



Australian Government
Department of Defence

Simulation Safety Guide

Australian Defence Simulation Office

Department of Defence, Canberra

DRAFT

Copyright Notice

© Commonwealth of Australia 2005

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968 (Cwlth)*, no part may be reproduced by any process without prior written permission from the Director-General, Simulation, Department of Defence.

Requests and inquiries should be directed to:

Director-General, Simulation
Australian Defence Simulation Office
Russell Offices [R1-3-B065]
Canberra ACT 2600
AUSTRALIA

Produced by the Australian Defence Simulation Office
in collaboration with:

Booz | Allen | Hamilton

Booz Allen Hamilton (Australia) Limited
Level 7, 12 Moore Street
Canberra City ACT 2601
AUSTRALIA

Telephone: +61 2 6279 1900
Facsimile: +61 2 6279 1990
Visit us on the web: www.boozallen.com

The principle authors, Brian McBride and Sal Sidoti, would like to recognise the contributions made by the following Defence members. Your support is greatly appreciated.

- Mr. Darren McFarlane, Australian Defence Simulation Office
- WGCdr Tom Wickham, Australian Defence Simulation Office
- Mr. Ralph Wittwer, Aerospace Systems Division
- LTCol James MacRae Land 134 Project Director



Australian Government
Department of Defence

Foreword

In their Defence Occupational Health Safety Policy Statement the Chief of the Defence Force and Secretary have reiterated that safety is core Defence activity. The Simulation Safety Guide (SSG) provides a source of initial information and advice in relation to safety issues regarding the acquisition, development, management, support and use of Defence Simulation capabilities in support of a number of applications areas, as cited in Defence Simulation Policy DIG (OPS) 42-1. The Guide also directs the reader to where more detailed information and advice can be found.

The SSG is a living document and will be updated as required given changes in policy and guidance. Comments or further clarification on any aspect of the SSG are welcomed. Please complete the evaluation form at the back of this document.

Cliff White
Director-General, Simulation
Australian Defence Simulation Office

Telephone: (02) 6265 2019
Facsimile: (02) 6265 2223
Email: cliff.white@defence.gov.au

Table of Contents

1	Background.....	1
1.1	Introduction	1
1.2	Purpose of the Simulation Safety Guide	1
1.3	Scope of the Simulation Safety Guide	1
1.4	Structure of the Simulation Safety Guide	2
1.5	Relationships to Other Documents.....	3
1.6	Acronyms, Abbreviations and Definitions.....	4
2	Key System Safety Concepts	5
2.1	The Concept of Safety.....	5
2.2	The System Safety Context.....	7
2.3	The Accident Model – How Do Accidents Occur	7
2.3.1	The Basic Accident Model	8
2.3.2	The James Reason Model	8
2.4	Risk Management and control.....	10
3	The Defence Safety Management Context	11
3.1	Legislation and Defence Safety Policy	11
3.2	Framing Regulations, Guidance & Standards.....	12
3.2.1	Regulations, Procedures and Instructions	12
3.2.2	Standards and Guidance	13
3.3	Key Issues for Simulation Safety	14
4	Overview of Safety Management throughout the Capability Life Cycle For Simulation	15
4.1	Overview of the Capability Life Cycle	15
4.2	Key Safety Management Activities.....	15
5	Simulation Safety Risk Factors, Case Studies & Lessons Learnt.....	19
5.1	Safety in Live Simulation.....	20
5.1.1	Key Contributors to Safety Risks	20
5.1.2	Key Mitigation Measures	21
5.2	Safety in Constructive Simulation.....	22
5.2.1	Key Contributors to Safety Risks	22
5.2.2	Key Mitigation Measures	23
5.3	Safety in Virtual Simulation.....	24
5.3.1	Key Contributors to Safety Risks	24
5.3.2	Key Mitigation Measures	25
5.4	Safety in Distributed Simulation Environments.....	26
5.4.1	Key Contributors to Safety Risks	26
5.4.2	Key Mitigation Measures	26
5.5	Examples of Simulation Safety in ADF Practice	27
5.5.1	The AP-3C Orion Advanced Flight Simulator	27
5.5.2	Australian Army Combat Training, Range Instrumentation and Live Instrumentation System (CTC-LIS)	28
5.5.3	RAN Guided Missile Frigate Embedded Simulation Capability	29
5.5.4	Future Combat Aircraft Aircraft Embedded Simulation and Training (ES&T) Capabilities	29
6	Specialist Simulation Safety Topics	31

6.1	Simulation for Safety Critical System Design & Verification.....	31
6.2	The role of VV&A in Simulation Safety	32
6.3	Human Factors and Simulation Safety	32
6.3.1	Negative Training Transfer	33
6.3.2	Simulation Fatigue and Sickness	33
7	Simulation Safety Support Network.....	35
7.1	The Defence Safety Management Agency	35
7.2	Group Safety Committees	35
7.3	Safety and Emergency Management Across Establishments	36
7.4	Other specialist Agencies and COE	36
8	Simulation Safety Training	37
Annex A Abbreviations and Acronyms.....		35
Annex B Definition of Terms.....		36
Annex C Simulation Safety References.....		37

List of Figures

Figure 1-1: Structure of this Simulation Safety Guide	2
Figure 1-2: Relationship of the Simulation Safety Guide to other Key Defence Documents	3
Figure 1-3: Relationship of Simulation Safety Guide to other Parts of SIMMAN	4
Figure 2-1: The Risk/Probability/Exposure/Consequence Relationship	6
Figure 2-2: The Safety/Cost Trade-off	6
Figure 2-3: The System Safety Context	7
Figure 2-4: A Basic Accident Model	8
Figure 2-5: Accident Feedback Loops and Indicators	9
Figure 2-6: Risk Reduction Flowchart	10
Figure 2-7: Transfer of Acceptable and Unidentified Risks	10
Figure 3-1: The Technical Regulatory and OHS Framework	11
Figure 3-2: High Level Defence Technical Regulatory Documents	13
Figure 4-1: Capability Systems Life Cycle	15
Figure 5-1: Classes of Simulation	19
Figure 5-2: CTC-LIS Concept	28
Figure 5-3: Aircraft Embedded Simulation and Training Concept	30

List of Tables

Table 4-1: Safety Management Activities at Different Stages of the Capability System's Life Cycle	18
Table 5-1: Key Live Simulation Hazards and Examples	20
Table 5-2: Key Live Simulation Hazards and Mitigation Measures	21
Table 5-3: Key Constructive Simulation Hazards and Examples	23
Table 5-4: Key Constructive Simulation Hazards and Examples	23
Table 5-5: Key Virtual Simulation Hazards and Examples	24
Table 5-6: Key Virtual Simulation Hazards and Example Mitigation Measures	25
Table 5-7: Key Distributed Simulation Hazards and Example Mitigation Measures	26
Table 5-8: Key Distributed Simulation Hazards and Mitigation Measures	26

1 BACKGROUND

1.1 INTRODUCTION

1. As the cost of Defence human and material resources climb increasing reliance is being placed upon the use of various forms of Simulation to maintain Defence capabilities. Simulation is beginning to impact all areas of Defence activities and is used to teach and maintain skills, develop and refine procedures and to test and evaluate equipment and munitions. These Simulation activities can immerse people into complex systems incorporating many hazards. Like any complex system, a Simulation can endanger the people and environment around it if it is not designed, constructed and operated safely. Safety cannot be added onto a complex system like a coat of paint, it must be designed into the system from the start and maintained like any other system element. Further, the potential for these activities to present a hazard increases as the variety, number, scale and complexity of Simulation activities increase.

2. Simulation can be used to reduce the risk inherent in many Defence activities such as training, and test and evaluation. However, care must be taken to ensure that when Simulation and synthetic environments are applied to these activities they do not also introduce new risks.

3. In November 2002 the Chief of the Defence Force and the Secretary issued a joint Defence Occupational Health and Safety (OHS) policy statement. In this, they reinforced their commitment to creating a culture where the health and safety of everyone in Defence was of fundamental importance in every workplace and business process. Further, they directed that health and safety were to be integrated into all Defence activities and that these strategies were to be integrated with other management functions. As such, OHS needs to be considered in all facets of Simulation conducted by Defence.

1.2 PURPOSE OF THE SIMULATION SAFETY GUIDE

4. The purpose of this Guide is to assist the acquirers, developers, managers, users, and supporters of simulation in understanding how to manage Safety Risk in the acquisition, development, management, support and use of Simulation.

1.3 SCOPE OF THE SIMULATION SAFETY GUIDE

5. This guide provides specific advice on the application of safety within the Defence simulation environment across the different types of simulation, including: 1

- a. **Constructive Simulations.** In constructive Simulations individuals generally stimulate (make inputs to) the constructive Models but they are not directly involved in determining the outcomes of the Simulations. Constructive Simulations are used typically in situations, such as combat engagement Simulations for example, where participants seek to achieve a specified military objective given pre-established resources and constraints. They may also use

¹ Definitions from the Australian Defence Simulation Glossary

engineering, cost and support Models. Examples include wargames, models and analytical tools.

- b. **Virtual Simulations.** Virtual Simulations inject humans in the loop to exercise motor control, decision-making, or communications skills. The human element of a virtual Simulation is not modelled. The simulated systems in virtual Simulation would be made up of constructive Models. Examples include individual aircraft (or weapon system) simulators and virtual prototypes.
- c. **Live Simulations.** Traditionally having a training focus, live simulations represent military operations using military personnel and equipment in which simulated experiences are achieved using near-combat conditions. The advances of computer-based simulation support is enriching this field, enabling real time data collection and exercise control, including the real-time insertion of virtual simulations to stimulate live responses (eg; computer controlled targets on live-firing ranges, EW threat/missile engagement scenarios).
- d. **Distributed simulation.** A synthetic environment within which humans may interact through Simulation at multiple sites networked using complaint architecture, modelling, Protocols, standards and databases.

1.4 STRUCTURE OF THE SIMULATION SAFETY GUIDE

6. This Guide has been structured into the following chapters as identified in Figure 1-1.

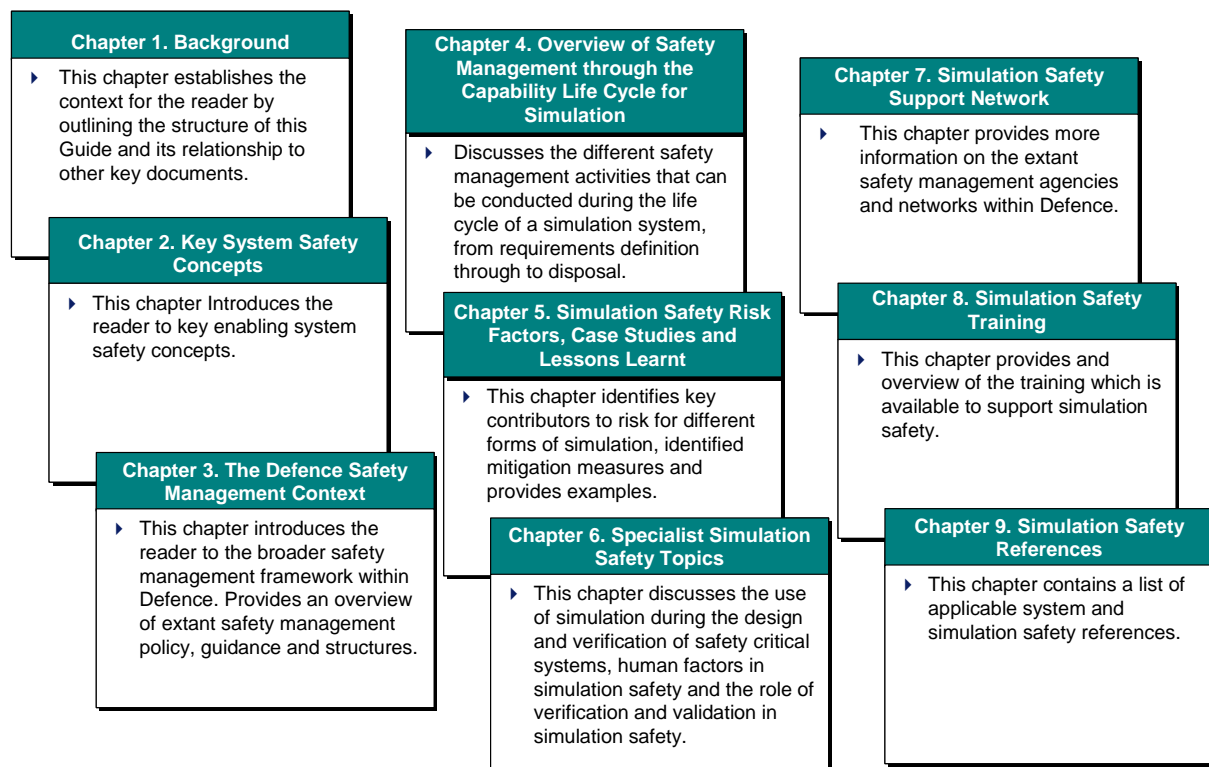


Figure 1-1: Structure of this Simulation Safety Guide

1.5 RELATIONSHIPS TO OTHER DOCUMENTS

7. This Guide forms part of the Defence Simulation Manual (SIMMAN). The relationship between the Simulation Safety Guide and other key Defence documents is shown in Figure 1-2.

