N/A/R)1 or the Equipment Topic 5W. The SPS should be reviewed at least every 5 years or sooner if there is a significant change to the support policy or there are changes to the responsibilities of the staffs or formulations that provide ILS.

2.3.9 - Maintenance Schedule

139. The maintenance schedule should be produced, for application to the maintenance programme, using MSG3 logic, and must be modified in light of aircraft modifications.

140. The first maintenance schedule review should be carried out no later than 5 years after the in-service date for the platform, and must be carried out using RCM techniques. The requirements of JAP(D)100C-20 and JAP(D)100C-22 are the MOD's preferred options to ensure that standardised measures are applied to maintenance schedules for aircraft, air launched guided weapons and their installed systems. The frequency of subsequent maintenance schedule reviews should be set by the TAA and published in the relevant SPS. The periodicity of the maintenance schedule review should be re-assessed as part of the overall SPS review process.

2.3.10 - Maintenance

141. Maintenance is an integral part of an air system's Sustaining activities since the correct and timely application of preventative maintenance, supported by the SPS and Maintenance Schedules, underpins SysI throughout the life of an aircraft or system's life.

142. Maintenance is either carried out at predetermined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the functioning of an item, and falls in three distinct categories:

a. Flight servicing

b. Scheduled maintenance

c. Condition based maintenance

2.3.11 - Training

143. To ensure that SysI is sustained, adequate and timely training of all personnel involved in operating, maintaining and supporting the aircraft, or system, is required. Training is key to sustaining SysI for the life of the air system.

2.3.12 - Ageing Aircraft Audit

144. An Ageing Aircraft Audit; RA 5723, is a periodic, independent assessment of the effectiveness and applicability of procedures, management processes, technical information and documentation, established to assure a fleet's system's airworthiness is maintained throughout it's life. It is conducted to give confidence that airworthiness risks are at least tolerable and As Low As Reasonably Possible (ALARP), as the fleet ages and regulatory requirements evolve.

145. The AAA also reviews the physical condition of the aircraft, to ensure it is consistent with the management processes that have been applied to it, rationalising the as flown, as maintained and as-designed conditions for the aircraft against the requirements of the aircraft document set.

146. These AAA activities give an indication of how well the air system has been managed through its life and what impact long term exposure to the threats to SysI is having on the platform and its processes. Analysis of AAA reports may also give an indication of any system or process interactions that may be at play.

2.3.13 - Countering the Threats

147. It is useful when Sustaining SysI to consider the threats themselves and consider how they might be manifest on the aircraft, whether this constitutes a threat to SysI, and whether the supporting processes are managing the threat effectively, or whether recovery action might be necessary. Inviting the SysIWG stakeholders to consider the threats to SysI prior to the SysIWG gives the opportunity for the working group to present potential issues for consideration by attendees across organizational boundaries, allowing a multi disciplined, broad based consideration. It supports a proactive approach to the identification and recovery of potential compromises to System Integrity.

2.4 - RA5721 (4): Validating System Integrity

148. The TAA shall regularly assess SysI to ensure that system airworthiness assumptions remain valid'. RA 5721(4) validates the design assumptions through consideration of the outputs of some of the processes that support SysI. It also requires consideration of the usage assumptions, to ensure they haven't changed in a way which may compromise Integrity.

149. Validating is the part of the ESVRE framework where the design assumptions are validated by considering the outputs of the processes that have been set up in regulatory compliance during Establishing and maintained in regulatory compliance and process

control during Sustaining. The process outputs can be considered in isolation, but should also be considered in concert, as indications of a loss of SysI, or the potential for the loss of SysI may only become apparent when a variety of indicators are considered together.

150. When validating SysI it is preferable to identify where there is the potential for a compromise of SysI, as recovery action can be taken before the compromise is realized, reducing the airworthiness risks associated with the system failure.

151. Some of the design assumptions that are being validated are tied up in the definition of SysI and are amplified in the AMC which support the regulation. These definition based design assumptions must also be consider any change in use or environment of use that may compromise the design assumptions.

152. That a system can operate within defined limits is validated by the use of technical publications, including the ADS, for system testing. The test schedules for the systems incorporate design assumption that relate to system performance against functional requirements for the use specified. These technical publications are dependent on effective publications configuration control and the management of publication changes through the CCB and F765, or equivalent, processes. It is also dependent on the use of competent organizations for their development and management, as well as their technical content. The technical publications themselves should also have had validation and verification activity carried out on them to ensure that they are fit for purpose. Some of the system testing requirement is identified through the scheduled maintenance programme and some is through recovery of system faults.

