2º Simpósio Internacional de Confiabilidade e Gestão de Segurança Operacional

09 a 11 de novembro de 2010

DCA-BR

Organização Brasileira para o Desenvolvimento da Certificação Aeronáutica

Programas de Confiabilidade e Segurança: Semelhanças e Diferenças entre Setores

Sydnei Marssal

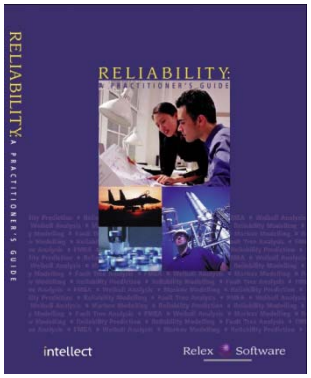
sydnei@realsafe.com.br

www.realsafe.com.br

www.relex.com

Relex Software Corporation

- Incorporated in 1986 and acquired by PTC in 2009
- Complete, truly integrated suite of reliability, availability, maintainability and safety applications
- Reliability engineering organization
  - ASQ CRE's in all departments
  - Publish technical papers and books
  - Provide training, consulting and implementation services



ASQ
AMERICAN SOCIETY FOR QUALITY

Thousands of Satisfied Customers

Aerospace and Defense Dominance

- Lockheed Martin
- General Dynamics
- Northrop Grumman
- Boeing
- Raytheon
- EADS
- General Atomics
- L3
- Sukhoi
- Tenix Defense
- Wyle Labs
- Sikorsky
- Orbital Sciences

- ITT
- Rockwell Collins
- Smiths Aerospace
- DRS
- CTC
- CAE
- Thales
- Selex
- Oerlikon Contraves
- Marshall's Aerospace
- SAIC
- Saab
- Eaton Aerospace

- BAE Systems
- Goodrich
- NASA
- Airbus
- Galileo Avionica
- Rheinmettal
- Naval Surface Warfare Center
- Honeywell
- MEADS
- MBDA
- Bell Helicopter
- Augusta Westland

Histórico: 1939 a 1945

Histórico: 1948

1948 - AEC (Atomic Energy Commision) cria o Advisory Committee on Reactor Safeguards (ACRS)

1949 - DoD publishes MIL-P-1629 FMEA/FMECA

Item	
	System
	Subsystem
	Component

Failure Mode and Effect Analysis
DFMEA / PFMEA

Process/ product name	
Core team	

Process responsibility: _____
Key date: _____

FMEA number

Prepared by	Page of
FMEA issue date	
FMEA update	Rev.

System/ Design/ Process/ Service Function	Potential failure mode	Potential failure effect(s)	S E V	C L A S S	Potential cause of failure	O C C	Current action	D E T	R P N	Recommended action	Responsibility	Completion date	Action results				
													Action taken	S E V	O C C	D E T	R P N

Histórico: 1951 a 1957

1951: 7 estudos de caso sobre a distrib. de *Weibull*

1952: DoD *c*ria o **AGREE** (Advisory Group on Reliability Electronic Equipment)

ARINC-Captura e análise de dados de campo (válvula)

Army Signal Corps, Cornel University, Vitro Corp. e Bell Labs

1953:Testes de vida de B. Epstein e M. Sobel

1954: Conferência para Qualidade e Confiabilidade

1956: RCA (Radio Corporation of America), publica seu trabalho sobre predição TR1100

Histórico: 1951 a 1957

Junho de 1957: Relatório AGREE

Reliability of Military Electronic Equipment

Fundação da disciplina de confiabilidade

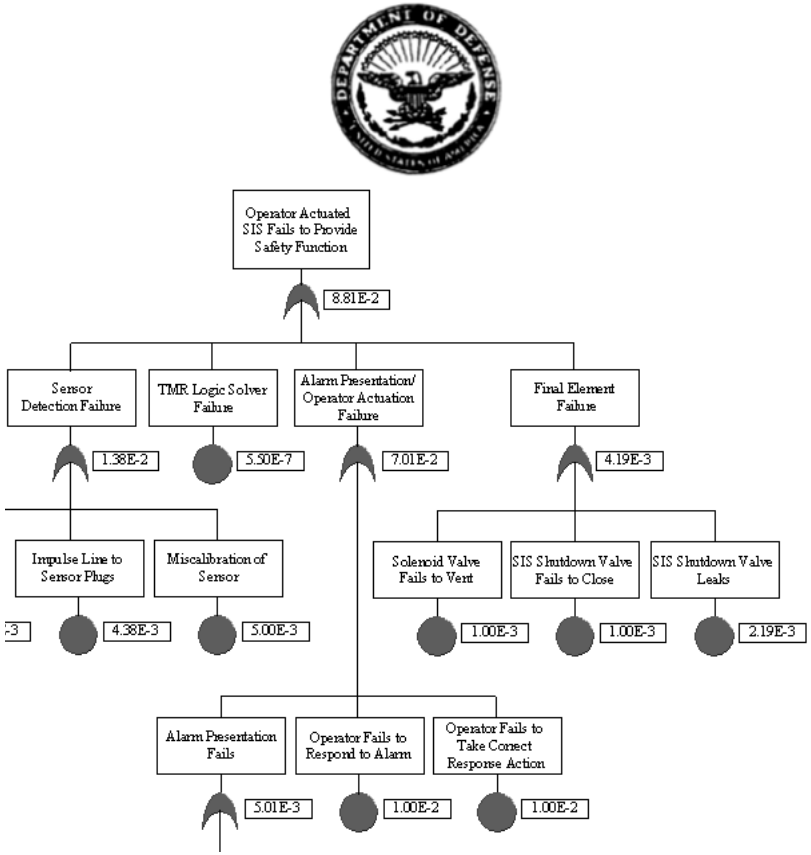
1957: 1ª planta termonuclear comercial (Pittsburgh)

WASH-740, Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants, AEC

Histórico: 58 a 69

MILITARY HANDBOOK

RELIABILITY PREDICTION OF ELECTRONIC EQUIPMENT



Histórico: Década de 70

1975: Equipe do Prof. Norman Rasmussen publica a WASH1400, Reactor Safety Study sobre **PRA**

TMI - 1979

Objetivos

1. Identificar as principais similaridades e dissimilaridades entre os programas de Confiabilidade e Segurança entre os principais setores.

2. Avaliar potencial harmonização entre os setores analisados considerando desenvolvedores de sistemas críticos embarcados

"This program was designed to help U.S. defense companies diversify their operations; the firms were encouraged to produce so-called "**dual-use**" products that could also be sold in the commercial sector."