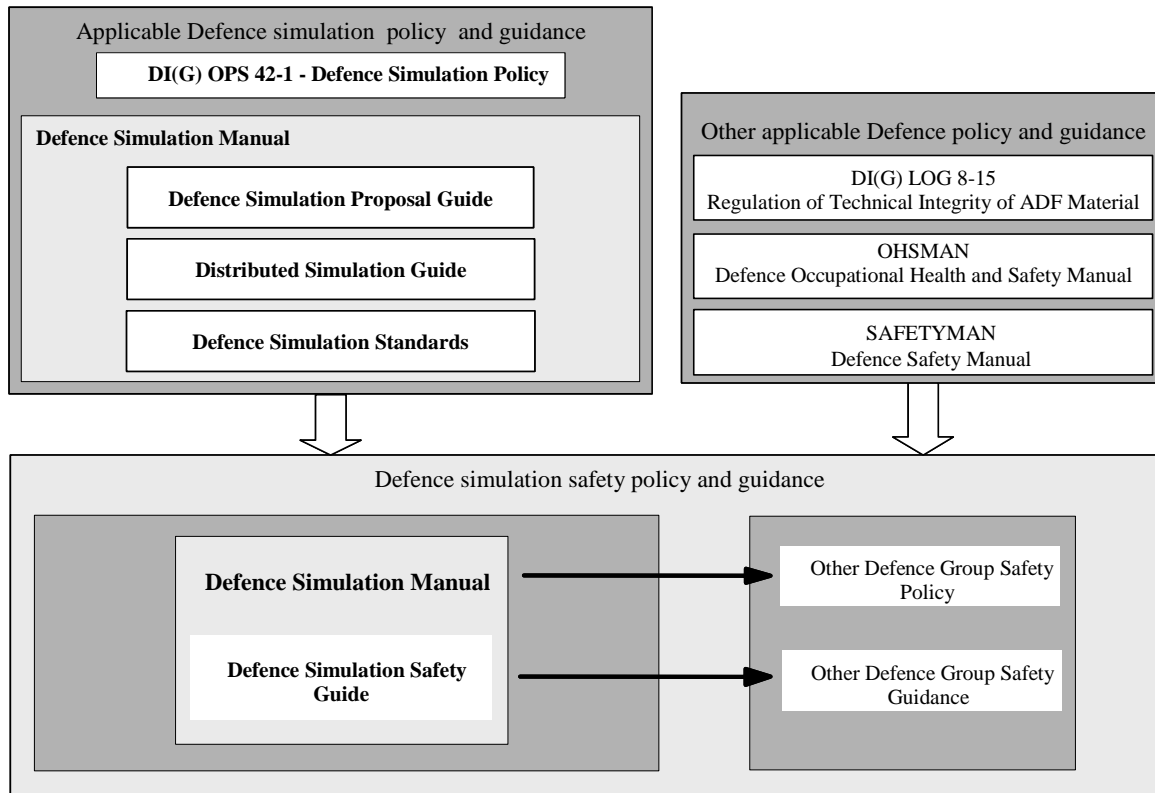


Figure 1-2: Relationship of the Simulation Safety Guide to other Key Defence Documents

8. Currently a work in progress the SIMMAN will eventually comprise two volumes containing 21 parts. The relationship between this Simulation Safety Guide and these other elements, some of which are still in draft form, or to be completed, is shown in Figure 1-3.

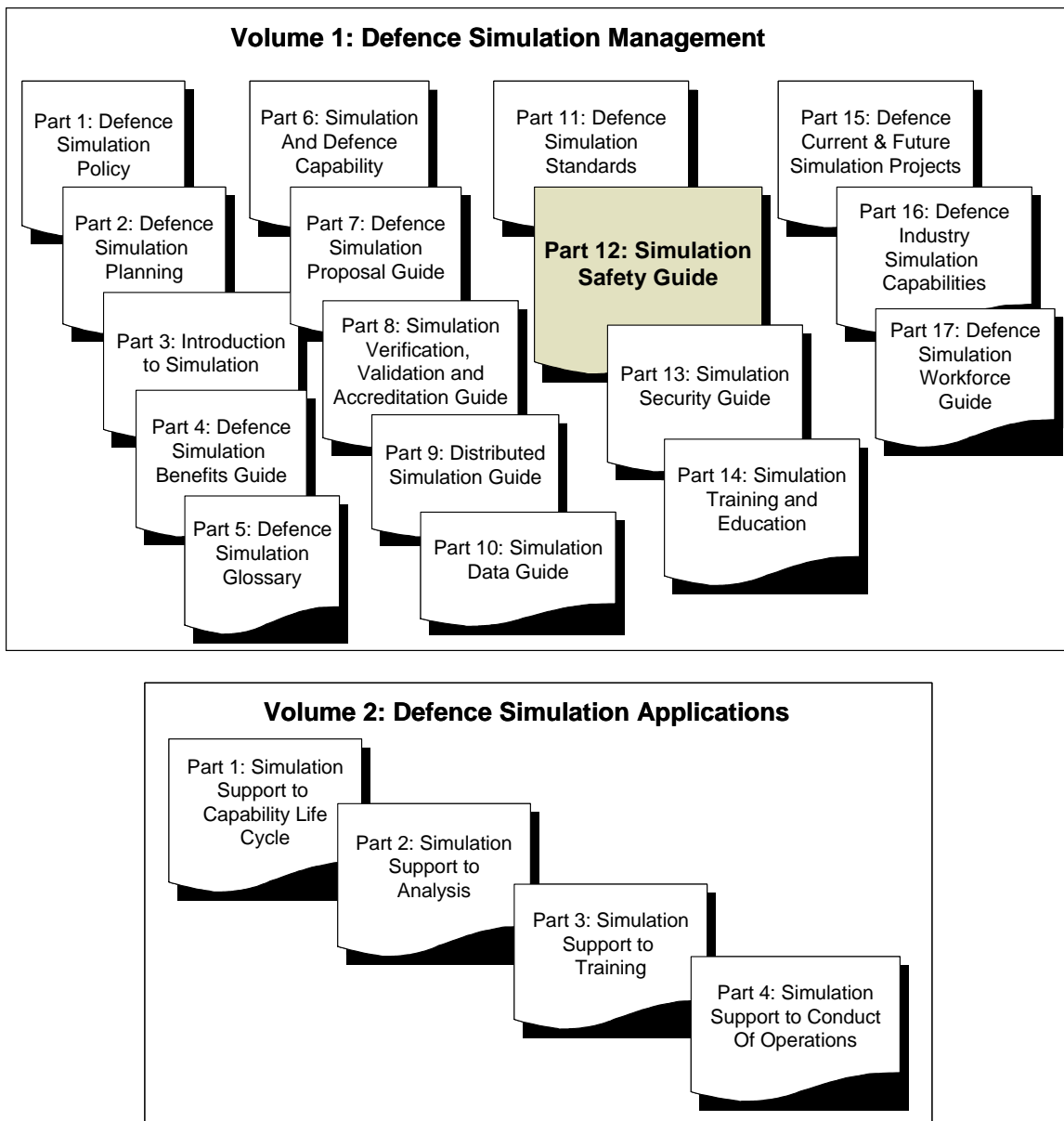


Figure 1-3: Relationship of Simulation Safety Guide to other Parts of SIMMAN

1.6 ACRONYMS, ABBREVIATIONS AND DEFINITIONS

9. Refer to Annex A for a list of relevant acronyms and abbreviations used in this Guide.
10. Refer to Annex B for a list of definitions of terms used in this Guide.

2 KEY SYSTEM SAFETY CONCEPTS

2.1 THE CONCEPT OF SAFETY

11. The aim of this Section is to provide a brief overview of the concept of System Safety and to highlight different methods by which accidents can be caused. It is important for both developers and users of Simulation to have an understanding of the concept of Safety due to the range of hazards which Simulation can present. “There is no totally reliable method of eliminating risk from the operation of safety critical systems. However, when systems are developed in ignorance of safety issues, the probability of deaths, or injuries, resulting from design flaws in the system increases.”²

12. Safety can be an abstract concept. MIL-STD-882D defines safety as “Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment.” Systems can be developed that are completely safe, but this will often compromise their ability to perform the function for which they were designed. Accordingly, for a system to be useful, there will normally be a need for the acceptance of some level of residual risk to safety. The more complex a system, and the more interactions that it has with the external environment, the more likely it is that the management of this residual risk will remain an ongoing requirement for the system throughout its operational life.

13. It is also important to note that in the real world it is usually not possible to completely remove all the hazard from a complex system, even if this is the intention. Irrespective of how a system is designed it is rarely possible to control the external environment or human actions to the extent sufficient to completely prevent all mishaps. Similarly, as described above, designing too many safety features into a system may make it ultimately unsuitable for its intended purpose. The degree to which safety and functionality may need to be compromised becomes a decision based on risk, and therefore the ability to manage this level of risk is the key to real-world safety management.

14. The risk posed by a potential Mishap is the combination of the likelihood of a Mishap occurring multiplied by the negative consequences likely to be caused to those people, equipment and the environment exposed to the event. Hence a Mishap which would cause only mild effects and is highly unlikely to occur presents a small risk. Similarly, a mishap with moderate consequences, but to which large numbers of people are exposed may present high risk. This concept is illustrated in Figure 2-1.

² DEF(AUST) 5679 *The Procurement of Computer-Based Safety Critical Systems*, p 7.