153. That a system can operate without undue frequency of failure is validated through the maintenance schedule review process for those system elements that are identified as candidates for preventative maintenance as part of the RCM analysis and fault trending for those system elements that do not meet the RCM requirements for preventative maintenance. In the early stages of validating undue frequency of failure the systems that can have the largest impact on airworthiness and safety should have the greatest effort expended on their validation. Close attention should be paid to any items that are lifed as they are likely to have been identified as having a critical failure mode. At the next level, those items that have a preventive maintenance activity against them will have been identified as FSIs and should be considered. Fortunately, items from both these lists are covered by the maintenance schedule review activities and associated RCM analysis.

154. System elements that have system redundancy as part of the design are unlikely to have been identified as candidates for preventative maintenance through the RCMA and are dependent on their combined probability of failure in meeting their system level safety target. These failure probabilities are design assumptions and depending on their method of calculation may prove to be inaccurate when tested in use. Analysis of failure data is required to validate these design assumptions but this can be a massive undertaking and is dependent on the availability of the original design information for the system elements.

155. For systems with multiple redundancies using the same system elements there may also be further complications over the possibility of cascade failure, where the additional loads imposed by failure of one system element on the rest of the system increases the probability of failure for other system elements. It may also be possible to identify adverse

trends by analyzing fault data against failure effects, for example considering fault data for fuel leaks may identify an adverse fault trend that may indicate that there is the potential for a compromise to SysI and highlight the need for recovery action to be initiated.

156. That a system can operate without adverse effects on other systems is something that is designed into the aircraft from the start and is developed through the application of techniques such as Zonal Hazard Analysis as well as designing and subsequent testing for Electro-Magnetic Compatibility (EMC), plus consideration of common cause failures that could be internally generated by other aircraft systems and also particular risks. These assumptions can be validated through fault analysis and trending, as well as by consideration of other FRACAS data outputs. These design assumptions must also be validated when changes are introduced to the air system to ensure that the changes do not compromise strategies such as system segregation, which may have been employed to reduce the risk from zonal and common cause failures.

2.5 - RA5721 (5): Recovering System Integrity

157. Once compromise or the potential for compromise of SysI is identified the situation must be recovered:

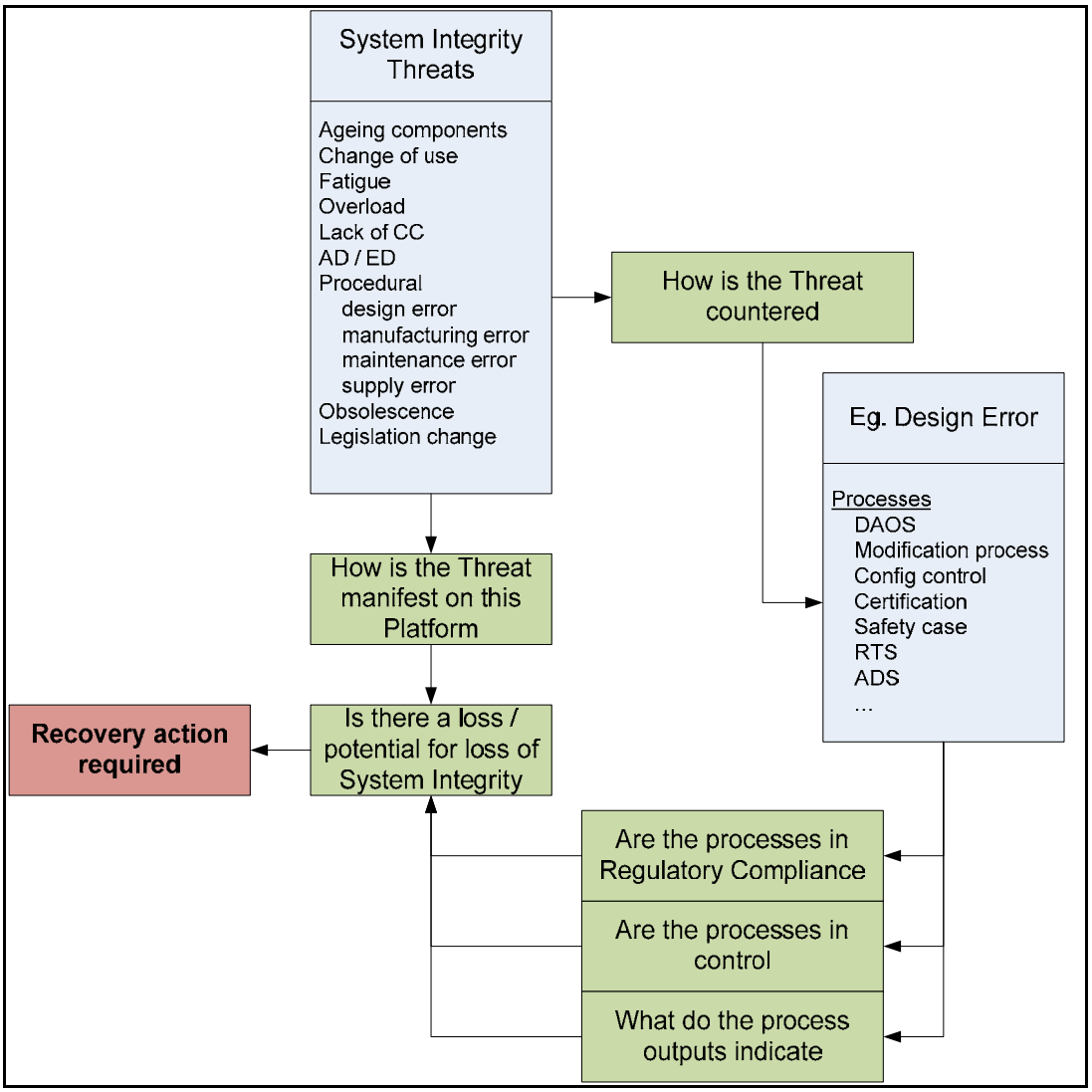
> *"The TAA **shall** recover System Integrity when it is lost, or when there is a potential for its loss".*