Source: DoD Acquisition Strategy, 2002

Programas de Confiabilidade e Segurança

Espaço

Militar

Nuclear

Aeronáutico

Médico

Ferroviário

Análise dos Programas

	Space	Aeronautics	Nuclear	Military	Rail	Medical
Órgão Internacional Referência	NASA ESA	ICAO	IAEA	DoD	ERA	FDA
Documentos Internacionais Referência	NASA PRA Guide	DOC 9859 ARP 4761 ARP 5150 ARP 4754	SF-1 NSG 2.11 SSG 3 e 4 NUREG 6823	MIL STD 882 MIL HDBK 338	EN 50126	ISO 14971
Órgão Nacional Especializado	IFI	ANAC	CNEN	IFI	ANTT	Anvisa
Principais normas geradas pelo setor	YES	YES	YES	YES	NO	NO
Certificação Obrigatória	NO	YES	YES	NO	NO	YES

1. Performance Based Approach

Defense Acquisition Reform: DOD promoted performance-based contracting, as well as the use of acquisition reform "pilot" programs to test the effectiveness of some reform initiatives; one such example is mission-oriented program management.
Performance-based contracting defines work to be performed in measurable, mission-related terms.

Source: DoD Acquisition Strategy, 2002

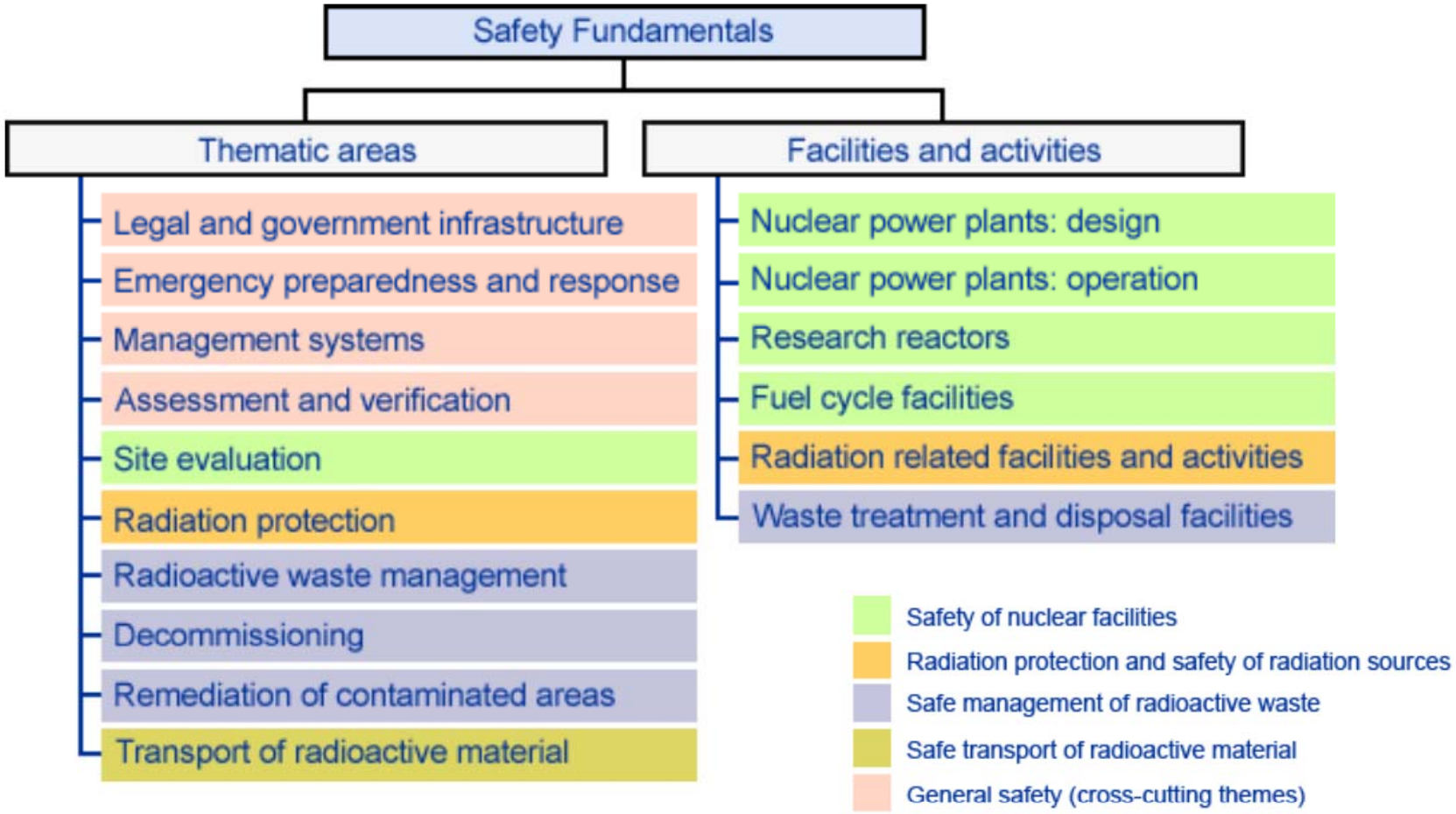
Performance-based requirements involve quantitative measures of product performance such as the number of failures over time, life expectancy, and time to repair a product within specified environmental

Source: NASA-STD-8729 Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program, 1998

2. CRM - Continuous Risk Management

Source: NASA - Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners

3. Systemic Vision



Source: IAEA Safety Standards

4. Life Cycle Understanding

PORTFOLIO	
MARKET INTELLIGENCE	BUSINESS MANAGEMENT

PROGRAM A			
Historical Data	Quality	Business Results	Requirement Monitoring
PRODUCT LIFE CYCLE MANAGEMENT (PLM)			

PROGRAM X			
Historical Data	Quality	Business Results	Requirement Monitoring
PRODUCT LIFE CYCLE MANAGEMENT (PLM)			

PRODUCT A_1	PRODUCT A_N	PRODUCT X_1	PRODUCT X_N
Requirements	Requirements	Requirements	Requirements
Project / Design	Project / Design	Project / Design	Project / Design
Manufacturing	Manufacturing	Manufacturing	Manufacturing
Distribution	Distribution	Distribution	Distribution
Operation and Maintenance	Operation and Maintenance	Operation and Maintenance	Operation and Maintenance
Disposal	Disposal	Disposal	Disposal

