SAFETY AND STANDARDS

CHALLENGES TO SAFETY EVALUATION IN THE FUTURE RAIL AND AIR TRANSPORTATION SYSTEMS

João Batista Camargo Junior

Safety Analysis Group (GAS)

Computer and Digital Systems Engineering Department

School of Engineering (Escola Politécnica) of University of São Paulo (USP)

São Paulo, Brazil

OVERVIEW

- The Safety Analysis Groups (GAS) at USP.
- Trends in Computer-based Rail and Air Transportation Systems.
- Safety and Standards in Transportation Systems.
- Challenges to Computer-based Dependable Systems.

: a Research Group at "*Computer and Digital Systems Engineering Department*" in the School of Engineering at USP (Poli-USP) .

⇩

GAS in numbers: 6 Professors,
13 D.Eng Students,
8 M.Eng Students,
Several direct collaborators (from industry and academia).

Academic Research*, *R&D* and *Consultancy Projects* related to Safety, Reliability and Availability of *Computer-Based Safety-Critical Systems

Our main research and application topics:

Safety and Risk Assessment Methodologies
Fault Tolerance (including Software Quality aspects)
Redundancy Techniques (HW / SW)
Certification to Safety
Safe Software
Human Reliability / Usability

GAS Grupo de Análise de Segurança
Escola Politécnica da USP

USP Escola Politécnica
Universidade de São Paulo

Some examples of current *Application Areas* and our *Related Works*:

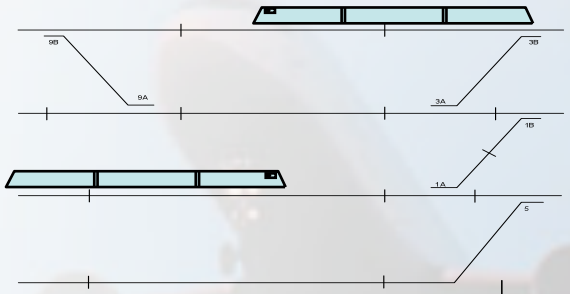
- **Subway / Railway Transportation**
  - Safety Assessment of computer-based supervision and control systems to METRO-SP, CPTM-SP, CBTU-RJ, DMETRO-BH, METROREC,TRENSURB, VALE, DATAPROM.
- **Air Transportation**
  - Air Traffic Management (Embraer, Atech, Brazillian Air Traffic Control Authority (CGNA,DECEA, CISCEA))
    - Genetic Algorithms applied to Demand *versus* Capacity balancing.
    - Safety and Availability Assessment to Air Traffic Control (ATC) Systems.
  - The CNS/ATM paradigm.
- **Aerospace**
  - Brazilian Satellite Launcher Vehicle (IAE)
    - Challenges in aerospace software application
- **Brazilian Army** – safety and availability
- **Energy** - availability

Trends in Computer-based Rail e Air Transportation Systems

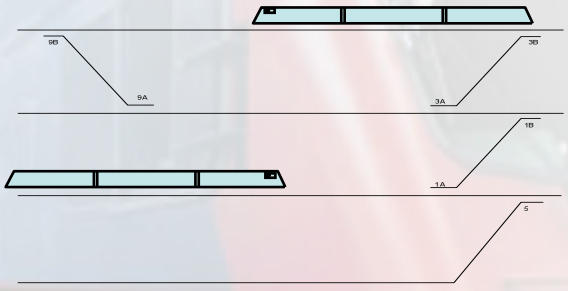
RAIL TRANSPORTATION DEVELOPMENT (A subway example)

EVOLUTION (Signaling Paradigm)

Fixed Block



Moving Block

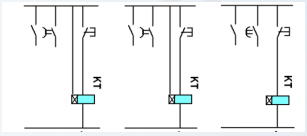


Supervision

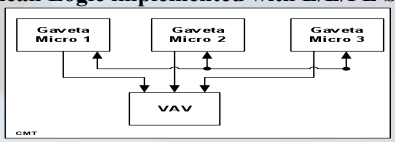
Control

Application Domain

Control System (interlocking) based on Boolean Logic implemented with Electromechanical Relays



Control System (Interlocking) based on Boolean Logic implemented with E/E/PE Systems



- Ground-centered control.
- E/E/PE systems with **customer-oriented solution.**
- **SW source code (most of the time) available to the analysis team.**