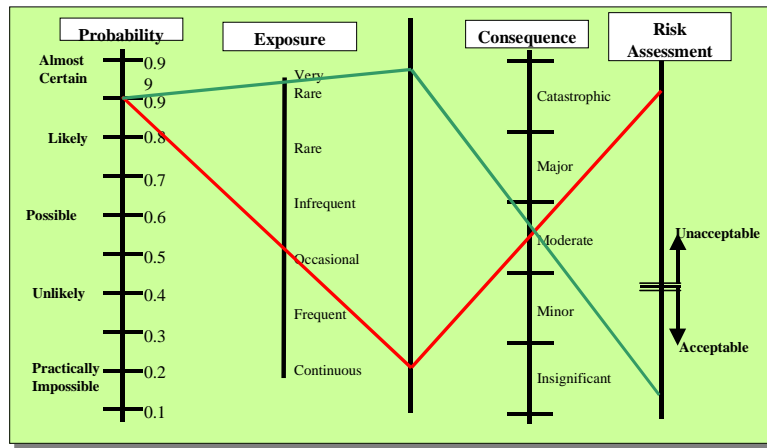


Figure 2-1: The Risk/Probability/Exposure/Consequence Relationship

15. Each industry and circumstance should have a level of risk which it is prepared to accept. Where the risk posed by possible mishaps exceeds this level measures can be taken to reduce the risk by either reducing the potential of the Mishap occurring, or reducing the likely severity if it does. Numerous systems and frameworks are available to help quantify the level of risk posed by a hazard by assessing the likelihood and potential consequence of it occurring.

16. In practice, what is required is a trade-off between the residual hazard levels in the system and the cost and effort expended in making it safe. This compromise is illustrated graphically in Figure 2-2. It is important to note that cost in the Defence context is not purely monetary, but must reflect the total cost of safety incidents (including the effects of any mission failure so caused).

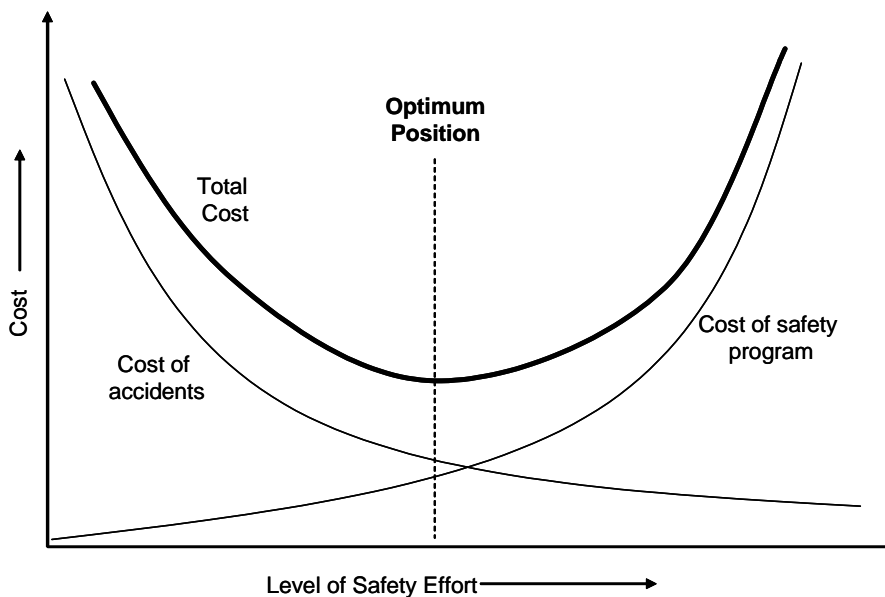


Figure 2-2: The Safety/Cost Trade-off³

³ FAA System Safety Handbook, Chapter 17, p 3-3.

17. In summary, when considering safety and risk, three important concepts must be accepted:
- Safety is a degree of freedom from harm.
 - Nothing is perfectly safe.
 - Safety is to an acceptable level of risk.

2.2 THE SYSTEM SAFETY CONTEXT

18. In a complex technical environment, such as is common in distributed Simulations, it is critical to consider safety in the context of the entire system. A system is defined as an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.⁴ The complexity of a system will be determined to a large extent by the number of interactions (both functional and physical) which occur within it, and between the system and its external environment.

19. If only one aspect of the system is analysed it will produce a set of unique hazards applicable only to part of the system. However, if that aspect of the system is analysed taking into account all other aspects of the system the analysis results will identify numerous other hazards. Conversely, the results of a system analysis may demonstrate that hazards identified in the subsystem analysis were either reduced or eliminated by other components of the system. In particular, it is the complex, and often difficult to exhaustively map, interactions amongst diverse system elements that can lead to the least foreseen hazards.

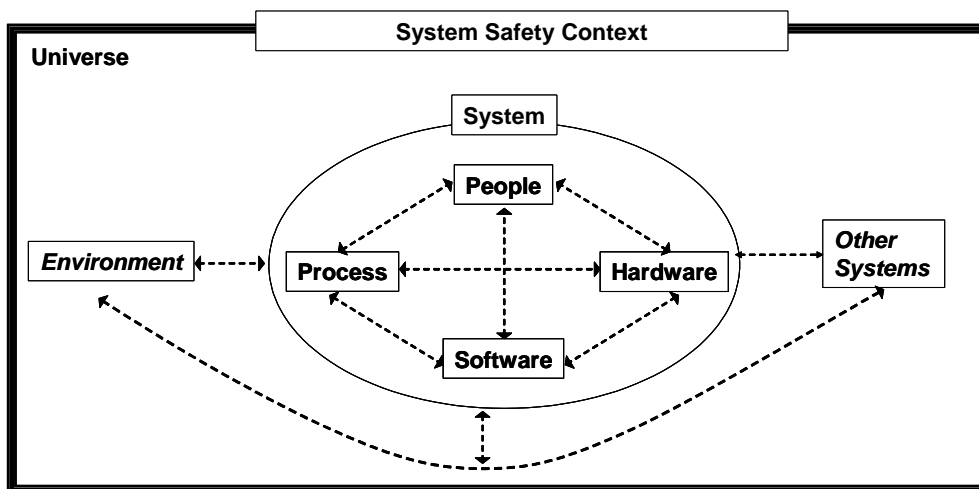


Figure 2-3: The System Safety Context

2.3 THE ACCIDENT MODEL – HOW DO ACCIDENTS OCCUR

20. In order to mitigate the risks posed by the potentially hazardous Simulation environment it is important to understand how accidents occur. An understanding of the manner in which accidents normally happen is critical to being able to put into place measures

⁴ (MIL-STD-882D).

and systems to prevent them from occurring. The aim of this section is to provide a layman's description of a couple of accident models.

2.3.1 The Basic Accident Model

21. An accident is an unplanned process of events that leads to undesired injury, loss of life, damage to the system or to the environment. Accidents are normally the result of a long chain of events usually including hazards, exposure frames, control mechanisms, and initiating events

22. Accident models can be used to show the major events that give rise to an accident. The simplified view states that a hazardous situation, when triggered by some initiating event, will go through a sequence of events that may result in an accident. It is a fact that hazards exist, but they can be managed by a series of verified control mechanisms. The more complete view of an accident model shows that if an accident is to occur control mechanisms have to fail. This process is illustrated in Figure 2-4. Yet more complex models will show often longer causal chains where multiple groups of hazardous situations may need to be traversed and multiple control mechanisms by-passed before an accident can occur.

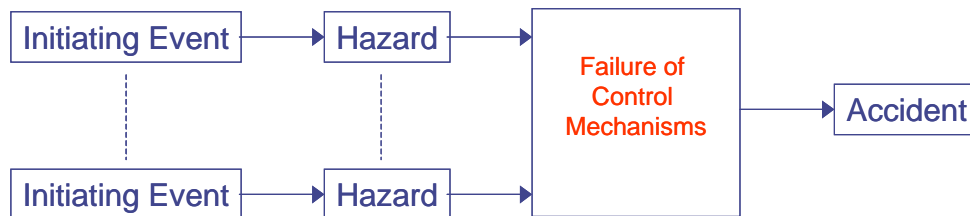


Figure 2-4: A Basic Accident Model

2.3.2 The James Reason Model

23. The James Reason Model is a more complex representation of the basic accident model which attempts to map at what points in the accident chain effective control measures are able to reduce the probability of accidents occurring.

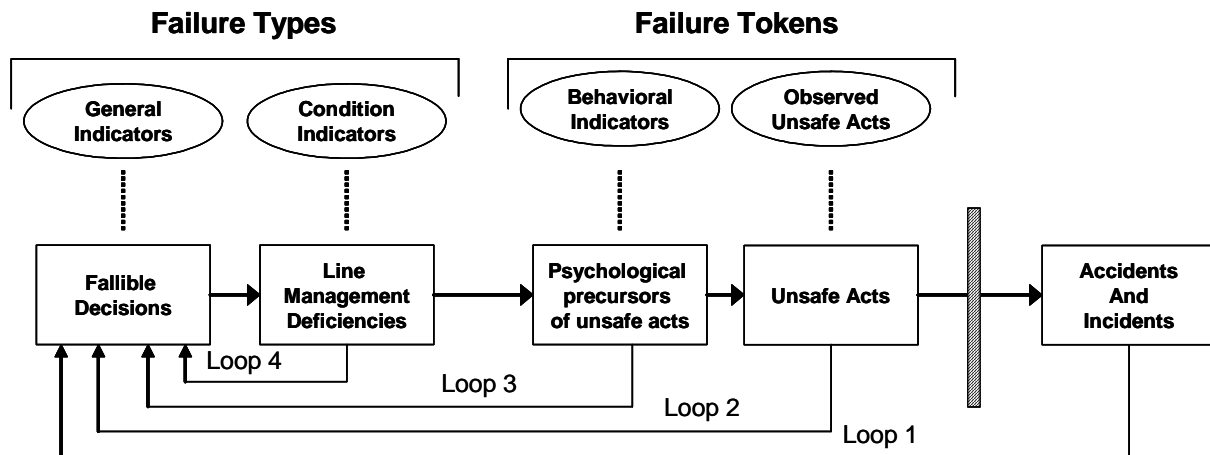


Figure 2-5: Accident Feedback Loops and Indicators⁵

24. Figure 2-5 shows a number of feedback loops and indicators which can be used to better manage system safety. Collectively these feedback mechanisms and indicators can be referred to as a Safety Information System (SIS). At each point in the accident causal chain there is opportunity for the potential accident to be noted, reported and control mechanisms employed to removed the hazard or unsafe act.

25. Loop 1 is the minimum requirement for any SIS and constitutes the reporting of accidents and undesired incidents. However, this post-reporting does not allow the prevention of the initial accident and is often relatively ineffective in preventing future accidents as the information furnished may only contain statistics which provide little insight into solving systemic safety issues. Loop 2 is less frequently implemented and relies upon the frank and timely reporting of unsafe acts or near misses. However, as unsafe acts are normally the precursors to accidents, Loop 2 can contribute to proactive safety control. Loops 3 and 4 are the ones which can be most effectively used for effective pro-active safety management as they identify hazardous situations early in the causal chain. This is an important concept in the Simulation environment where it must be appreciated that accidents can be caused by not only technical accidents, but also by flawed decisions at any stage of the specification, acquisition and operation chain.

26. Fundamental to this model is the concept that there are two main failure classifications used – active and latent. When designing, constructing or operating simulations it is important to understand these two different ways in which hazards can be introduced into a system.

- a. Active failures are defined as errors or violations which have an immediate adverse effect. Active failures are usually associated with the actions of people within the system. Active failures are often introduced into systems when unauthorised decisions are made, or system changes are made without undergoing proper review.
- b. Latent failures are decisions or actions which lead to circumstances that have no immediate effect. They produce situations which may lie dormant for long periods of time until a local triggering action causes an accident or incident to occur. Latent failures are most commonly introduced into a system by people removed from its immediate operation, such as designers and high-level decision makers.

⁵ Reason, James., Human Error, Cambridge University Press, Cambridge, UK, 1990.