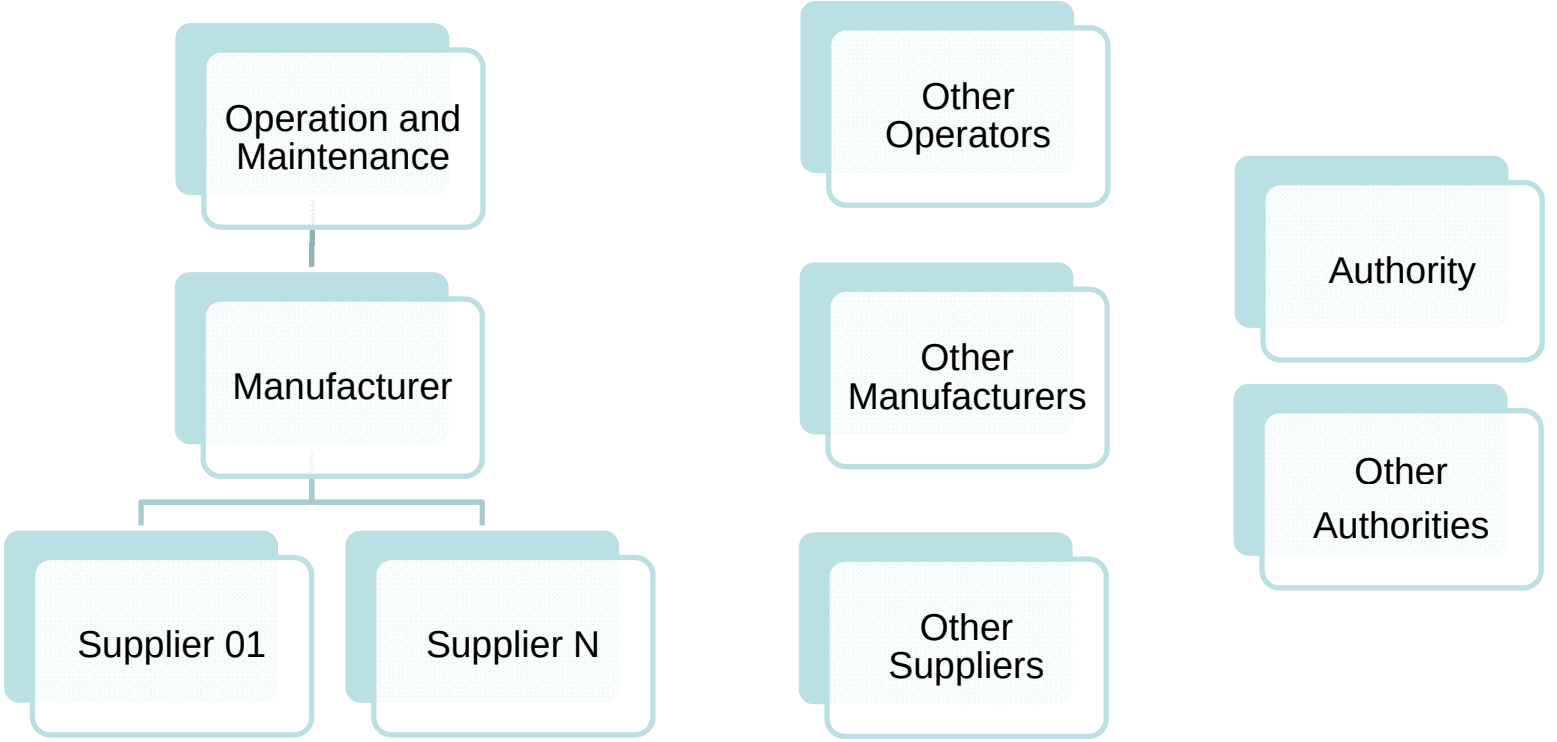
6. Human Factor Assessment

- **Human Error Risk Assessment**
- **Human Factors**
- **Human Factors Engineering**
- **Human Factors Task Analysis**
- **Human Reliability Analysis (HRA)**

Source: NASA-STD-8729 Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program, 1998

Source: NASA - Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners

7. Multi-Level Orientation



8. Multiple Scope

CONSEQUENCE CATEGORY	CRITERIA / SPECIFICS		NASA PROGRAM/PROJECT (Classes and/or Examples)	PRA SCOPE*
Human Safety and Health	Public Safety	Planetary Protection Program Requirement	Mars Sample Return	**F**
		White House Approval (PD/NSC-25)	Nuclear payload (e.g., Cassini, Ulysses, Mars 2003)	**F**
	Human Space Flight		International Space Station	**F**
			Space Shuttle	**F**
			Crew Return Vehicle	**F**
Mission Success (for non-human rated missions)	High Strategic Importance		Mars Program	**F**
	High Schedule Criticality		Launch window (e.g., planetary missions)	**F**
	All Other Missions		Earth Science Missions (e.g., EOS, QUICKSCAT)	**L/S**
			Space Science Missions (e.g., SIM, HESSI)	**L/S**
			Technology Demonstration/Validation (e.g., EO-1, Deep Space 1)	**L/S**

*Key: F – Full scope PRA is defined in Section 3.1.a of Reference 6.
L/S – A Limited scope or a Simplified PRA as defined in Section 3.1.b of Reference 6.

Source: NASA - Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners

Getting the Measure of Risk

- Potential accident sequences associated with a hazard (ETA)
- Failure Conditions (FHA)
- Determine the severity
- Two different approaches:
  - Estimate probability of accident, and hence get a measure of accident risk… then decide whether estimated risk is acceptable
    - Used in many domains, including rail, military and space
  - Establish acceptable risk, and set probability targets
    - Civil aerospace approach (ARPs etc.)