Control System based on IT

COTS

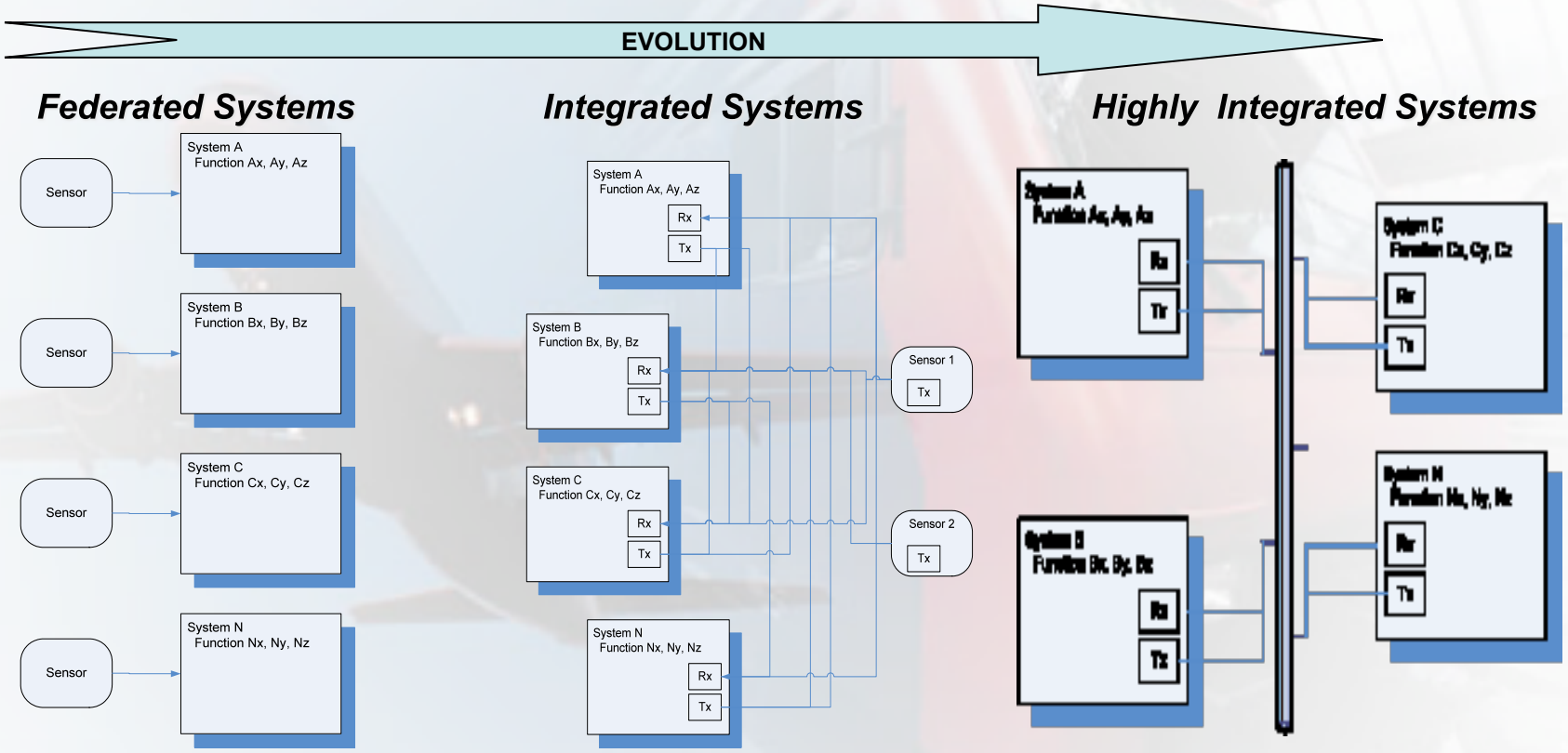
- Distributed control over (open std) communication systems.
- E/E/PE systems with **commercial (COTS) solution.**
- **SW source code (most of time) not available to analysis team.**

S&C Domain

EVOLUTION (Control Systems)

AIR TRANSPORTATION DEVELOPMENT

AIRCRAFT (AVIONICS)



- Intensive use of mechanical, electromechanical and analog electronic systems.

- Use of analog and digital electronic systems and some electromechanical controls.

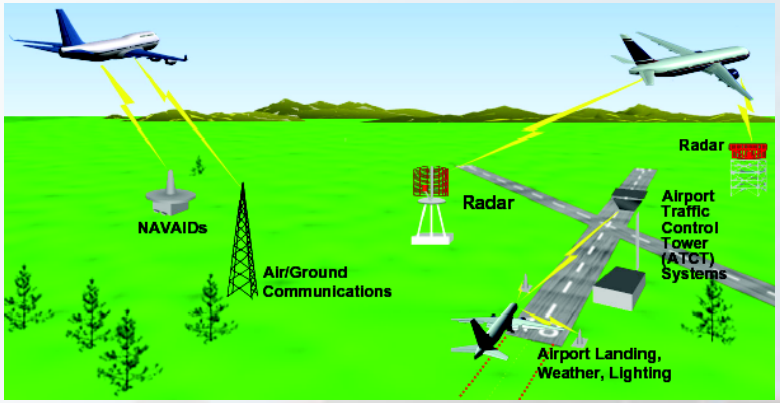
- Control systems implemented with E/E/PE modules