2.4 RISK MANAGEMENT AND CONTROL

27. Once risks are identified there are a number of measures which can be used to eliminate, reduce or manage them. Figure 2-6 illustrates a simple indicative risk treatment process. Obviously, the most desirable course of action is to eliminate or reduce the hazard through design, however if this cannot be achieved there are several options to control the risk. These include methods such as providing safety devices, providing warning devices, or through the training of system users.

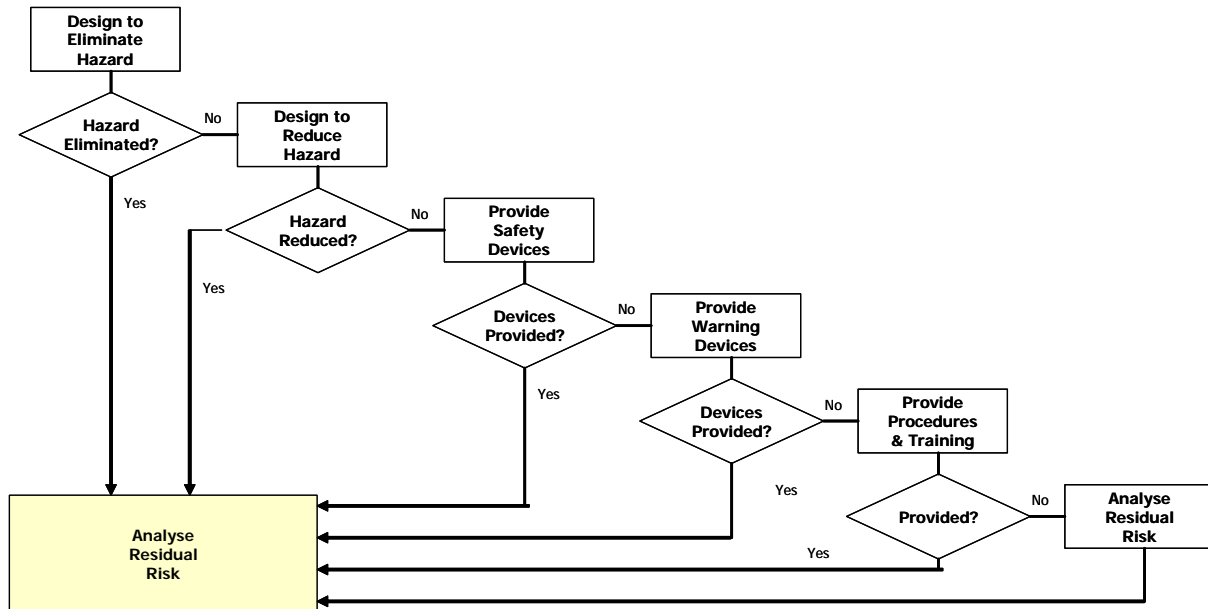


Figure 2-6: Risk Reduction Flowchart

28. However, once the identified risks have been eliminated or dealt with to the maximum extent possible some will ultimately remain. These are referred to as residual risks and will be passed onto the Simulation system owner for acceptance and management.

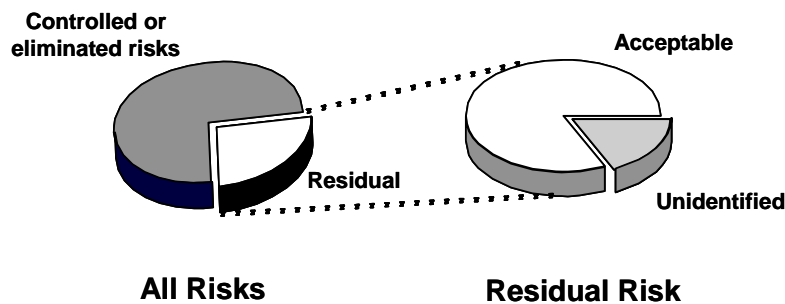


Figure 2-7: Transfer of Acceptable and Unidentified Risks

29. As shown in Figure 2-7, these residual risks will be a combination of those identified risks which are deemed acceptable (or simply unreducible) and a number of further risks which have remained so far unidentified. Where known risks are passed onto a user, the key point is for them to be documented and communicated to the user, who will need to manage them.

3 THE DEFENCE SAFETY MANAGEMENT CONTEXT

3.1 LEGISLATION AND DEFENCE SAFETY POLICY

30. The Commonwealth Occupational Health and Safety (OHS) Act forms the capstone safety legislation for the ADO.

31. The commitment of the Department to observance of the Act is expressed in the ADO Occupational Health and Safety Policy Statement. Issued jointly by the Chief of the Defence Force and the Secretary in November 2002 this statement mandates that every person in the ADO has a duty of care in regard to safety and that it is a fundamental element of leadership to look after the well being of their people. They reinforced their commitment to creating a culture where the health and safety of everyone in Defence was of fundamental importance in every workplace and business process. Further, they directed that health and safety were to be integrated into all Defence activities and that these strategies were to be integrated with other management functions.

32. Other specialist legislation mandates additional requirements in different environments, and will be applicable to simulation activities conducted within them. For example, safety at sea is governed by regulations issued under the Navigation Act 1912, airworthiness is governed by the Air Navigation Act 1908.

33. In addition to this legislative and policy framework governing the safety of people, there is also a body of regulation which ensures the technical integrity of materiel in all the Defence environments. These Technical Regulatory Frameworks (TRF) mandate system safety requirements, even when danger to personnel is not necessarily involved. They establish systems to ensure materiel acquired and operated by the ADF is both safe and fit for purpose.

34. This combination (and overlap) of Technical Regulation and OHS guidance and their hierarchy is illustrated in Figure 3-1.

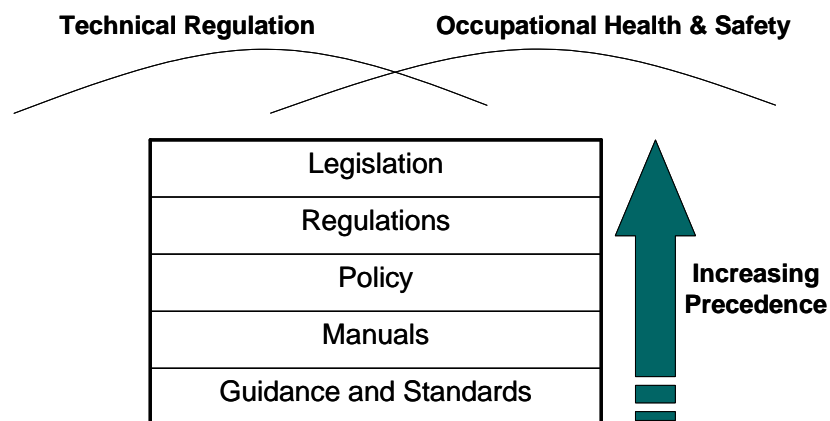


Figure 3-1: The Technical Regulatory and OHS Framework

35. Some Defence safety and technical regulatory policy relevant to Simulation includes:
- a. The Occupational Health and Safety Manual (OHSMAN)
 - b. The Defence Occupational Health and Safety Manual (DOHSMAN)

- c. The Defence Safety Manual Series (SAFETYMAN).
- d. DI(G) PERS 19-2 Occupational Health and Safety (Commonwealth Employment) Act 1991 Implementation within the ADF.
- e. DI(G) PERS 19-5 Notification of Casualties and Dangerous Occurrences in the Defence Organisation.
- f. DI(G) PERS 19-20 Occupational Health and Safety – Contractor Safety Management.
- g. Australian Army Manual of Occupational Health and Safety – edition 3.

3.2 FRAMING REGULATIONS, GUIDANCE & STANDARDS

3.2.1 Regulations, Procedures and Instructions

36. The ADO OHS Policy Statement forms the basis of safety policy for the ADO. Enacting this statement, and guiding the Defence Organisation in the application of relevant legislation are a number of Defence and externally produced documents. Some of the documents most relevant to Simulation are:

- a. Civil Aviation Safety Authority Civil Aviation Safety Regulations 1998 Part 60 Synthetic Training Devices
- b. DI(G) LOG 08-15 Regulation of Technical Integrity of Australian Defence Force Materiel.
- c. DI(N) LOG 47-3 Technical Regulation of Navy Materiel
- d. DI(A) LOG 12-1 Regulation of the Technical Integrity of Land Materiel
- e. AAP 7001.053 Technical Airworthiness Management Manual (TAMM)
- f. ABR 6492 Navy Technical Regulations Manual
- g. Technical Regulation of Army Materiel Management (TRAMM)

37. The structure of the top level Defence technical regulations can be seen in Figure 3-2.

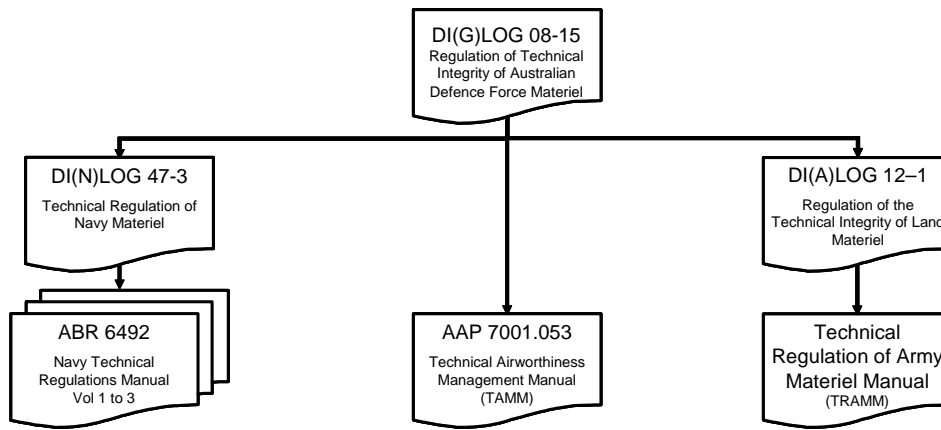


Figure 3-2: High Level Defence Technical Regulatory Documents

3.2.2 Standards and Guidance

38. Although there are a multitude of system safety standards throughout the world, a small number of the documents most applicable to Simulation are included here:

- a. Materiel Acquisition and Sustainment Framework SAMS Systems Safety Guide
- b. DEF (AUST) 5679 The Procurement of Computer Based Safety Critical Systems
- c. MIL-STD-882D, US DoD Standard, Department of Defense Standard Practice For System Safety
- d. MIL-STD-882C, US DoD Standard, Military Standard, System Safety Program Requirements (Superseded by MIL-STD-882D)
- e. ISO/IEC 15026:1998 Information Technology - System and Software Integrity Levels
- f. AS/NZS 4360:2004 Risk Management
- g. HB 436:2004 Risk Management Guidelines Handbook
- h. AS/NZS 3931:1998 Risk Analysis of Technological Systems – Application Guide
- i. Def-Stan-56, UK MoD Standard, Safety Management Requirements For Defence Systems
- j. FAR 25.1309, Federal Aviation Regulation, Airworthiness Standards: Transport Category Airplanes
- k. FAR 23.1309, Federal Aviation Regulation, Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes
- l. RTCA/DO-178B Software Considerations in Airborne Systems and Equipment Certification

3.3 KEY ISSUES FOR SIMULATION SAFETY

39. There is a large body of safety guidance available for application in the Simulation domain. Some of this includes mandatory legislation, other high level policy guidance, and a further body of standards and manuals. The key safety issues that these raise for Simulation safety are:

- a. Only authorised individuals can make judgements regarding matters concerning simulation safety
- b. All simulation systems should be viewed as safety critical unless they are demonstrated not to be.⁶
- c. Synthetic environments can introduce their own hazards such as simulation sickness and negative training transfer.
- d. A large number of safety support and advisory networks exist within and outside the ADO.
- e. Hazards can be introduced into a Simulation system through either active or latent failures.
- f. During distributed simulation the diverse nationality and backgrounds of participants can mean they have different safety standards, perceptions, safety attitudes and technical capabilities. This can lead to hazards flowing through the simulation systems.
- g. When reusing simulation components or software a careful assessment must be made of their fitness for the new purpose and their interactions with the new systems other components.