Risk Classif.: Aeronautics

Severidade	FAA	JAA	Probabilidade por hora de missão
Catastrophic	Extremamente Improvável	Extremamente Improvável	P < E-9
Hazardous	Improvável	Extremamente Remoto	P < E-7
Major		Remoto	P < E-5
Minor	Provável	Razoavelmente Provável	P < E-3
		Frequente	P < 1

Source: SAE ARP 4761

Risk Classif.: Military, Space

Frequency of Occurrence	Hazard Severity Categories			
	IV - Negligible	III - Marginal	II - Critical	I - Catastrophic
Frequent	MEDIUM	HIGH	HIGH	HIGH
Probable	LOW	MEDIUM	HIGH	HIGH
Occasional	LOW	MEDIUM	HIGH	HIGH
Remote	LOW	LOW	MEDIUM	HIGH
Improbable	LOW	LOW	LOW	MEDIUM

Source: MIL-STD-882C

Risk Classif.: Rail

Occurrence of a hazardous event	Risk Levels			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Negligible	Undesirable	Undesirable	Intolerable
Remote	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Tolerable
Incredible	Negligible	Negligible	Negligible	Negligible
	Insignificant	**Marginal**	**Critical**	**Catastrophic**
	Severity Level of Hazard Consequence			

Risk Category	Actions to be applied against each category
Intolerable	Shall be eliminated
Undesirable	Shall only be accepted when risk reduction is impracticable and with the agreement of the Railway Authority or the Safety Regulatory Authority, as appropriate
Tolerable	Acceptable with adequate control and with the agreement of the Railway Authority
Negligible	Acceptable with the agreement of the Railway Authority

Source: EN 50126 - Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

Risk Classif.: Medical Devices

ANVISA RDC n° 185/2001 - Quanto a Classe de risco:

- Classe I – baixo risco;
- Classe II – médio risco;
- Classe III – alto risco; e
- Classe IV – máximo risco.

} Requisitos Essenciais de Segurança e Eficácia de Equipamentos Médicos

Source: Manual para Regularização de Equipamentos Médicos na ANVISA, 2009

Risk Classif.: Medical Devices

ITEM	Fatores de Risco
1	Toxicidade
2	Flamabilidade
3	Incompatibilidade biológica
4	Contaminantes residuais
5	Incompatibilidade com outros materiais, substâncias ou gases
6	Infecção e contaminação microbiana
7	Incompatibilidade de combinação ou conexão com outros produtos
8	Instabilidade e limitações de características físicas e ergonômicas
9	Sensibilidade a condições ambientais

ITEM	Fatores de Risco
10	Interferência recíproca com outros produtos
11	Impossibilidade de calibração e manutenção
12	Imprecisão ou instabilidade de medida
13	Controle inadequado das radiações
14	Proteção inadequada das radiações
15	Controle inadequado de energias ou substâncias administradas
16	Proteção inadequada de energias ou substâncias administradas
17	Inteligibilidade de sistemas digitais programáveis

ITEM	Fatores de Risco
18	Instabilidade de sistemas digitais programáveis
19	Falhas da fonte de energia para funcionamento
20	Inadequação de alarmes para alerta
21	Susceptibilidade a choques elétricos

Source: Manual para Regularização de Equipamentos Médicos na ANVISA, 2009

Risk Classif.: Medical Devices

Table D.3 — Example of five qualitative severity levels

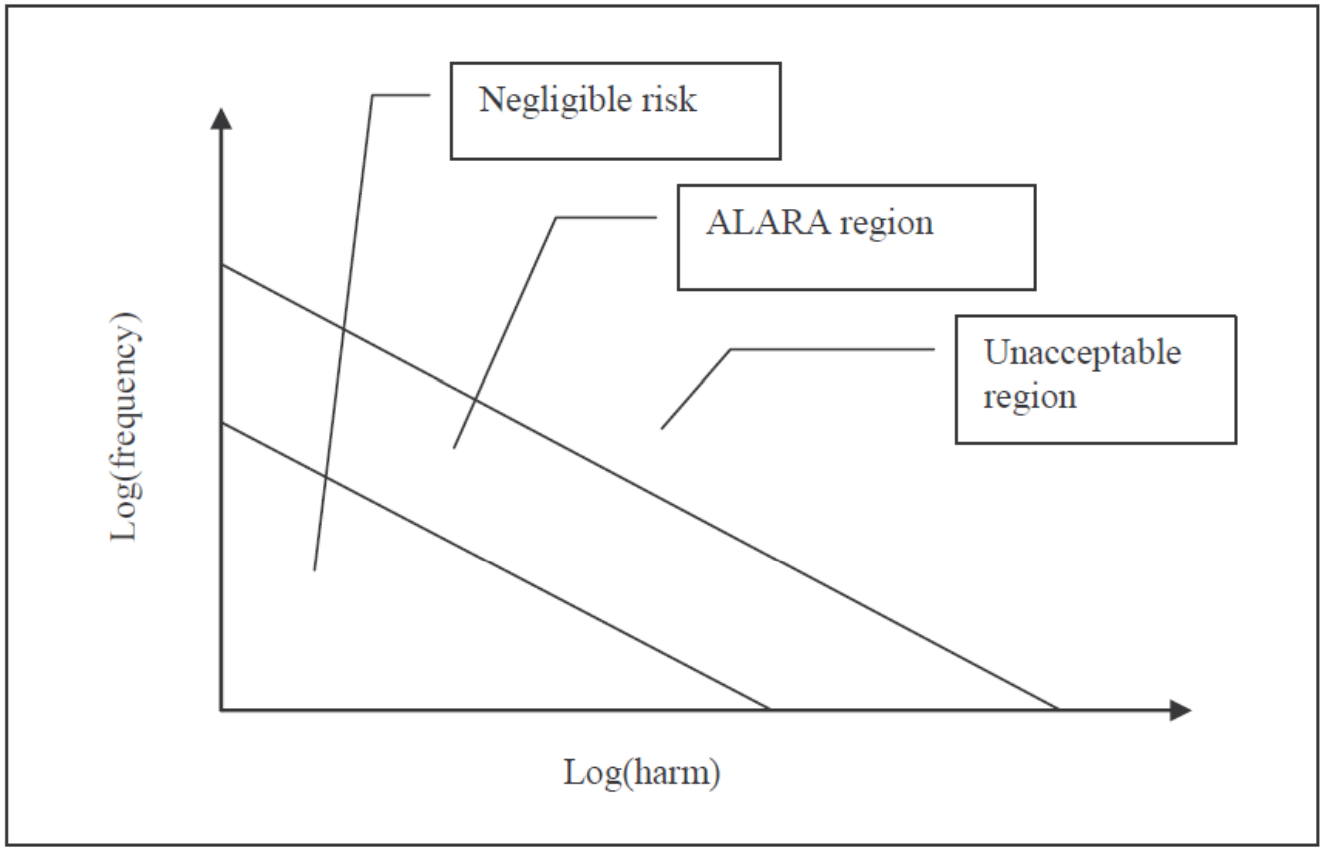
Common terms	Possible description
Catastrophic	Results in patient death
Critical	Results in permanent impairment or life-threatening injury
Serious	Results in injury or impairment requiring professional medical intervention
Minor	Results in temporary injury or impairment not requiring professional medical intervention
Negligible	Inconvenience or temporary discomfort