GAS Grupo de Análise de Segurança
Escola Politécnica da USP

USP Escola Politécnica
Universidade de São Paulo

AIR TRANSPORTATION EVOLUTION

AIR TRAFFIC MANAGEMENT (ATM) SYSTEMS



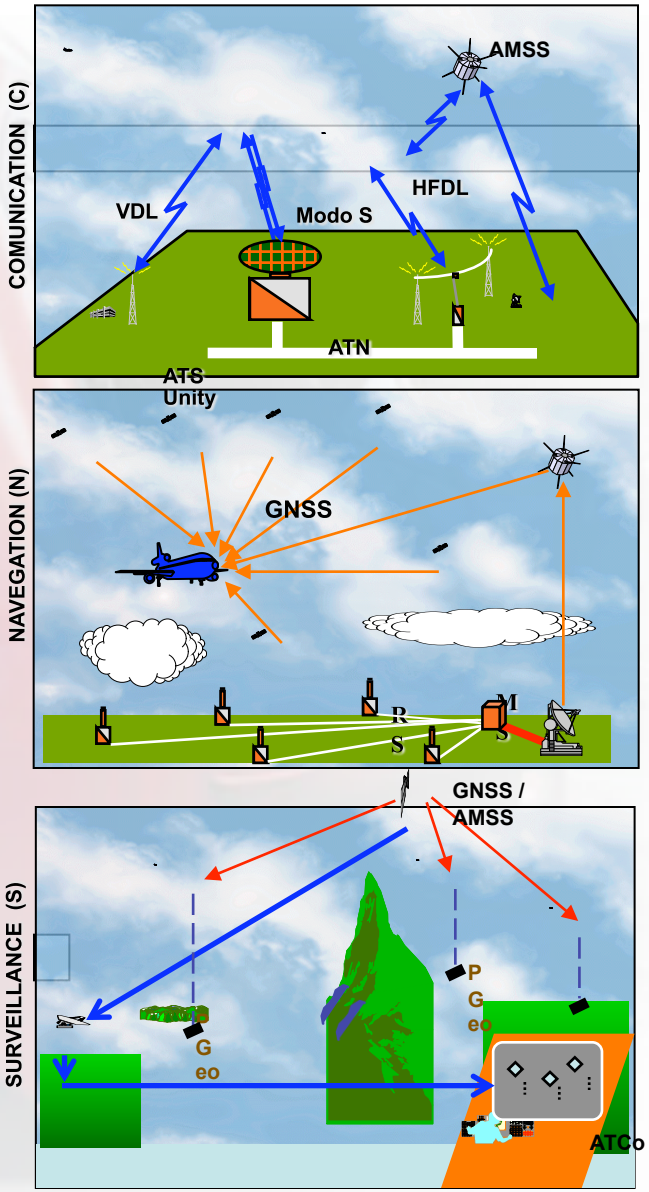
Today's Air Traffic System

- Ground-based (NavAids, Radar)
- Single Channel voice control
- Human-centered with non automated support.
- Proprietary Hardware and Software.

EVOLUTION (Technologies and Procedures)

CNS/ATM System

- Satellite-based Navigation and Communication
- Data-based Control (ATN)
- Human-centered, but "automated" Decision-Making.
- Hardware COTS, Proprietary Software



Safety and Standards in Transportation Systems

Transportation systems have a consolidated Standard Base regarding safety aspects.

STANDARDS

(some examples related to computer-based systems)

Rail Transportation

IEC 61508: Functional safety of E/E/PE safety-related systems

EN 50126: Railway applications - the Specification and Demonstration of RAMS.(*)

EN 50128: Railway applications - SW for Railway Control and Protection System.

EN 50129: Railway applications - Safety related electronic systems for signaling.

FRA 49 CFR (parts 200-299) (209, 213, 234, 236): Federal Railroad Authority Regulations.

Air Transportation - Aircraft

SAE ARP 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

SAE ARP 4754: Certification Considerations for Highly-Integrated or Complex Aircraft Systems.

RTCA DO-178B: SW considerations in Airborne Systems and Equipment Certification.

RTCA DO-254: Design Assurance Guidance for Airborne Electronic Hardware.

RTCA DO-297: Integrated Modular Avionics (IMA) Development

Air Transportation – Air Traffic Management

ICAO Doc 4444: ATM – Procedures for Air Navigation Services.

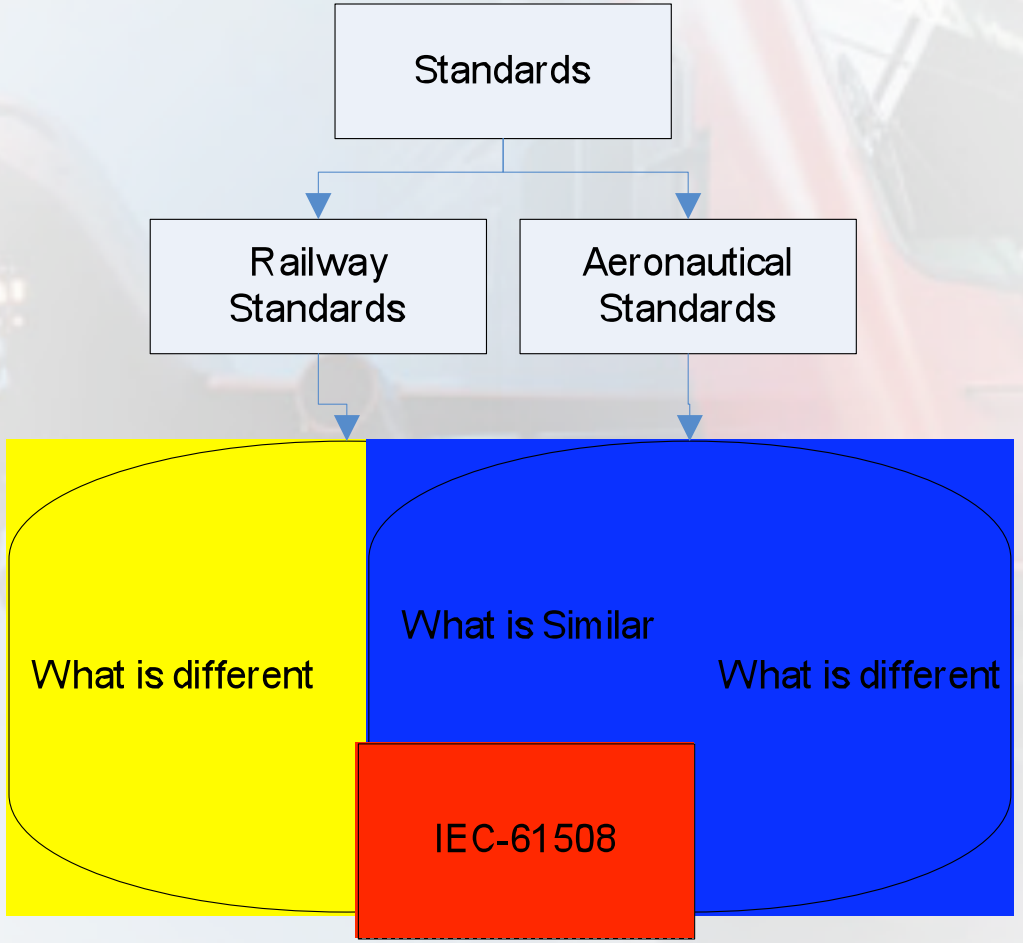
ICAO Annex 11: Air Traffic Services.