⁶ DEF(AUST) 5679 *The Procurement of Computer-Based Safety Critical Systems*. This standard mandates that unless a software system can meet very specific criteria it is to be considered safety critical unless demonstrated otherwise through the conduct of a Preliminary Hazard Analysis.

4 OVERVIEW OF SAFETY MANAGEMENT THROUGHOUT THE CAPABILITY LIFE CYCLE FOR SIMULATION

4.1 OVERVIEW OF THE CAPABILITY LIFE CYCLE

40. Systems which provide capabilities to the ADF are referred to as capability systems and as they are acquired and operated, they progress through the capability systems life cycle, which is comprised of five main phases. The process is initiated by the identification of a need for a new capability and proceeds through the acquisition, in-service support and ultimate disposal of the capability.

41. Simulation Safety needs to be considered throughout the complete life cycle of any Simulation Capability. The reference model utilised by Defence, which applies equally to all capabilities, including any Simulation Capabilities, comprises of five main phases (Figure 4-1) extending from an initial needs identification phase, through requirements definition, acquisition, in-service operation and eventual disposal.

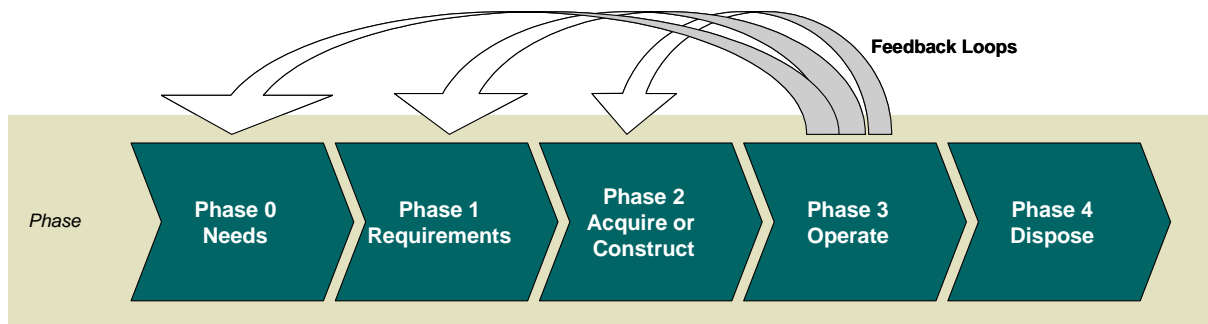


Figure 4-1: Capability Systems Life Cycle

42. In addition to considering the need for safety management during the acquisition and operation of Simulation systems, it is also important to note the contribution that Simulation can make during the life cycle of other systems.

4.2 KEY SAFETY MANAGEMENT ACTIVITIES

43. Many safety related tasks will need to be undertaken during the life cycle of a Simulation system. These range from initial safety planning through to test and evaluation activities and the safety activities required during the eventual disposal of the system.

44. These safety management activities need to be conducted throughout all the phases of a simulation capability's life cycle. The different safety management activities which should be conducted at different stages of a capability system's life cycle are described in Table 4-1.

45. Experience in other industries and lessons learned in investigation of military and aircraft accidents have emphasized the importance of managing safety in an explicit, systematic and proactive manner.

- a. Explicit means that all safety management activities should be documented, visible and performed independently from other management activities.

- b. Systematic means that safety management activities will be in accordance with a pre-determined plan, and will be applied in a consistent manner throughout the organization.
- c. Proactive means the adoption of an approach which emphasizes prevention, through the identification of hazards and the introduction of risk mitigation measures before the risk-bearing event occurs and adversely affects safety performance.

Specific Safety Activities to be Conducted by Capability Life Cycle Phase				
Phase 0 Needs	Phase 1 Requirements	Phase 2 Acquire or Construct	Phase 3 Operate	Phase 4 Dispose
<ul style="list-style-type: none"> • Develop risk evaluation criteria • Set safety targets • Establish safety management agencies and frameworks • Identify external audit responsibilities • Define system operating environment and concepts • Draft T&E safety concepts and plans • Define pre-existing sub-contractor arrangements, including safety conditions. • Establish hazard tracking standards and frameworks • Establish safety analysis standards and frameworks • Define safety equipment standards • Establish safety training frameworks 	<ul style="list-style-type: none"> • Capture Defence Safety Policy in requirements • Set project safety targets • Establish system safety management committee • Draft System Safety Management Plan • Form Project System Safety Committee • Establish Project System Safety Manager • Refine system operating environment and concepts • Develop system safety case • Conduct preliminary design review • Develop system T&E safety plans • Determine key safety parameters to be subject to T&E 	<ul style="list-style-type: none"> • Establish compliance with Defence requirements • Refine System Safety Management Plan • Conduct critical design review. • Conduct safety review of Engineering Change Orders • Establish system hazard control measures • Conduct safety T&E activities • Acquire training systems and documentation • Conduct safety training prior to system implementation • Audit sub-contractor safety programs • Assess tenderer's safety experience • Develop hazard tracking log 	<ul style="list-style-type: none"> • Monitor Defence safety policy for change • Verify controls are in place • Audit safety plan • Maintain system safety case • Conduct safety review of Engineering Change Orders • Conduct system change hazard analysis. • Conduct ongoing safety T&E activities to support through life management • Undertake safety continuation training. • Update and maintain safety training. • Monitor contract and system change proposals. • Maintain visibility of hazards subsequently identified. • Update and maintain hazard log • Manage hazards and 	<ul style="list-style-type: none"> • Establish disposal plans compliance with Defence requirements • Verify disposal method is in accordance with safety plan requirements • Review disposal sub-contractor's safety plan • Archive hazard log • Document any hazardous materials or pollution generated by the system. • Conduct safety analysis of disposal plan • Dispose of safety equipment appropriately

Specific Safety Activities to be Conducted by Capability Life Cycle Phase				
Phase 0 Needs	Phase 1 Requirements	Phase 2 Acquire or Construct	Phase 3 Operate	Phase 4 Dispose
	<ul style="list-style-type: none"> • Define system safety training requirements • Define sub-contractor safety management requirements • Ensure requirements are in tender documents • Develop preliminary hazard list • Conduct preliminary system safety assessment • Define system safety equipment requirements 	<ul style="list-style-type: none"> • Identify residual risks • Establish system safety reporting mechanism and criteria • Evaluate and manage system risks • Evaluate and manage system external interface risks • Identify and acquire safety equipment 	<ul style="list-style-type: none"> • residual risks • Evaluate and manage risks • Conduct mishap investigations • Inspect safety equipment • Monitor safety equipment standards changes 	

Table 4-1: Safety Management Activities at Different Stages of the Capability System's Life Cycle⁷

⁷ These activities have been drawn from a number of sources including the SAMS Systems Safety Guide and Bahr, N.J. *System Safety Engineering and Risk Assessment: A Practical Approach*.

5 SIMULATION SAFETY RISK FACTORS, CASE STUDIES & LESSONS LEARNT

46. The Hazards and Risks presented by a Simulation system will depend upon the nature, scale, scope and complexity of the Simulation, but can be broken into two broad types. The first of these are the risks to simulation participants by the synthetic environment itself. Typical examples include the hazards posed by pyrotechnics and lasers, the sickness which can be induced by immersive synthetic environments, and the threat posed by gasses and toxic substances during simulated damage control training. The other broad class of risks are those posed when the synthetic environment interacts with the real one to leading to confusion and possible unintended consequences. A typical example would be the launch of a real missile based upon simulated threat data.

47. Simulation systems can be generally divided into three classes – Constructive, Virtual and Live depending upon whether the human and equipment components are real or simulated. The differentiation of these three categories is explained in Figure 5-1.⁸

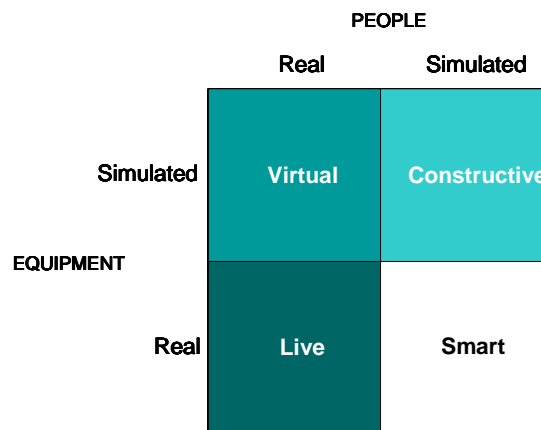


Figure 5-1: Classes of Simulation

- a. **Constructive Simulations.** In constructive Simulations individual generally stimulate (make inputs to) the constructive Models but they are not directly involved in determining the outcomes of the Simulations. Constructive Simulations are used typically in situations, such as combat engagement Simulations for example, where participants seek to achieve a specified military objective given pre-established resources and constraints. They may also use engineering, cost and support Models. Examples include wargames, models and analytical tools.
- b. **Virtual Simulations.** Virtual Simulations inject humans in the loop to exercise motor control, decision-making, or communications skills. The human element of a virtual Simulation is not modelled. The simulated systems in virtual Simulation would be made up of constructive Models. Examples include individual aircraft (or weapon system) simulators and virtual prototypes.

⁸ Definitions taken from Australian Defence Simulation Glossary

- c. **Live Simulations.** Traditionally having a training focus, live simulations represent military operations using military personnel and equipment in which simulated experiences are achieved using near-combat conditions. The advances of computer-based simulation support is enriching this field, enabling real time data collection and exercise control, including the real-time insertion of virtual simulations to stimulate live responses (eg; computer controlled targets on live-firing ranges, EW threat/missile engagement scenarios).
- d. **Smart Simulations.** Systems of simulated people and real equipment. For example, DSTO has completed several projects on penetrating injuries where simulated-instrumented people (ie; dummies) were exposed to live fire.

48. A further significant group of simulations is referred to as distributed. They are a synthetic environment within which humans may interact through Simulation at multiple sites networked using compliant architecture, modelling, protocols, standards and databases. Distributed simulations may be live, virtual, constructive or a combination of the above.

49. The safety of software intensive systems (of which Simulation systems and synthetic environments routinely depend) can be particularly difficult to determine. The flexibility of modern programming languages and the processing power of modern hardware elements mean that a high level of complexity is easily introduced. This can make it harder to predict the behaviour of equipment under software control. Further, these systems are superficially easier to modify, making hazards introduced by uncontrolled or unassessed system configuration changes more likely.⁹ Accordingly, any Safety Case for a software intensive or controlled system should explicitly consider the software safety aspects of the system.

5.1 SAFETY IN LIVE SIMULATION

50. Live simulations combine real people with real equipment. As such this form of activity presents many of the same hazards as does real operational activity. The synthesizing of additional aspects of the activity can introduce further complexity, again increasing the opportunity for compromise of safety.

5.1.1 Key Contributors to Safety Risks

51. Table 5-1 lists some of the hazard inherent in Live Simulation and an example of each.

Table 5-1: Key Live Simulation Hazards and Examples

Hazard	Live Simulation Example
Explosives and pyrotechnics	Grenade simulators
Live or blank ammunition	Blank ammunition
Flammable or explosive fuels	Vehicle fuel tanks or bladders
Toxic or corrosive substances	Confined spaces fire fighting training
Lasers	Laser rangefinders or designators
Ionising radiation	Radar systems
High pressure gas or liquid	Hydraulics or compressed air
Moving machinery and vehicles	Moving armoured vehicles

⁹ DEF(AUST) 5679 *The Procurement of Computer-Based Safety Critical Systems*, pp 7-8.