Table D.4 — Example of semi-quantitative probability levels

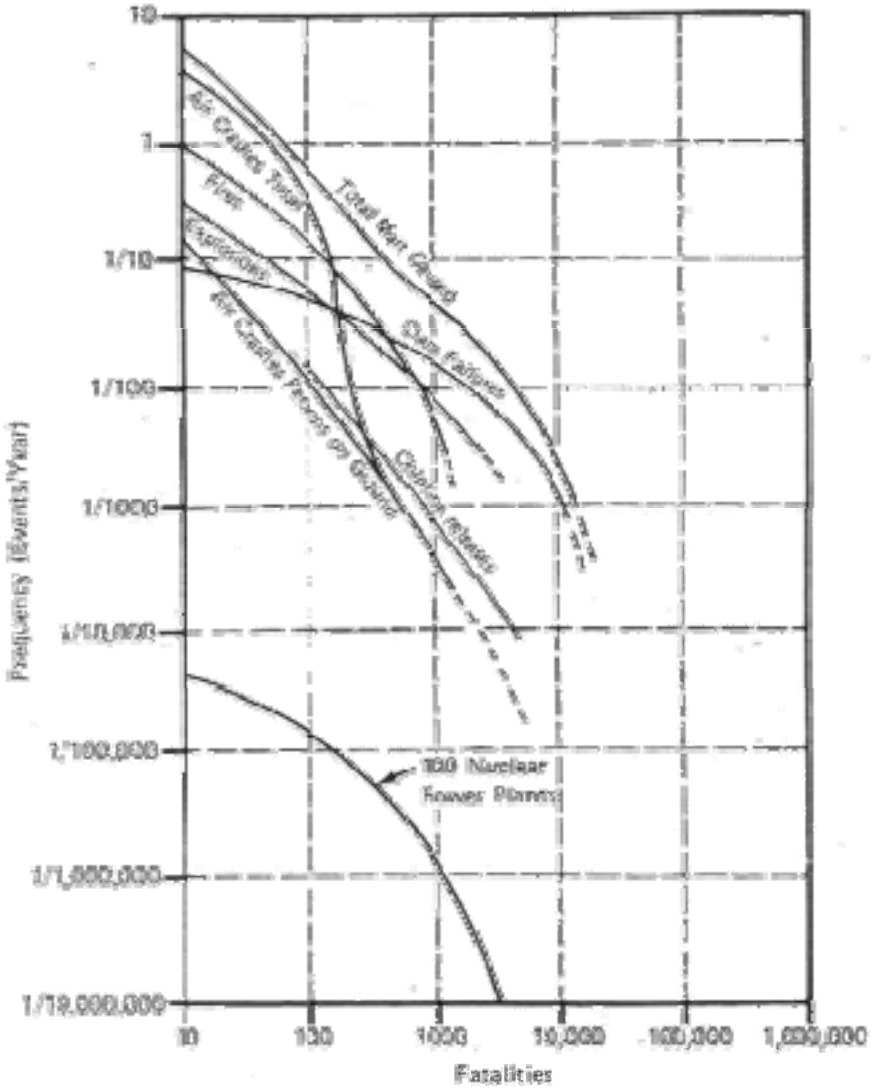
Common terms	Examples of probability range
Frequent	$\geqslant 10^{-3}$
Probable	$< 10^{-3}$ and $\geqslant 10^{-4}$
Occasional	$< 10^{-4}$ and $\geqslant 10^{-5}$
Remote	$< 10^{-5}$ and $\geqslant 10^{-6}$
Improbable	$< 10^{-6}$

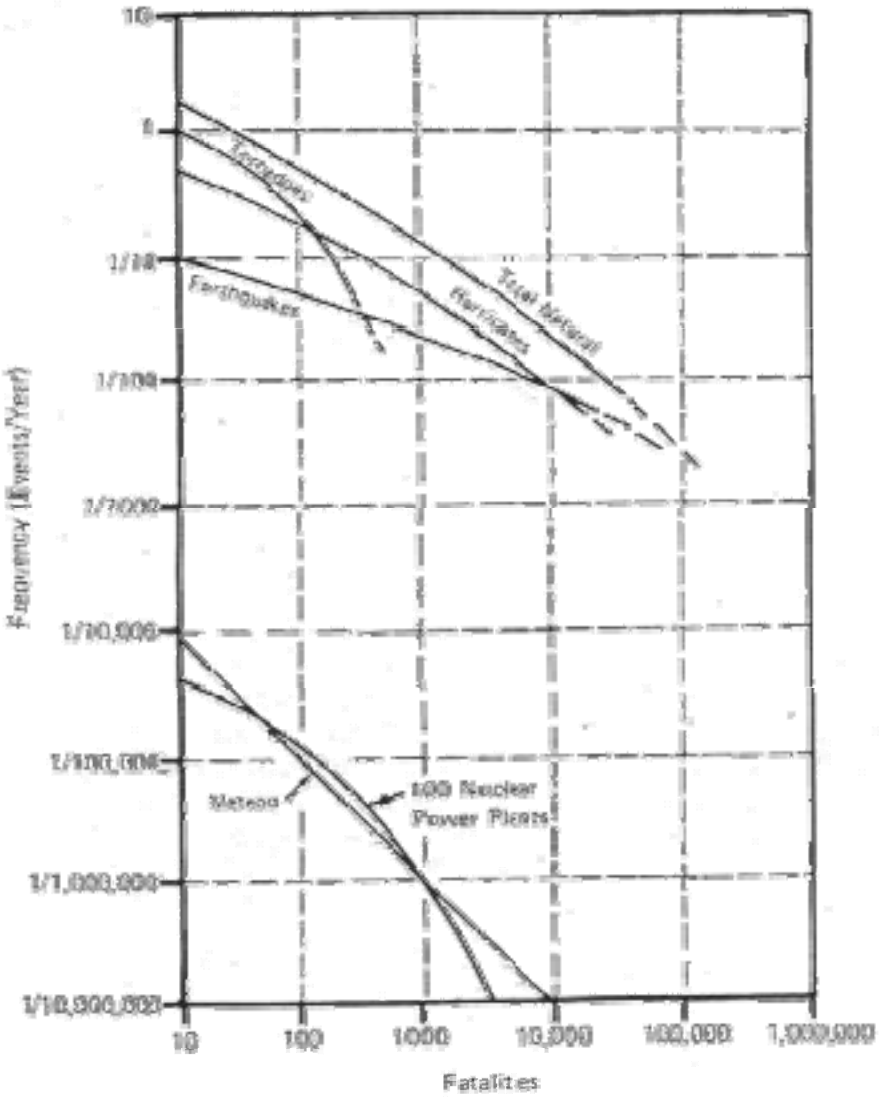
Source: ISO 14971 - Medical devices - Application of risk management to medical devices