158. Procedures are in place within the ADS to recover SysI automatically for routine faults and occurrences; particularly for those systems that are designed using fail safe design principles that incorporate redundancy and that are expected to be replaced through corrective maintenance. These faults are unlikely to require the attention of the SysIWG and will be recovered by routine maintenance; however, as an example, fault trending may indicate that system reliability might be compromising design assumptions and indicate there is the potential for a loss of SysI. Prevalence of a particular fault might then require elevation to the SysIWG.

159. The required recovery action might need to be process or engineering based, or a combination of both. Recovery may require a range of actions, perhaps only short-term mitigation in the first instance, leading to further activity to implement a long-term solution. Significant arisings, with the potential to compromise SysI, should be reported to the SysIWG by other stakeholders, other working groups or identified through the routine PT business associated with SysI Management.

160. Depending on the risk associated with the compromise, recovery action may need to be managed through the SysIWG. Recovery action requires that the root cause(s) are identified and addressed. Processes that support SysI and can lead to Recovery actions are illustrated in Figure 12:

Figure 12 - Threat / Process Relationship



161. Loss of SysI may result in evident damage or failure, suspected damage or hidden failure, degradation of performance and/or accuracy or loss of configuration control.

2.5.1 - Evident Damage or Failure

162. Evident damage or failure to a system can become apparent:

a. Visually.

b. Through investigative activities.

c. Through reduced performance or function.

d. From Built-in Test Equipment indications.

e. From other failure indicators.

163. This damage or failure can be readily assessed. Although damage may be evident on individual aircraft, it may be necessary to assess whether such occurrences have fleet-wide implications.

164. An evaluation of system damage or failure to a single aircraft must be undertaken as it may indicate potential for similar damage or failure on, or likely to be sustained by, other aircraft. The investigation into, and recovery of, significant damage or failure must be monitored by the SysIWG. The PT must ensure that the DO brings to its attention any potential damage or failure information that can be read across from other operators of a similar system or aircraft type. Evident damage or failure will be assessed and recovered using procedures contained within, or referred out from, the ADS or schemes provided by the aircraft Repair Organizations or the DO. If a particular system exhibits persistent, recurring failures, it may be necessary to review maintenance schedules, operating procedures, or consider modification action in order to recover SysI.

2.5.2 - Suspected Damage

165. Suspected damage may occur during a specific incident to an individual system or aircraft, or during its operation outside expected usage parameters. Recovery actions are prompted by, and dependent upon, the reporting of triggering events such as:

a. Hazardous Incidents as listed in the ADS.

b. Uncommanded flying control movements.

c. Exposure of system components to extreme temperature variations.

d. Contamination of system components.

166. Type-specific procedures must be published within the ADS detailing the action to be taken following any Hazardous Incident. For other triggering events where damage is suspected, an investigation must be conducted to ascertain whether any damage has occurred. If damage is identified, the principles of recovering evident damage apply. However, the impact on a specific system caused by an unusual or unexpected event may require further specialist advice.