ICAO Doc 9859: Safety Management Manual.

(*) CENELEC - European Committee for Electrotechnical Standardization

STANDARDS

(some examples related to computer-based systems)



CENELEC

CFR 49 200-299

…

ICAO

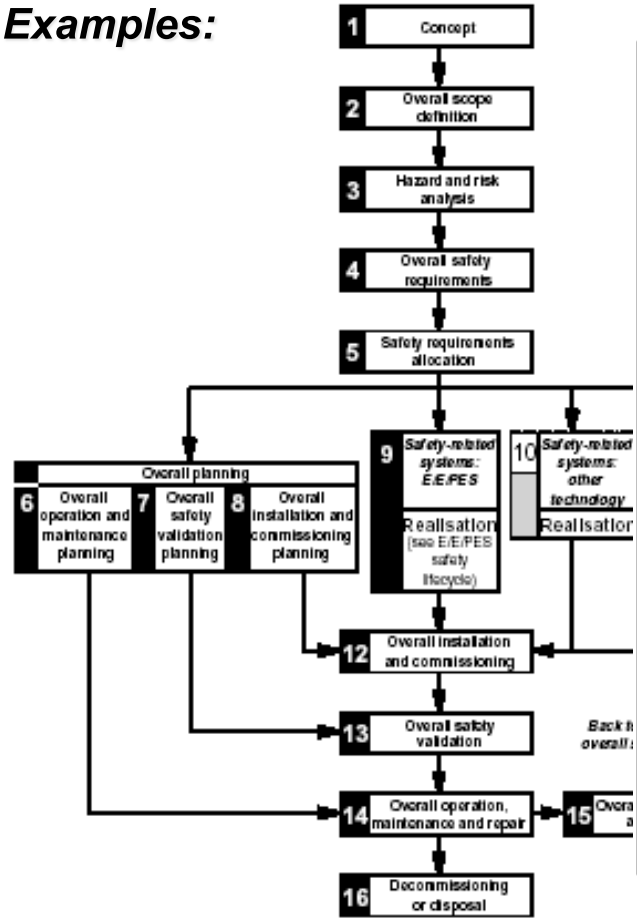
EUROCONTROL

FAA

…

Transportation systems standards deal with the concept of safety at all stages of their system lifecycles.

Examples:



IEC 61508 - Overall safety lifec

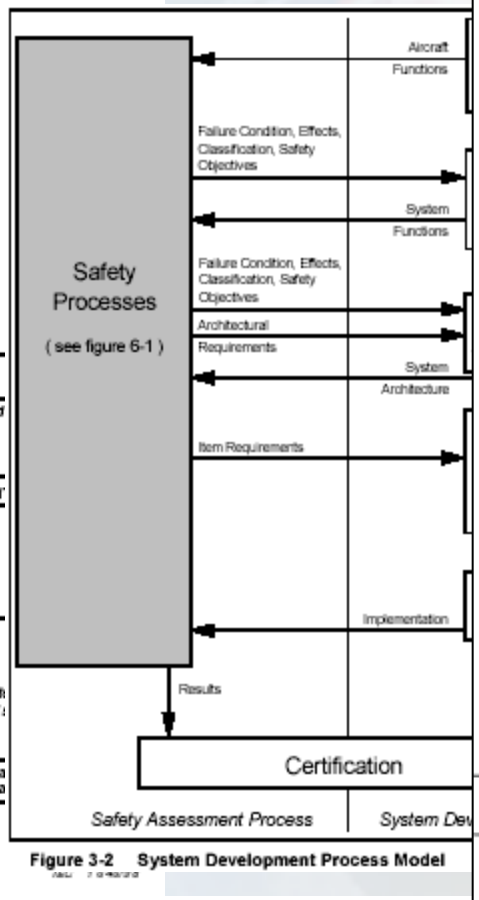
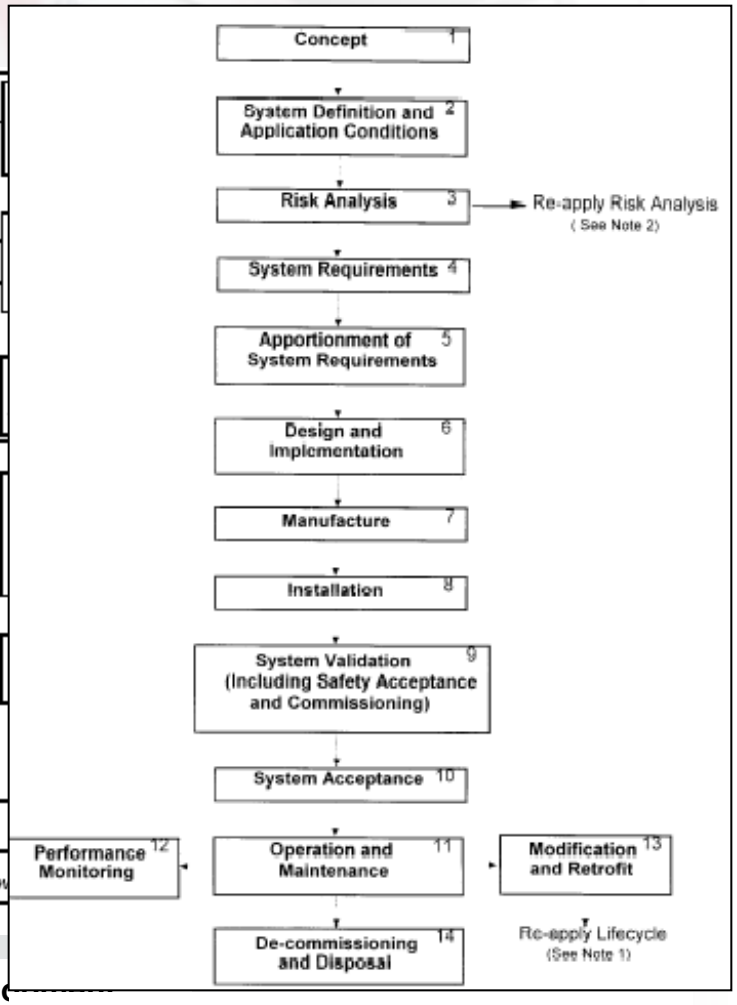