Risk Classif.: Nuclear



Risk Classif.: Nuclear



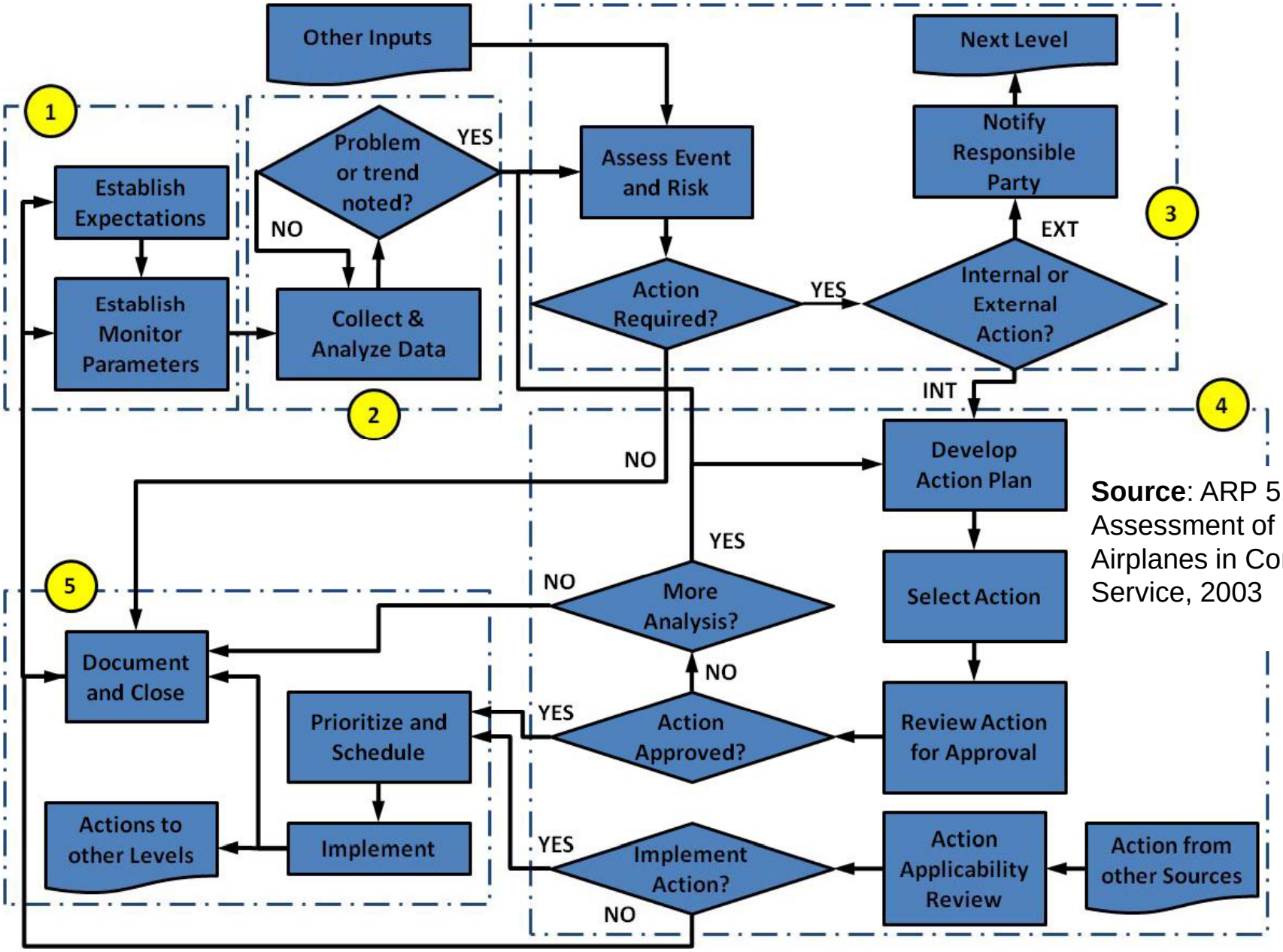


Source: WASH 1400, 1975

Análise das Técnicas

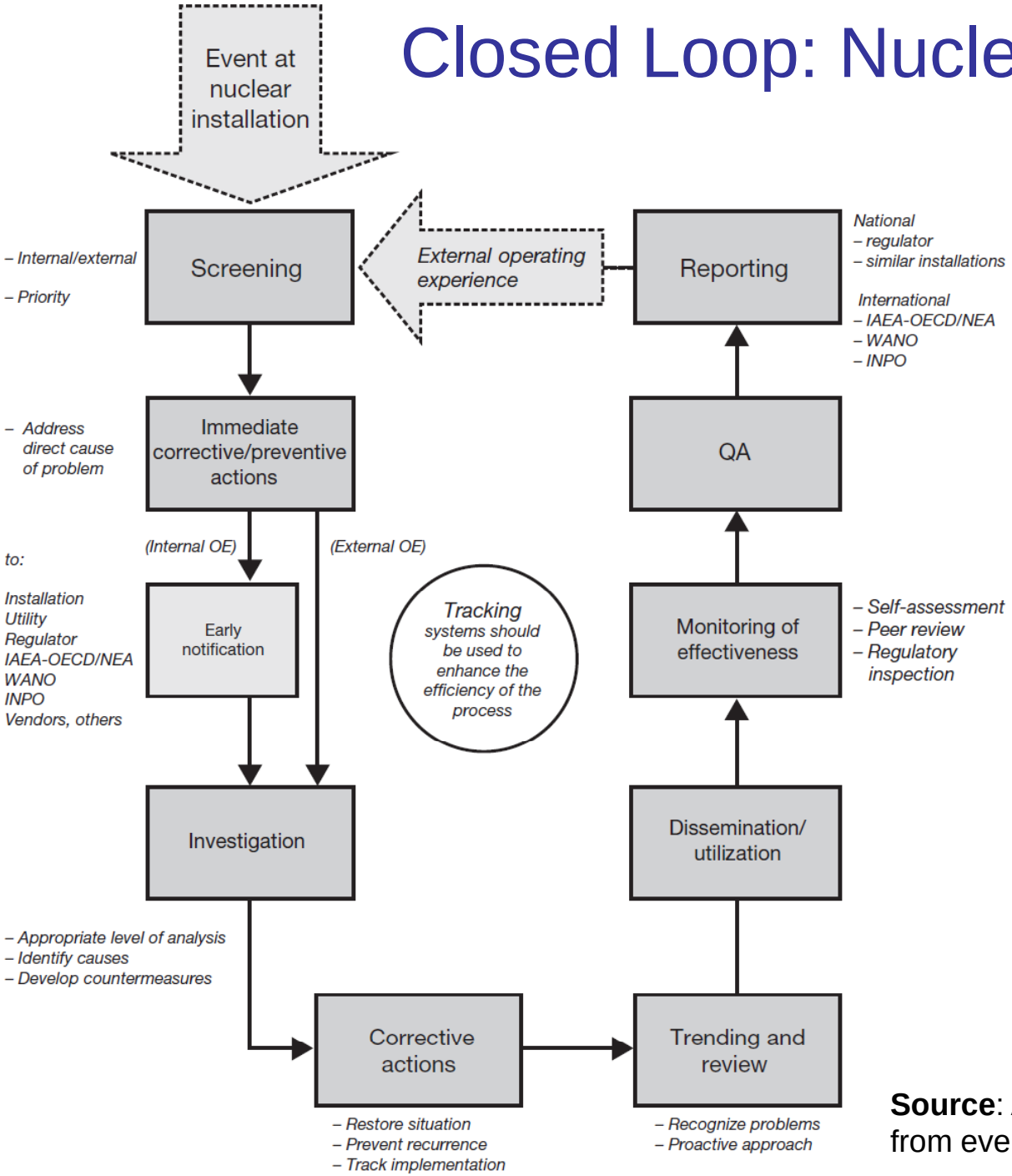
Analysis Techniques	Military	Space	Aeronautics	Nuclear	Rail	Medical
FMEA / FMECA	OK	OK*	OK	NO	OK	CIT[2]
Reliability Prediction	OK	CIT	CIT	NO	CIT	OK[2]
Event Tree	OK	OK	OK	OK	OK	OK[2]
Fault Tree	OK	OK	OK	OK[3]	OK	OK[2]