2.5.3 - Hidden Failure

167. A hidden failure is a failure not evident to the crew or operator during the performance of normal duties. However, most of these failures can be detected by inspections or tests performed by maintenance personnel. Although hidden failures may be detected on an individual aircraft's systems, it may be necessary to assess whether such occurrences have fleet-wide implications. Many systems have more than one function; consequently, there can be one or more hidden failures that lead to a loss of confidence in SysI. Hidden system failures fall into 2 categories:

a. Failure of a system that is normally active but gives no indication to the operating crew if it ceases.

b. Failure of a system that is normally inactive so that the crew cannot know whether it will be available when it is needed.

168. An evaluation of a hidden failure on a single aircraft must be undertaken as it may indicate potential for similar failure on, or likely to be sustained by, other aircraft. The investigation into, and recovery of, a significant hidden failure must be monitored by the SysIWG. The PT must ensure that the DO brings to its attention any potential hidden failure information that can be read across from other operators of a similar system or aircraft type. Hidden failures will be assessed and recovered using procedures contained

within, or referred out from, the ADS or schemes provided by the aircraft Repair Organizations or the DO. If a particular system exhibits persistent, recurring hidden failures, it may be necessary to review maintenance schedules operating procedures, or consider modification action in order to recover SysI.

2.5.4 - Degradation of Performance and/or Accuracy

169. Over time a system's operating performance and/or accuracy may degrade and exceed its specified tolerances and/or operating parameters, which will compromise System Integrity. Trend analysis may allow prediction of when any tolerance or parameter will be exceeded.

170. Degradation may be unnoticeable by the operator and only become apparent during maintenance, testing, or via information provided by a third party. Any discernable trend towards decreasing performance or accuracy must be investigated and recovery action taken.

2.5.5 - Compromised System Configuration Control

171. Compromised system configuration control, which can have an adverse effect on SysI, may be identified through other ESVRE or maintenance activities. Recovery action must be carried out to restore confidence in SysI.

172. Once Sys CC has been compromised action must be taken to restore Configuration Control. Concurrent with restoration an investigation and analysis of the root cause must be carried out. Part of the Configuration Control Plan should be the reasoned process of recovering CC; this will allow full documentation root cause, restoration measures and process improvement to ensure the failure route is correctly closed.

2.6 - RA5721 (6): Exploiting System Integrity

173. Exploiting SysI involves the use of data from other platforms and operators and the regulation highlights some constraints on its use.

> *"The TAA shall exploit data from other platforms or operators to support System Integrity".*

174. Data from other platforms or operators, whether UK military, overseas military or civil operators, may be exploited by PTs to support SysI. SysI evidence from accident rates, investigations, maintenance databases and usage data could be considered providing:

a. The period and nature of operations considered has to be broad and representative of UK MAE usage.

b. The current and expected UK MAE service operating envelope has to be either: benign in comparison with that of other users; or the future operating envelope must be restricted as necessary.

c. The effect of any configuration differences between UK MAE and read-across fleet aircraft needs to be considered.

2.6.1 - Supporting Arrangements and Processes

175. SysI is supported by a variety of other stakeholder organizations. These may be industry or Service organizations and may fulfil discreet, overlapping or parallel roles in support of System Integrity. Examples of stakeholder organizations have already been identified in Figure 9.

176. Design Organization (DO). Typically, the DO will be a Defence Contractor and its relationship with the PT will be articulated through a contract. Design Approved Organization Scheme (DAOS) approval is a mandatory requirement for contracts with DOs, and the DO approval will be for a defined range of products. DAOS is specified in the 5000 series RAs and is managed on behalf of the MAA by MAA-OA-DAOS. DAOS provides for independent assessment of the competence of Defence Contractors and Service Organizations involved in the design of aircraft systems. DAOS approval and the ongoing surveillance provides a level of assurance of a DO's competence, which gives confidence that they have processes in place to counter the threats to SysI associated with design error.

177. Maintenance Organization (MO). The Maintenance Approved Organization Scheme (MAOS) is a means by which the MOD can assess the competency of Organizations wishing to provide continuing airworthiness support services for military registered aircraft. Typically, the MO will be a Defence Contractor and its relationship with the PT will be articulated through a contract. Maintenance Approved Organization Scheme (MAOS) approval is a mandatory requirement for contracts with MOs, and the MO approval will be for a defined range of services. MAOS is specified in the 5000 series RAs and is managed on behalf of the MAA by MAA-OA-MAOSGroup.