Hazard	Live Simulation Example
Activities conducted at heights	Fast roping or rope insertions
Activities conducted underwater	Underwater mine countermeasures training
High voltage electricity	Power cables
Flying vehicles	Target drone systems
Excessive noise exposure	Pyrotechnic simulators
Negative training transfer	Skills and responses taught in the synthetic environment produce different effects in the real world. This may cause hazards and accidents.
Confusion between real and simulated environments	Confusion between real and simulated activity caused by leak-through from simulated to operational systems or the failure to purge live systems of simulated data.

5.1.2 Key Mitigation Measures

52. Mitigation measures can be put in place during Live Simulation to remove or reduce these Hazards. Table 5-2 provides examples of some possible Hazard mitigation measures.

Table 5-2: Key Live Simulation Hazards and Mitigation Measures

Hazard	Example Mitigation Measures
Explosive Ordnance (EO) and pyrotechnics	<ul style="list-style-type: none"> All items of EO to be assessed as being safe and suitable for service prior to acquisition Personnel training and certification Range safety procedures
Live or blank ammunition	<ul style="list-style-type: none"> Personnel training and certification Range safety procedures
Flammable or explosive fuels	<ul style="list-style-type: none"> Spill clean up kits and training Personal Protective Equipment (PPE) Warning signs and devices
Toxic or corrosive substances	<ul style="list-style-type: none"> PPE Environmental Health assessments Containment facilities and equipment Safety barriers and access controls
Lasers	<ul style="list-style-type: none"> Range safety templates Protective eye-wear
Ionising radiation	<ul style="list-style-type: none"> Environmental assessments Safety templates Warning signs and devices Safety interlocks on equipment Training courses Monitoring and warning devices

Hazard	Example Mitigation Measures
High pressure gas or liquid	<ul style="list-style-type: none"> • Safety interlocks on equipment • System certification, inspection and maintenance • Training courses • Warning signs and devices
Moving machinery and vehicles	<ul style="list-style-type: none"> • Range procedures • Warning devices
Activities conducted at heights	<ul style="list-style-type: none"> • Certified and inspected equipment • Training courses
Activities conducted underwater	<ul style="list-style-type: none"> • Certified and inspected equipment • Training courses • Escape devices and procedures
High voltage electricity	<ul style="list-style-type: none"> • Safety interlocks on equipment • Training courses • Warning signs and devices • Isolation and lock-out switches
Flying vehicles	<ul style="list-style-type: none"> • Aerospace equipment certification and regulation
Excessive noise exposure	<ul style="list-style-type: none"> • Personal Protective Equipment (PPE) • Warning signs and devices
Negative training transfer	<ul style="list-style-type: none"> • Simulation VV&A programs • Simulation system certification • Simulation system training audit
Confusion between real and simulated environments	<ul style="list-style-type: none"> • Simulation operational procedures • Synthetic input warning on all display and processing systems • Purging of simulated data from operational system prior to removal from synthetic environment

5.2 SAFETY IN CONSTRUCTIVE SIMULATION

53. Constructive simulations combine simulated people with a synthetic environment. Accordingly, constructive simulation presents different hazards as people (apart from those managing the simulation) are not directly participating in the simulation itself. However, the risk posed by invalid simulation outcomes can endanger those personnel and operations which rely upon them to inform real-life decision making.

5.2.1 Key Contributors to Safety Risks

54. Table 5-3 lists some of the hazard inherent in Constructive Simulation and provides an example of each.

Table 5-3: Key Constructive Simulation Hazards and Examples

Hazard	Constructive Simulation Example
Simulation fatigue	Constructive simulation can allow training activities to continue for long periods of time. This can cause fatigue and strain on the simulation operators.
Negative training transfer	Skills and responses taught in the synthetic environment produce different effects in the real world. This may cause hazards and accidents.
Invalid simulation results	The results of the simulation are used to feed safety mitigation decisions in a live system. If the simulations results are invalid, this could lead to incorrect decisions being made.
Confusion between real and simulated environments	Confusion between real and simulated activity caused by leak-through from simulated to operational systems or the failure to purge live systems of simulated data.

5.2.2 Key Mitigation Measures

55. Mitigation measures can be put in place during Constructive Simulation to remove or reduce these Hazards. Table 5-4 provides examples of some possible Hazard mitigation measures.

Table 5-4: Key Constructive Simulation Hazards and Examples

Hazard	Example Mitigation Measures
Simulation fatigue	<ul style="list-style-type: none"> • Procedures to limit individual exposure times to simulations. • Staff and supervisor training • Simulation supervisor oversight and awareness • Interlocks and warning devices on simulators to warn of excessive exposure
Negative training transfer	<ul style="list-style-type: none"> • Robust training needs analysis and design process • Simulation VV&A programs • Simulation system certification • Simulation system audit
Invalid simulation results	<ul style="list-style-type: none"> • Simulation VV&A programs • Simulation system certification • Simulation system audit • Cross check of simulation results by other means

Hazard	Example Mitigation Measures
Confusion between real and simulated environments	<ul style="list-style-type: none"> • Simulation operational procedures • Synthetic input warning on all display and processing systems • Purging of simulated data from operational system prior to removal from synthetic environment

5.3 SAFETY IN VIRTUAL SIMULATION

56. Virtual simulation exposes real people to simulated equipment or synthetic environments to develop skills or refine procedures. As with constructive simulation, there is a risk that the outcomes of the simulation will introduce risks into real life activity depending upon it. However, the emersion of people into synthetic environments can introduce its own hazards such as simulation induced sickness.

5.3.1 Key Contributors to Safety Risks

57. Table 5-5 lists some of the hazard inherent in Virtual Simulation and provides an example of each.

Table 5-5: Key Virtual Simulation Hazards and Examples

Hazard	Virtual Simulation Example
Confusion between real and simulated environments	Confusion between real and simulated activity caused by leak-through from simulated to operational systems or the failure to purge live systems of simulated data.
Simulation fatigue	Virtual simulation can allow training activities to continue for long periods of time. This can cause fatigue and strain on the simulation operators.
Invalid simulation results	The results of the simulation are used to feed safety mitigation decisions in a live system. If the simulations results are invalid, this could lead to incorrect decisions being made.
Simulator motion or actuators	Virtual simulation systems can incorporate full motion systems incorporating hydraulic or electric power. These can cause physical injuries or damage if the motion is not properly controlled.
Simulation sickness	Immersive virtual simulators can cause symptoms similar to motion sickness.
Negative training transfer	Skills and responses taught in the synthetic environment produce different effects in the real world. This may cause hazards and accidents.

5.3.2 Key Mitigation Measures

58. Mitigation measures can be put in place during Virtual Simulation to remove or reduce these Hazards. Table 5-6 provides examples of some possible Hazard mitigation measures.

Table 5-6: Key Virtual Simulation Hazards and Example Mitigation Measures

Hazard	Example Mitigation Measures
Confusion between real and simulated environments	<ul style="list-style-type: none"> • Simulation operational procedures • Synthetic input warning on all display and processing systems • Purging of simulated data from operational system prior to removal from synthetic environment
Simulation fatigue	<ul style="list-style-type: none"> • Procedures to limit individual exposure times to simulations. • Staff and supervisor training • Simulation supervisor oversight and awareness • Interlocks and warning devices on simulators to warn of excessive exposure
Invalid simulation results	<ul style="list-style-type: none"> • Simulation VV&A programs • Simulation system certification • Simulation system audit • Cross check of simulation results by other means
Simulator motion or actuators	<ul style="list-style-type: none"> • Safety interlocks on motive devices • Safe design • System inspection and maintenance • Protective barriers • Warning devices • Personnel training • Supervisor training and awareness
Simulation sickness	<ul style="list-style-type: none"> • Acclimatisation and gradual introduction to immersive synthetic environments • Medical supervision • Medication • Supervisor monitoring and awareness
Negative training transfer	<ul style="list-style-type: none"> • Robust training needs analysis and design process • Simulation VV&A programs • Simulation system certification • Simulation system audit

5.4 SAFETY IN DISTRIBUTED SIMULATION ENVIRONMENTS

59. Distributed Simulation can combine the characteristics of all other forms of Simulation, but has the additional characteristic of being conducted over a geographically dispersed area, or in distributed venues. This immediately adds to the complexity of the simulation

5.4.1 Key Contributors to Safety Risks

60. Table 5-7 lists some of the hazard inherent in Distributed Simulation and provides an example of each.

Table 5-7: Key Distributed Simulation Hazards and Example Mitigation Measures

Hazard	Distributed Simulation Example
Breakdown of situational awareness	Confusion over participant location or identity resulting in casualties from misdirected fire.
Cultural, language or technical differences between participants	In distributed simulation the participants may be of different nationalities, potentially operating from different countries and using different languages. This can cause safety risks as different standards and methods may be applied by different participants whilst managing the difference between simulated activity and real operations.
Confusion between real and simulated environments	Confusion between real and simulated activity caused by leak-through from simulated to operational systems or the failure to purge live systems of simulated data.

5.4.2 Key Mitigation Measures

61. Mitigation measures can be put in place during Distributed Simulation to remove or reduce these Hazards. Table 5-8 provides examples of some possible Hazard mitigation measures.

Table 5-8: Key Distributed Simulation Hazards and Mitigation Measures

Distributed Simulation Hazard	Example Mitigation Measures
Breakdown of situational awareness	<ul style="list-style-type: none"> • Robust communications links • Participant identification and/or location system (eg “Blue Force Tracking”) • Operating procedures to verify and validate participant and non-participant locations prior to live fire occurring. • Oversight by experienced umpiring staff to detect and warn of such confusion

Distributed Simulation Hazard	Example Mitigation Measures
Cultural, language or technical differences between participants	<ul style="list-style-type: none"> • Common synthetic operating environment procedures • Robust communications links • Common training program • Exchange program to familiarize participants with other's users systems and procedures • Common equipment and/or interface standards. • Oversight by experienced umpiring staff to detect and warn of emerging hazards
Confusion between real and simulated environments	<ul style="list-style-type: none"> • Simulation operational procedures • Synthetic input warning on all display and processing systems • Purging of simulated data from operational system prior to removal from synthetic environment

5.5 EXAMPLES OF SIMULATION SAFETY IN ADF PRACTICE

5.5.1 The AP-3C Orion Advanced Flight Simulator

62. With the upgrade of the RAAF fleet of P-3C maritime patrol aircraft to AP-3C standard the RAAF undertook to acquire an Advanced Flight Simulator (AFS) to support training of AP-3C aircrew. The AFS can be used to train flight station crews as a stand-alone simulator, or linked to either the AP-3C Operational Mission Simulator or other ADF simulators.

63. In bringing this simulator into service a number of safety issues and concerns have been identified and dealt with. These were divided into two main groups – the impact of the AFS on the safety of the AP-3C weapon system, and the safety of personnel using and working with the AFS itself.

64. The principal purpose of the AFS is to provide AP-3C aircrew training and therefore it must provide a faithful representation of the real aircraft. If flight deck instrumentation or aircraft handling characteristics differ from the real aircraft crews will be surprised when the aircraft responds in an unexpected manner when learned activities are performed. In the AP-3C AFS a number of these such effects have been identified and managed. They included issues such as the aircraft's ground and flying handling characteristics, response to control inputs, and misleading control feedback and simulated motion. The veracity of the trainer and the management of these potential negative training transfers is a major requirement in the accreditation process of the simulator. They are achieved by the conduct of proof of match testing where objective tests compare the performance of the simulator with real aircraft data.