Figure 3-2 System Development Process Model

ARP 4754 - System Develo
Process Model



EN 50126 - System lifecycle

The means to achieve the safety requirements relates to controlling the factors which influence safety throughout the life of the system.

Effective control requires the establishment of mechanisms and procedures to defend it against (random and systematic) sources of error being introduced during the realization and support of the system.

The means used to achieve safety (dependability) requirements are based on taking precautions to minimize the possibility of an impairment occurring as a result of an error during the lifecycle phases.
➔ Precaution is a combination of *prevention* and *protection*.

Standards (as IEC61508 and EN5012x) recommend techniques and measures to avoid ("prevention") and to control ("*protection*") failures (both random and systematic).

Techniques and Measures ⇔ Lifecycle Phase and/or HW/SW domain.

➔ RECOMMENDATION EXAMPLES (IEC61508) ... ←

➔ RECOMMENDATION EXAMPLES (IEC61508) ... ←

Techniques and measures for E/E/PE safety-related systems: control of failures during operation [Annex A (normative) – IEC61508-2]

This normative contains:

Specific techniques and measures applicable to control (protection) **random HW failures** of E/E/PES components (*electrical, electronic, processing units, memories, I/O units and interfaces, ventilation and heating, sensors, actuators* ...): e.g: self-test (hw/sw), diagnostics, hw redundancy, …)

Specific techniques and measures applicable to control **systematic failures** of E/E/PE Systems:

- caused by hardware and software design (e.g.: *"Program sequence monitoring", "Tests by redundant hardware", "Fault detection and diagnosis", "Recovery block", "Diverse programming"*, …);
- due to environmental stress or influences (e.g.: *"Increase of interference immunity", "Program sequence monitoring", "Spatial separation of multiple communication lines"*, …); and
- during operation (e.g.: *"*Input acknowledgement*"*, "Modification protection", …).

➔ RECOMMENDATION EXAMPLES (IEC61508) ... ←

Techniques and measures for E/E/PE safety-related systems: avoidance of systematic failures during the different phases of the lifecycle

[Annex B (normative) – IEC61508-2]

This normative contains recommendations to avoid:

Mistakes during specification of E/E/PES requirements (e.g.: *"Project management", "Inspection of the specification", "Computer aided specification tools", …*)

Faults introduction during E/E/PES design and development (e.g.: *"Observance of guidelines and standards", "Use of well-tried components", "Simulation", "Checklists", …*)

Faults during E/E/PES Integration (e.g.: *"Functional testing", "Black-box testing", "Statistical testing", …*)

Faults and failures during E/E/PES operation and maintenance procedures (e.g.: *"Operation and maintenance instructions", "Limited operation possibilities", "Limited operation possibilities", …*)

Faults during E/E/PES safety validation

The establishment of mechanisms and procedures to defend system against error sources demands the correct and complete identification of error that could really occur.

STANDARDS RECOMMEND SIMILAR TECHNIQUES / MEASURES FOR SAFETY ASSESSMENT AND SAFETY VALIDATION PROCESSES

Examples:

SAFETY ASSESSMENT ANALYSIS METHODS **(SAE ARP 4761 and others)**

- Fault Tree Analysis/Dependence Diagram/Markov Analysis (FTA/DD/MA)
- Failure Modes and Effects Analysis (FMEA)
- Failure Modes and Effects Summary (FMES)
- Common Cause Analysis (CCA)

IEC 61508-3 (SW Requirements)

Table A.10 – Functional safety assessment (see clause 8)

	Assessment/Technique*	Ref	SIL1	SIL2	SIL3	SIL4
1	Checklists	B.2.5	R	R	R	R
2	Decision/truth tables	C.6.1	R	R	R	R
3	Software complexity metrics	C.5.14	R	R	R	R
4	Failure analysis	Table B.4	R	R	HR	HR
5	Common cause failure analysis of diverse software (if diverse software is actually used)	C.6.3	---	R	HR	HR
6	Reliability block diagram	C.6.5	R	R	R	R
*	Appropriate techniques/measures shall be selected according to the safety integrity level.					