178. System Airworthiness Regulatory Compliance Scorecard (SysARCS) PTs use the SysARCS to identify their level of compliance with RA 5721 and associated RAs. The MAA take note of the SysARCS as an indication of the management effect.

179. The Air Safety Dashboard (ASD). The ASD is the MAA scoring system for platform compliance and risk levels. This is informed by all groups within the MAA to give a cohesive overall picture of each platform's rich picture which is then used as a focus for the formal MAA Audit activities. .

SECTION 3 - LIST OF ASSOCIATED REGULATIONS

The following referred RAs may be useful in managing SysI:

RA	Title
1002	Competent Persons
1003	Delegation of Airworthiness Authority and Notification of Air Safety Responsibility (DE&S)
1005	Competent Organizations and Responsibilities
1014	Design Organizations – Airworthiness Responsibilities
1015	Roles & Responsibilities: Type Airworthiness Authority
1016	Roles & Responsibilities: Continuing Airworthiness Management Organizations (CAMOs)
1017	Maintenance Organization – Airworthiness Responsibilities
1130	Corporate Memory and Standards
1140	Military Air System Technical Data Exploitation
1200	Defence Air Safety Management
1205	Air System Safety Cases
1210	Ownership and Management of Operating Risk (Risk to Life)
1220	Project Team Airworthiness and Safety
1230	Design Safety Targets
1300	Release to Service
1310	Aircraft Document Set
1320	Project Team Leader – Stakeholder Interfaces
1325	Drafting of Limitations in the Release to Service
1330	Special Clearances
1360	RTS Authorization
1370	RTS Upkeep
1410	Occurrence Reporting
4200	Maintenance Philosophy - General
4203	Preventive Maintenance
4204	Lifing of Aerospace Components
4205	Corrective Maintenance
4206	Deferment of Maintenance – Guidance on the Use of Limitations and Acceptable Deferred Faults
4210	Anti-Deterioration maintenance of Equipment in Store

4214 Support Policy Statements
4350 Through Life Management of Technical Information
4351 Production and Maintenance of Maintenance Schedules
4356 Topic 2(N/A/R) – General Orders, Special Instructions and Modifications
4457 Special Instructions (Technical)
4462 Aviation Local Technical Instructions
4700 Military Air Environment Quality Policy
4701 Quality Occurrence Reporting
4702 Quality Auditing
4947 Continuing Airworthiness Management – MRP Part M Sub Part G
4951 Quality System – MRP Part M Sub Part G
4953 Record Keeping – MRP Part M Sub Part G
4955 Findings – MRP Part M Sub Part G
4956 CAMO Tasks Performed by Other Organizations – MRP Part M Sub Part G
4970 Baseline Military Airworthiness Review – MRP Part M Sub Part I
4971 Airworthiness Review and Certification – MRP Part M Sub Part I
4972 Airworthiness Review Staff – MRP Part M Sub Part I
4973 Airworthiness Review Process – MRP Part M Sub Part I
4974 Circumstances When Military Airworthiness Review Certificates Become Invalid – MRP Part M Sub Part I
5001 Certification and Release of Materiel
5101 DAOS Approval Procedures and Responsibilities
5103 Certification of Design
5106 Aircraft Contractors Responsibilities
5201 Interchangeability
5203 Requirement Specifications
5206 Sampling Procedures for In-Service Materiel
5208 Testing of Experimental and Development Aircraft Equipment
5209 Relationship Between Service Units, MOD and Contractors in the Development of Materiel
5213 Final Examinations and Conferences
5214 Schedule of Equipment – Appendix A to the Aircraft Specification
5221 Traceability of Identifiable Parts
5301 Control of Designs
5302 Design Records

5303 Local Technical Committee (LTC)
5304 Configuration Control Board
5305 Modification Classification
5306 Draft Modification Leaflets
5307 Identification and Recording of Design and Modification States of Materiel
5308 Service Modifications
5311 Configuration Management – Project Team
5312 In-Service Design Changes
5313 Design Modifications – Project Team
5320 Aircraft Maintenance Programme – Design Guidelines
5401 Provision of Service Technical Publications
5402 Validation and Verification of Service Technical Publications
5403 Amendments to Service Technical Publications
5405 Special Instructions (Technical)
5502 Aircraft Maintenance Forms and Engineering Record Cards
5721 System Integrity Management
5723 Ageing Aircraft Audit
5724 Life Extension Programme
5725 Out of Service Date Extension Programme