65. In acquiring this training system, the Commonwealth required the contractor to develop a System Safety Program Plan to form a basis of understanding as to how the safety requirements of the project were to be met. In order to assure the safety of the AFS itself, a

large number of safety requirements were mandated in the acquisition contract. In many cases this was achieved by the calling out of applicable standards. An OH&S assessment of the AFS itself was also undertaken to ensure these requirements were met during the acquisition. This audit identified many issues, often relating to differences in standards between Australia and the country where the simulator was manufactured. A few of the key safety concerns requiring management included the ladders, gantries and elevated walkways surrounding the AFS, and the protection of personnel from the moving body of the simulator itself.

66. Simulation Induced Sickness is a concern for crews training in the AFS and is still the subject of ongoing study. Crews have reported the AFS causing nausea and disorientation and data is being collected to determine the extent and impact of the problem. One local safety measure already in place is that due to the disorientation that may be caused crews are not to drive motor vehicles within two hours of training in the simulator.

5.5.2 Australian Army Combat Training, Range Instrumentation and Live Instrumentation System (CTC-LIS)

67. The Australian Army has identified that training leaders and soldiers to overcome the rigours of battle is its greatest responsibility.¹⁰ To be effective, combat training must be rigorous, realistic and thorough. To the extent possible, combat realism during training should approximate war's enduring features - enemy action combined with the effects of weather, climate and terrain, danger, friction, chaos and uncertainty.

68. To this end, the ADF initiated the procurement of the Combat Training Centre Live Simulation, Range Instrumentation and Information System (CTC-LIS) – Project Land 134. The CTC(L)'s mission is to train Battle Group and Combat Team sized forces as combined arms teams for force on force combat in a realistic joint environment. The high-level CTC-LIS concept is depicted below in Figure 5-2.



Figure 5-2: CTC-LIS Concept

69. The CTC-LIS will be used to generate rigorous battlefield situations, and to provide realistic battle stresses during force-on-force engagements using the full spectrum of Army

¹⁰ Commonwealth of Australia (Australian Army), *Land Warfare Doctrine 1: The Fundamentals of Land Warfare, (LWD-1)* Published by Doctrine Wing CATDC, Puckapunyal, 1998, p. 5-10. To be updated during 2001.

equipment and will employ pyrotechnics for battlefield effects and laser devices and sensors to simulate firing of weapons.

70. The key safety hazards identified for the project include:

- a. Use, storage and transport of pyrotechnics to create battlefield conditions. Pyrotechnics will be used to simulate battlefield effects which will be mounted on vehicles and positioned throughout the training area for simulating mine field and indirect fire weapon effects. The safety objectives of the project in terms of pyrotechnics, smoke and flares is that devices employing these capabilities shall be non-toxic or low-toxicity, and safe for personnel within ten metres.
- b. Use of lasers and Radio Frequency (RF) emitters for the instrumentation system which will be hoisted on players, vehicles and weapons. Where hit/miss signalling devices are fitted to equipment, these must be positioned such that they do not reduce the inherent safety of that equipment or restrict the functioning of that equipment. One the challenges to the issue of safety at the onset of the program was the potential use of lasers in the training area. A conscious decision was made at the start of the acquisition program that it was essential that all laser devices were Class 1 Lasers meeting the appropriate Australian standards. The project office found that many providers of laser equipment for simulation offer Class 1 compliant laser systems, but to international standards which are not acceptable to Australia.
- c. The ability of the instrumentation system to adequately track the forces in the play space so that training forces are not exposed to the firing of pyrotechnic devices for simulated mines and indirect fire. Position location of players must be sufficiently accurate to allow realistic 'triggering' of area weapons (which includes the requirement to enable a path to be cleared through minefields), and to maintain safety of all participants.

71. The project strategy to minimise any potential safety risks is to strictly adhere to the certification processes required as part of the ADF regulatory environment and extant safety polices for certification of pyrotechnics and laser devices. The capability will need to fulfil the requirements of these regulations and policies prior to its operational employment.

5.5.3 RAN Guided Missile Frigate Embedded Simulation Capability

72. To be completed. This section will discuss the safety management issues pertaining to the FFG Embedded simulation capability.

5.5.4 Future Combat Aircraft Aircraft Embedded Simulation and Training (ES&T) Capabilities

73. Embedded Simulation and Training (ES&T) is a concept which is gaining increasing interest with military forces. In the context of combat aircraft ES&T is intended as *“the creation of a simulated or virtual environment in order to permit more realistic and effective training on operational aircraft as well as the addition of simulated weapon systems (sensors/functions/weapons) in order to allow training without the use of real and expensive*

sensors/functions on training aircraft”¹¹ (Concept illustrated in Figure 5-3). Initial work has been conducted in demonstrating this capability in assets such as the Aeromacchi training Aircraft and the Eurofighter, and the future ADF Joint Strike Fighter may also employ this form of capability.



Figure 5-3: Aircraft Embedded Simulation and Training Concept

74. For any capability designed into an aircraft platform safety is of paramount importance and airworthiness regulations need to be strictly adhered to. Some of the safety issues that have been identified from some early work in this area include:¹²

- a. Simulation can only be executed within a well defined and controlled training area, with aural and visual warnings when training area limits are approached.
- b. Simulation cannot be operated during takeoff and landing phases or when real armament is being carried.
- c. Visual indication that the on-board simulation is active will be visible to the pilot.
- d. Control of the Man-Machine Interface is kept by the aircraft mission processor
- e. In case of any failure, the displays will return to a normal flight state.

¹¹ EUCLID CEPA Defence Modelling and Simulation Technologies, Research and Technology Paper RTP 11.12, “In-Flight Demonstration of Embedded Simulation for Training Purposes On-Board Fighter Aircraft”, Klaus H. Bartoldus

¹² EUCLID CEPA Defence Modelling and Simulation Technologies, Research and Technology Paper RTP 11.12, “In-Flight Demonstration of Embedded Simulation for Training Purposes On-Board Fighter Aircraft”, Klaus H. Bartoldus

6 SPECIALIST SIMULATION SAFETY TOPICS

6.1 SIMULATION FOR SAFETY CRITICAL SYSTEM DESIGN & VERIFICATION

75. The design, development and testing of complex military systems can be expensive and time consuming. For example, an air to air missile system may need to be tested and evaluated against many thousands of parameters such as target height, target signature, target manoeuvre, background environment, launch height, and countermeasures employment. If these were all to be investigated by actual missile firings, the cost would be prohibitive. Further, where the equipment to be tested is safety critical, it may simply be too dangerous to test the actual system during development.

76. Simulation is one method that can be used to verify and study the performance and operation of safety critical systems. This has obvious advantages in allowing system performance to be determined without the potential for accident inherent in the test and evaluation of safety critical systems. This not only reduces the likelihood of human casualties and equipment damage, but can also lead to testing efficiencies and economies.

77. The key determinant in how effectively a Simulation can be used to validate and verify a corresponding physical system is the degree to which the Simulation maps the actual system. It is also important to note that when a Simulation is used to assist in the VV&A of a safety critical system, the Simulation itself must be certified to the same levels of integrity.

78. One novel application of modelling and simulation during safety critical design is the Exodus Simulation used to predict and model passenger evacuation from mass transport vehicles. Since 1965, international regulations have required aircraft manufacturers to demonstrate that their cabin designs allow a full load of passengers to be evacuated within 90 seconds. This must occur in the dark, with only half the exit doors available and the participants representing a genuine cross section of the travelling public. However, between 1972 and 1991 6% of the volunteers participating in such trials have sustained injury. Further, the trials are expensive with a typical wide bodied aircraft evacuation trial costing in excess of \$US2 million. By replacing some of the live tests and trials with modelling and simulation, the Exodus program assists in the development of this safety critical capability, whilst minimising cost and injury.

79. The Exodus Simulation is expert system based with the progressive motion and behaviour of each passenger determined by a set of heuristic rules. Existing information on human behaviour in emergencies is comprehensive, but as little of this directly relates to transport emergencies the program allows users to modify simulated participant's behaviours to allow for new data or theories. The Simulation itself employs a two dimensional grid in which the vehicle's interior is mapped and a master system clock against which activities progress. Passengers are defined by submodels and are susceptible to incapacitation by toxic gases or heat.

80. The continued use of the program in different transport scenarios and its validation against hopefully less frequent live tests will improve the models used and its subsequent veracity.¹³

¹³ The University of Greenwich, Fire Safety Engineering Group,
<http://www.greenwich.ac.uk/~lp03/firegroup.old.html>

6.2 THE ROLE OF VV&A IN SIMULATION SAFETY

81. The purpose of verification, validation and accreditation is to assure the development of correct and valid Simulations and to provide Simulation users with sufficient information to determine if the Simulation can meet their needs.¹⁴ One of these requirements will be System Safety.

82. During the requirements definition phase of a Simulation system acquisition safety targets will be set. These will specify the acceptable mishap rates and the minimum level of assurance and confidence required of the various system elements. In complex distributed systems, or systems employing potentially lethal effects such as pyrotechnics, these safety expectations are likely to be very high. In some cases formal levels of system safety and integrity can be specified using existing frameworks and standards. One such metric is Software Integrity Levels (SIL) which are defined in ISO/IEC 15026-01. This International Standard introduces the concepts of SILs and software integrity requirements. It defines the concepts associated with integrity levels, defines the processes for determining integrity levels and software integrity requirements, and places requirements on each process. This International Standard does not prescribe a specific set of integrity levels or software integrity requirements. These must be established either on a project by project basis, or for a specific sector and/or country.

83. The design and development of the Simulation system will then be an iterative process in order to meet these targets. VV&A will be used during this process to determine if the system, and its various sub-components, actually perform in accordance with the design specification. The quantity and nature of the VV&E required will be determined, in part, by the safety and integrity required from the Simulation system in question. Elements which fail test or do not meet their design intent will need to be redesigned, rebuilt or recoded. Once the development process is complete and the system is entering service, the results of the VV&A process are likely to form an essential element of any certification basis required for the system.

6.3 HUMAN FACTORS AND SIMULATION SAFETY

84. Human factors impinge on Simulation safety in two key ways. Firstly, there is the likelihood that human actions or inactions will cause the Simulation environment to present a hazard. An example of this would be a pyrotechnic grenade simulator used in a live simulation. If actuated by an operator in too close proximity to a Simulation participant, that device could cause injury or harm. Secondly, the Simulation environment may be hazardous through insufficient consideration of human factors design. As an example, a virtual Simulator with exposed machinery or electrical wiring used for training tank crews could cause injury to users if these hazards are not properly addressed.

85. The likelihood that any given system will perform correctly is the probability that the hardware and software will perform correctly, times the probability that the operating

¹⁴ Australian Defence Simulation Office, *Simulation Verification, Validation and Accreditation Guide*.

environment will not degrade the system operation, times the probability that the user will perform correctly. By defining total system performance in this way, human performance is identified as a component of the system.¹⁵

86. Two key Simulation safety human factors issues are Negative Training Transfer and Simulation sickness and fatigue.

6.3.1 Negative Training Transfer

87. One of the key uses of synthetic environments is to provide training and to develop skills. Cockpit flight simulators, maintenance simulators and virtual command posts each teach and develop different natures of skills, some procedural, some instinctive, some conceptual.