Methods and Data (see paragraphs 7.6.1.a - f and 7.7)	Development Assurance Level			
	A & B	C	D	E
PSSA (paragraph 6.2)	R	R	A	A
Validation Plan	R	R	A	N
Validation Matrix	R	R	A	N
Validation Summary	R	R	A	N
Requirements Traceability	R	A	A	N
Analysis, Modeling, or Test	R	One	A	N
Similarity (Service Experience)	A	recom-	A	N
Engineering Judgment	A	mended	A	N
Cross System Implementation Effects	R	A	A	N

R - Recommended for certification.
A - As negotiated for certification.
N - Not required for certification

requirements validation (SAE ARP 4754)

A typical Safety Assessment Process has the structure defined below [1]:

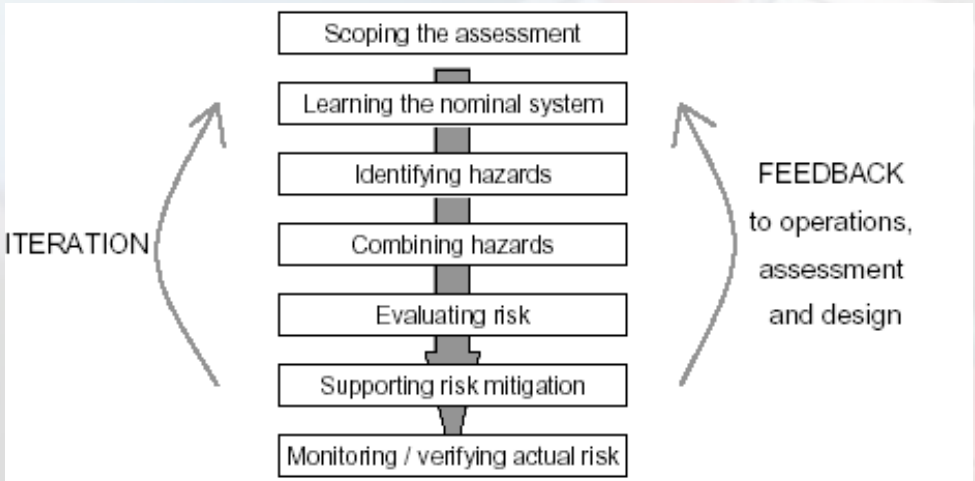


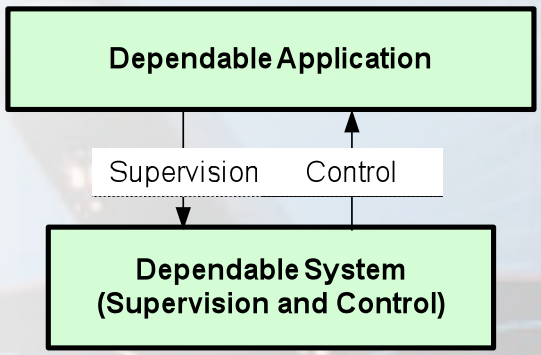
Figure 1: A generalized Seven-Stage Safety Assessment Process, with right-hand-side feedback loop as an 'eighth' stage that should be part of all other stages

The National Aerospace Laboratory (NLR) maintains a "Safety Methods Database" containing 701 methods (version 0.8) that can be used during a Safety Assessment [2]. Some of them are mentioned in the Standards.

1. FAA/Eurocontrol, ATM Safety Techniques and Toolbox, Safety Action Plan-15, Issue 1.1: For Comment, February 10, 2005,
2. http://www.nlr.nl/documents/flyers/SATdb.pdf

Challenges on Computer-based Dependable Systems

Rail and Aerospace Industry



Where "the unsafety consequences" occur.

Where the abnormal functioning could lead to disastrous (unsafety) consequences

The guarantee of dependable levels.

New and unknown abnormal functioning states.

APPLICATION DOMAIN

AFFECTS

DEMANDS

SYSTEMS DOMAIN

New social challenges
(capacity, efficiency, costs-reduction, …)

New technologies / concepts
(enabling the accomplishment of the application demands).

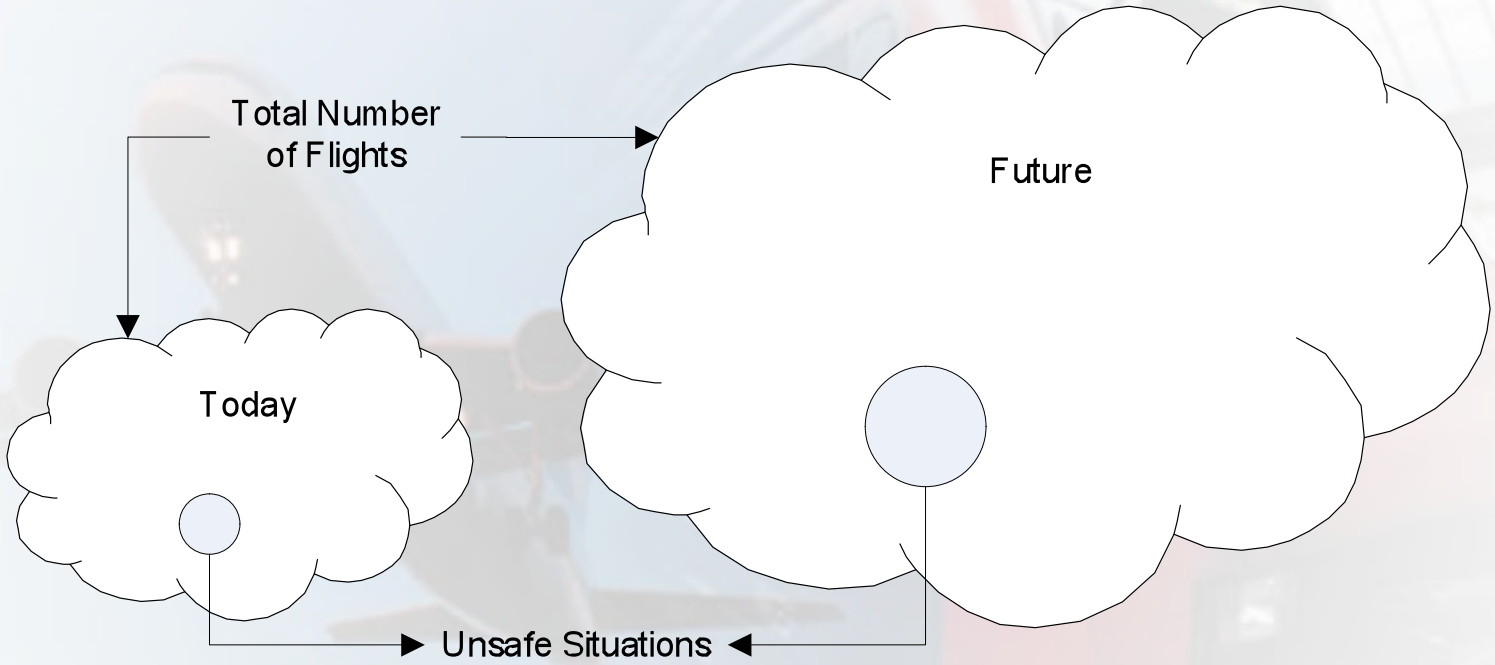
AIR TRANSPORTATION DOMAIN: "SESAR's Key Challenges"