Weibull	OK	OK	OK	OK[3]	CIT	NO
Reliability Growth	OK	OK	OK	NO	NO	NO
Monte Carlo	OK	OK	OK	OK[3]	CIT	NO
Markov	OK	NO	OK	OK[3]	OK	NO
Dependency/ Block Diagrams	OK	OK	OK	NO	CIT	NO
CCF Analysis	OK	OK	OK	CIT	CIT	CIT[2]

Closed Loop: Aeronautics (ARP 5150)



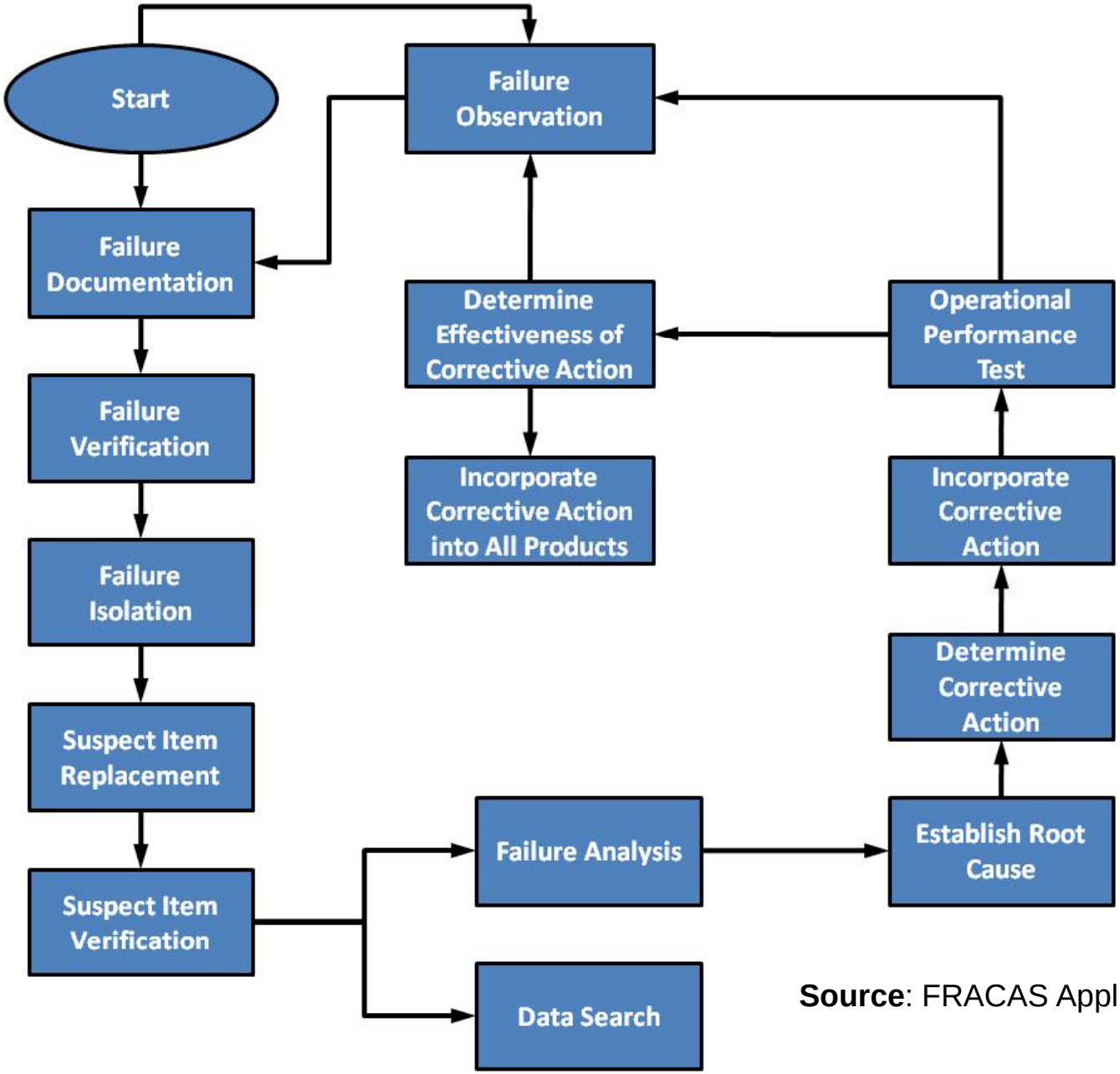
Source: ARP 5150 Safety Assessment of Transport Airplanes in Commercial Service, 2003