88. Where a Simulation is to be used to provide such training, it is obviously important that what is taught is representative of the actual environment in which the user must ultimately perform. To the limits of its fidelity, the Simulation should respond to the actions of the user in the same way in which the real system does. If it does not, there is potential the user will develop skills and responses which when used for real will not have the expected effect. In this case the use of the Simulation for training could actually have a deleterious effect on the trainee's subsequent performance. This is referred to as negative training transfer.

89. Some examples of negative training transfer would be:

- a. A cockpit simulator where the switches are in slightly different places to those in the real aircraft. The student trainee instinctively learns the position of the switches in the simulator, which then causes them difficulty in a real aircraft, causing a safety hazard.
- b. A weapon system simulator which has insufficient fidelity and omits several important operator actions. The trainee learns the required system operations and when confronted by the real weapon system continues to omit those steps.
- c. A flight simulator which responds to control stick and throttle inputs differently than the real aircraft. Again, the trainee pilot will be surprised by the response of the real aircraft.

90. An effective Simulation VV&A program is the most effective means of ensuring training transfer from synthetic to real world is positive. Refer to the Defence Simulation VV&A Guide for more information on the application of VV&A to Simulation.

6.3.2 Simulation Fatigue and Sickness

91. In many cases Simulations enable training to be conducted more efficiently and economically. They also remove some of the physical limitations imposed by training with or in real platforms such as aircraft. For example, a pilot training simulator enables a student to experience and master high-risk potentially lethal scenarios with no physical risk to personnel or equipment. However, in addition to these benefits, Simulated environments can remove the normal time limitations imposed by real machinery. A flight simulator can enable a pilot to train for longer than would be possible in a real aircraft which is limited by fuel load and

¹⁵ FAA System Safety Handbook, Chapter 17, p 17-2.

maintenance turn-around times. This endurance can be a benefit, contributing to the cost effectiveness of Simulation based training, but can also place extra physiological demands on the users. Long term exposure to immersive video environments, realistic vehicle motion, and long periods of stressful battlefield decision making can be physically and mentally draining and could lead to repetitive motion injuries and eyestrain.

92. Despite the advantages of using simulators there are potential negative impacts on health, safety and training due to the development of motion sickness symptoms and other after-effects such as balance disturbances, visual stress and altered hand-eye coordination.

93. With the availability of high fidelity full-motion simulators we can train pilots and other operators presented with high risk scenarios within a safe environment. Replicated cockpits and crew stations, and artificial scene generation and motion cues, generate the power to convince the user's sensory systems that they are actually flying an aircraft or driving a tank. Unfortunately this in turn can lead to a type of motion sickness known as Simulator Induced Sickness (SIS). SIS is similar to motion sickness but usually has fewer symptoms.¹⁶

94. SIS may remain an impediment to the wide spread use of virtual environments for applications such as training, rehabilitation, and rehearsal for medical procedures and military operations. One study notes that presence of simulator sickness may prevent virtual environment technology from reaching its full potential. In their research, 30% of the participants did not complete the research because their symptoms were severe enough to retain them on site until their symptoms subsided. Symptoms tended to be predominantly oculomotor in nature (e.g., eyestrain, headaches) but also include symptoms related to nausea and disorientation.¹⁷ Subtle differences in simulator characteristics can cause significant differences in the physiological effects they cause. Almost imperceptible differences in motion or video lag can dramatically affect the amount of discomfort caused.

¹⁶ Sinclair, CAPT L., *Motion Sickness – it's in the Bag*, Touchdown The Australian Navy Safety and Information Magazine, Issue 3, December 2003.

¹⁷ Fowlkes, J., et al, *Optimising Haptics Perceptions for Advanced Army Training Systems: Impacts on Performance*, US Army Research Institute for the Behavioural and Social Sciences.

7 SIMULATION SAFETY SUPPORT NETWORK

95. As Defence is legally obliged to meet the requirements of the OHS Act, the Chief of the Defence Force and Secretary hold Commanders and Executives responsible and accountable for accidents, illnesses and injuries that occur in their workplaces. To support managers in this responsibility Defence has established a number of safety management systems and structures.

96. Specialist safety management organisations exist within Defence at three key levels – whole of Defence support agencies, Group Safety Committees, and Establishment Safety and Emergency Management Committees. In addition to these three levels of safety management there are a number of specialist agencies and Centres of Expertise (COEs).

7.1 THE DEFENCE SAFETY MANAGEMENT AGENCY

97. The Defence Safety Management Agency (DSMA) is established within the Defence Personnel Executive and is responsible for providing safety policy, guidance and expert advice to all Defence Groups. They provide guidance on matters that arise from the OHS Act, Regulations, Approved Codes of Practice and on specific safety issues.

98. DSMA is also responsible for:

- a. Providing expert advice to regional CSIG Regional Health and Safety Coordinators.
- b. Sponsoring the Defence SAFETYMAN.
- c. Sponsoring the DEFCARE safety management computer system.

7.2 GROUP SAFETY COMMITTEES

99. The Defence SAFETYMAN requires that within each Defence Group the senior executive is responsible and accountable to ensure appropriate:

- a. Safety management systems and structures are established.
- b. Resource for the management of safety management systems are allocated.
- c. Documentation systems are established.
- d. Safety training programs are established.
- e. Key safety management performance indicators are established.
- f. Safety achievements are reported for inclusion in the Defence Annual Report.

7.3 SAFETY AND EMERGENCY MANAGEMENT ACROSS ESTABLISHMENTS

100. In order to manage safety at a local level, each ADF establishment is to establish a Safety and Emergency Management Committee (SEMC) structure. The SEMCs are to:

- a. Ensure local senior management commitment and involvement in the safety management process.
- b. To preside over safety programs that aim to identify, assess and control local workplace hazards.
- c. Ensuring establishment-wide cross-organisation hazards are recognised and managed.
- d. Ensure a mix of management and employees, and military and civilian staff are represented.
- e. Hold meetings at least once every three months.
- f. Assist in the dissemination of information relating to health, safety and emergency management.

7.4 OTHER SPECIALIST AGENCIES AND COE

101. There are a number of support agencies and COE throughout the ADO and beyond who can provide specialist advice which can contribute to Simulation Safety. Some of these agencies include:

- a. The ADF Regulatory Agencies
- b. Ordnance Safety Group
- c. Navy Subsafe program
- d. Aerospace Simulation System Program Office
- e. Army Simulation Wing

8 SIMULATION SAFETY TRAINING

102. Note that there were no institutions identified at the time of writing of this guide that provided training specifically in Simulation Safety. There are a number of Defence conducted and externally conducted safety training courses that address the issue of general safety training which then need to be applied in the context of simulation safety. As a point of contact in the first instance to identify any relevant training the appropriate domain regulatory authority should be contacted as well as the Defence Safety Management Agency.

ANNEX A ABBREVIATIONS AND ACRONYMS

Acronym/ Abbreviation	Explanation
ADF	Australian Defence Force
ADSO	Australian Defence Simulation Office
CGA	Computer Generated Actors
CGF	Computer Generated Forces
COE	Centre of Expertise
COTS	Commercial-Off-The-Shelf
DI(G)	Defence Instruction (General)
DIS	Distributed Interactive Simulation
DSN	Defence Secret Network
DSTO	Defence Science and Technology Organisation
FPS	Functional and Performance Specification
ISD	Information Systems Division
JSAF	Joint Semi-Automated Forces
OHS	Occupational Health and Safety
ORBAT	Order of Battle
PHA	Preliminary Hazard Analysis
SAF	Semi-Autonomous Forces
SIMMAN	Defence Simulation Manual
SIS	Safety Information System or Simulation Induced Sickness
SPG	Simulation Proposal Guide
T&E	Test and Evaluation
TAMM	Technical Airworthiness Management Manual
TRAMM	Technical Regulation of Army Material Management

ANNEX B DEFINITION OF TERMS

Term	Definition
Fidelity	The accuracy of the representation when compared to the real world. (Australian Defence Simulation Glossary)
Hazard	A condition that is a prerequisite to a mishap. (MIL-STD-882C) Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment. (MIL-STD-882D)
Mishap	An unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. (MIL-STD-882D)
Mishap Risk	An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence. (MIL-STD-882D)
Residual Mishap Risk	The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, in accordance with the system safety design order of precedence. (MIL-STD-882D)
Safety	Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. (MIL-STD-882D)
System	An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective. (MIL-STD-882D)
Safety Case	A comprehensive and exhaustive analysis of the nature, hazards and control mechanisms of a system. It summarises the consultation, design, research, analysis, and other activities undertaken to ensure that a proposed project or system will be implemented adequately safely. The Safety Case also presents the "case" or the argument that, based on the results of this effort, the risks associated with proceeding to implement the project have been reduced to "as low as reasonably practical".
Safety Critical	A term applied to a condition, event, operation, process or item of whose proper recognition, control, performance or tolerance is essential to safe system operation or use; eg. Safety critical function, safety critical path, safety critical equipment, etc. (MIL-STD-882C)
Simulation Induced Sickness	Symptoms similar to motion sickness induced by immersive synthetic environments.
System Safety	The application of engineering and management principles, criteria, and techniques to optimise all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle. (MIL-STD-882D)

For a complete list of Simulation terms refer to the Australian Defence Simulation Glossary.

ANNEX C SIMULATION SAFETY REFERENCES

In addition to the ADO documents already mentioned in this guide, the following key references provide useful information on system and simulation safety. Hyperlinks are provided where the documents are available on the Internet.

- a. MIL-STD-882D System Safety Program Requirements (<http://www.safetycenter.navy.mil/instructions/osh/milstd882d.pdf>).
- b. Federal Aviation Authority System Safety Handbook.
- c. Defence Materiel Organisation SAMS System Safety Guide.
- d. AS/NZS 4360:2004 Risk Management (<http://www.standards.com.au>).
- e. HB 436:2004 Risk Management Guidelines Handbook (<http://www.standards.com.au>).
- f. Bahr, N.J. *System Safety Engineering and Risk Assessment: A Practical Approach*, Taylor and Francis, London, 1997.

Simulation Safety Guide Evaluation Form

Because this Guide will continue to be a 'living' document, ADSO welcomes your comments and will use the feedback to ensure that the Guide meets the needs of the audiences for which it is intended. Please take a moment to answer some or all of the five questions below. Including your name and address will be appreciated but is not necessary. Send your responses to:

Mr Darren Mc Farlane
 ADSO Navy 1
 R1-3-B066
 Phone: (02) 6265-4797; Fax: (02) 6265-2223;
 e-mail: darrenmcfarlane@defence.gov.au

* * * * *

1. According to your understanding of Simulation Safety, is any information presented in this Guide incorrect or inaccurate? (You may want to attach a copy of the page marked with your suggested changes.)

<i>Page and line number</i>	<i>What is in error in this statement or discussion, in your estimation?</i>

2. In your opinion, should any discussions in the Guide be expanded and presented in greater detail? Is any statement or discussion unclear?

<i>Page and line number</i>	<i>What unanswered question(s) do you have after reading this material? For the work you do, what additional information do you need? Is this statement or discussion unclear?</i>

3. In your opinion, should any material in the Guide be eliminated or condensed?

<i>Page and line number</i>	<i>Why do you believe these statements or discussions should be omitted or shortened? (eg, 'too detailed for my needs,' 'redundant,' 'irrelevant for my needs,' 'too elementary.')</i>

4. Did you find any typos, misspellings, or other production errors in the Guide?

<i>Page and line number</i>	<i>Error</i>

5. Do you have any other suggestions for making the Guide a more effective and usable document?

Optional	
Name	_____
Address	_____

Phone	_____
	Fax _____
e-mail address	_____

Thank you for taking the time to share your opinions with ADSO.