SESAR – Single European Sky ATM Research Programme

- European Aviation Operations in 2006
  - Services are provided to ~200,000 General Aviation flights operated by ~50,000 aircraft
  - On a peak day, ATM controls ~30,000 flights operated by ~5,000 aircraft
  - "Point-to-Point" concept of operations creates a complex air transport network.
- Growth Projections
  - By 2025, demand is expected to be 2.4 times higher than today.
  - Diversity in the types of airspace users *(e.g., low-cost airlines, general & business aviation, unmanned aerial vehicles)* is expected to continue to grow.

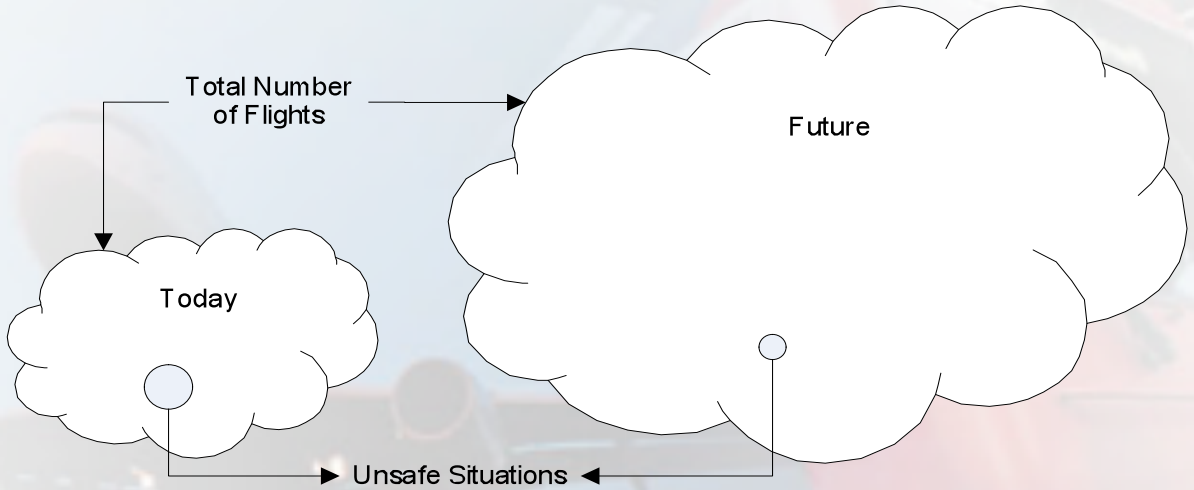
Source: www.eurocontrol.int/sesar/ and www.sesarju.eu/

Measuring Unsafe Events



$$\text{Unsafe Rate} = \frac{\text{Unsafe Situations}}{\text{Total Number of Flights}}$$

Measuring Unsafe Events



The ICAO (International Civil Aviation Organization)
GLOBAL AVIATION SAFETY PLAN - GASP (2004)

The aims of the ICAO GASP are to:

a) reduce the number of accidents and fatalities worldwide irrespective of the volume of air traffic; and

b) achieve a significant decrease in accident rates, particularly in regions where these remain high.

SESAR goal for 2020: improve the safety performance by a factor of 10.

SESAR Key Challenges (cont'd)

AIR TRAFFIC MANAGEMENT

- **ATM is a Network**

  Some 100 main European airport "nodes" which are linked together by ~600 airspace sector nodes operated by more than 36 different ANSPs.

- Measured ATM Performance:
  - **Safety**: 1992 to 2003: ATM contributed with 3.6% of commercial aviation accidents. No accident related with ATM since 2003.
  - **Capacity**: In 2005, delays due to flow restrictions fell by 75% as compared to 1999.

ANSP – Air Navigation Service Providers
Source: www.eurocontrol.int/sesar/ and www.sesarju.eu/

SESAR Key Challenges (cont'd)

SESAR Long Term and Innovative Research Agenda

SESAR Research Agenda will define research topics which are felt to be relevant for the evolution of the ATM Target Concept and beyond. Research example topics:

- **Highly-automated ATM;**
- Airport of the future (ATM part only); and
- Inter-modality (ATM impact only).