Closed Loop: Nuclear



Source: A system for the feedback of experience from events in Nuclear Installations, 2006

Closed Loop: Militar, Rail, Space

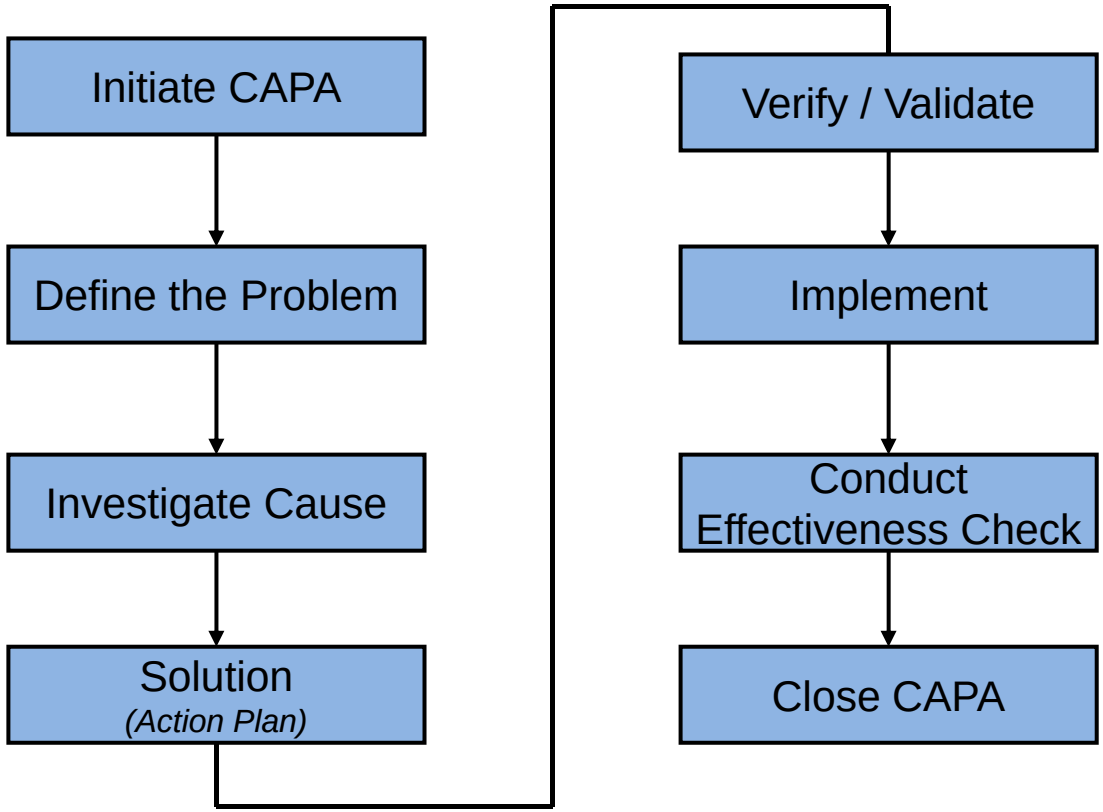


FAILURE REPORTING ANALYSIS CORRECTIVE ACTION SYSTEM

Source: FRACAS Application Guidelines, RiAC, 1999

Closed Loop: Medical Devices

CAPA: Corretive Action Preventive Action



Source:

High Integrated Systems: Aeronautics

ED-80/DO-254 “Design Assurance Guidance for Airborne Electronic Hardware”

ED-12/DO-178 “Software Considerations in Airborne Systems and Equipment Certification”

ED-79/ARP-4754 “Certification Considerations for Highly-Integrated or Complex Aircraft Systems”

High Integrated Systems: Military, Space

MIL-HDBK-338B “Electronic Reliability Design Handbook”

MIL-STD-2167 “Defense System Software Development”

High Integrated Systems: Nuclear

IEC 61226 “Nuclear Power Plants - Instrumentation and Control important to safety – Classification of instrumentation and control functions”

IEC 61513 “Nuclear Power Plants - Instrumentation and Control for systems important to safety – General requirements for systems”

IEC 60880 “Nuclear Power Plants - Instrumentation and Control for systems important to safety – Software aspects for computer-based systems performing category A functions”

High Integrated Systems: Rail

EN 50128 “Railway applications - Communications, signaling and processing systems – Software for railway control and protection systems”

EN 50129 “Railway applications - Communications, signaling and processing systems – Safety related electronic systems for signaling”

EN 50159 “Railway applications - Communications, signaling and processing systems.
Part 1: Safety related communication in closed transmission systems
Part 2: Safety related communication in open transmission systems

High Integrated Systems: Medical

IEC 60300-3-9 *Dependability management - Part 3: Application guide — Section 9: Risk analysis of technological systems*
IEC/TR 60513 *Fundamental aspects of safety standards for medical electrical equipment*
IEC 60601-1 *Medical electrical equipment — Part 1: General requirements for basic safety and essential performance*
IEC 60601-1-4 *Medical electrical equipment — Part 1-4: General requirements for safety — Collateral standard: Programmable electrical medical systems*
IEC 60601-1-6 *Medical electrical equipment — Part 1-6: General requirements for safety — Collateral standard: Usability*
IEC 60601-1-8 *Medical electrical equipment — Part 1-8: General requirements for basic safety and essential performance — Collateral standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems*

Conclusões

1. É incrível que em todos os setores a quantificação do risco seja tratada exatamente do mesmo modo.

2. Os programas maduros de apresentam mais similaridades que dissimilaridades

3. Alguns programas não são tão diretos na abordagem de confiabilidade e segurança, o que dificulta o entendimento da metodologia a ser seguida

4. As normas de terceiro nível mais utilizadas são as militares, contudo existe um movimento claro para que a IEC tenha normas similares e que sejam independentes de setor

5. O encontro entre setores pode trazer benefícios para os setores menos maduros, como é o caso de equipamentos médicos