Source: SESAR Definition Phase - Deliverable 6 - Work Programme for 2008-2013

ATM Major Functions

- Air Traffic Management Organization
- Airport Operations
- Demand/Capacity Balancing
- Air Traffic Synchronization
- Conflict Management

ATM Challenges

- New ways for air traffic management control:
  - Pilot as part of control (*)
  - Distributed “intelligent” System where aircrafts exchange information
  - Automated Tasks
- Distributed Decision System
  - Fault Tolerant Distributed Systems
  - High level of safety and security

(*) Airborne Separation Assistance System (ASAS)

ATM Challenges

- **A huge number of Agents** (airports, aircrafts, …)
- Common interests (safety operation), but …
  - Every agent just observes a **different** part of the same system... Actions and decisions **can** affect the other parts, involving conflicts of interests
- **A huge number of** Emergencies, unpredictable situations, weather conditions, and failures types.
- **ATM:** Collaborative Decision Making – CDM
  - Strategic, Pre-tactical and Tactical Plan (real time)

ATM Challenges

*"CDM is defined as a **set of applications** that improves flight operations by means of the **growth in involvement** of air traffic controllers and pilots in the **Air Traffic Management Process**" (ICAO)*

ATM Challenges

CDM

- What groups need information and what the best format for it?
- Do all groups need the same information?
- When does operational information become proprietary?
- When does information become a problem? (security, safety, availability)
- How to measure the value and the cost of a spread information?
- How to upgrade the system without a negative impact in some parts?

Human Factors in Automation Dependability

- ATM - today
  - procedures rely on technologies in which the human being is central,
  - Humans have to assure the safe and secure transit of aircraft all over the network,
  - rely upon procedures and human abilities to resolve problems.

- The role of humans in the system which is central to the design of automation is an important constituent of safety and a matter of debate within the profession.

Source: Eurocontrol – Sesar

Human Factors in Automation Dependability

- Human-centred automation,
  - focus of SESAR
  - requires human capabilities to be taken into account and built into the design of automation from the outset.
  - However, this does not guarantee optimum total system performance as studies have shown.
- In the long-term, the Air Traffic Controller's (ATCo) role will undergo radical change.
- The human role in future ATM (after SESAR) will be more strategic for Flow and Trajectory management.

Source: Eurocontrol - Sesar

Safety Aspects:

CHALLENGES

From Application Domain → ***To System Domain***

The following main challenges are observed in the field of computer-based safety related systems (specially in transportation systems):

- Automation x Safety
- Dependable COTS
- Complexity x Safety
- Complexity x Modeling and Simulation
- Safety Supported by Standards

Automation x Safety

- In Rail Systems, NTSB* recommends an increase in automation to improve safety
  - just a degree of freedom
  - Safe state (one can stop the train)
- In Aviation there are many more constrains about automation
  - There is "no" safe state.
  - "*To take off is an option, to land is an obligation*"

* NTSB MOST WANTED - www.ntsb.gov/Recs/mostwanted/positive_train.htm
NTSB – National Transportation Safety Board

Automation x Safety

- But …The use of Automation has been increased in Aviation as much as in Railway.
- Although the use of automation in aviation is not easily accepted, it has been used in new aircrafts, such as Automation to verify pilots' mistakes.

Aviation and Automation

- Flight Engineer substituted by avionics.
- Flight Control Systems
  - Mechanical → Hydromechanical → Analog Fly by Wire → Digital Fly By Wire → "fly-via-computer"
    - Future: Flight-By-Wireless Control System?
- Unmanned Vehicle System (UVS) in Civil and Military Applications.
- **Data link x Voice link: Security x Safety ... Quantum Computing!**

Automation x Safety

Security x Safety ... Quantum Computing

- The cryptography tools based on intractable computational problems was enough to ensure the security of communications systems.
- Quantum computation is able to cripple the widely current used cryptography techniques.
- This vulnerability represents a critical factor for networks where security fault could be associated to a safety fault (*)

(*) COSTA, C. H. A. ; CAMARGO JÚNIOR, João Batista . Information Security in aeronautical telecommunications: discussion of the feasibility and benefits of the use of quantum cryptography . In: V SITRAER, 2006, Brasília. V SITRAER 2006. Brasília : Editora da UnB, 2006. (in portuguese)

Automation x Safety

- UVS (Unmanned Vehicle System) in Civil Domain:
  - The paradigm is the opposite from the military point of view.
  - The main application is Surveillance.
  - International Organizations worried about it:
    - European Aviation Safety Agency developing UVS airworthiness criteria for *certifying UVS*
    - Joint Aviation Authorities and Eurocontrol working together to formulate the international *operation of UVS in a controlled airspace*
    - FAA: safely integrating unmanned aircraft into the National Airspace (USA) System.

CORREA, Mário Aparecido ; CAMARGO JUNIOR, João Batista ; GIMENES, R. A. V. ; Almeida Junior, Jorge Rady . Safety Concerns on Operating UAV Using Cooperative Multiagent Negotiation. In: MVS 2006 - First IFAC Workshop on Multivehicle Systems, 2006, Salvador. First IFAC Workshop on Multivehicle Systems, 2006. v. 1. p. 102-107.

Dependable COTS

- How to guarantee safety?
- How to cover all possible problems inside the COTS?
- Does the use of support tools (e.g. Matlab/Simulink®) generate safe codes? Who assures the resulting code?

  "If tools are used as part of design or assessment for any overall, E/E/PES or software safety lifecycle activity, they should themselves be subjected to the functional safety assessment. (IEC 61508)"
- Is the fusion of different methods the way of assessment?

E/E/PES = electrical/electronic/programmable electronic safety-related systems

What we understand as "System Complexity"?

System Complexity: composed of interconnected parts that as a whole present one or more properties (behavior among the possible properties) not obvious from the properties of the individual parts.

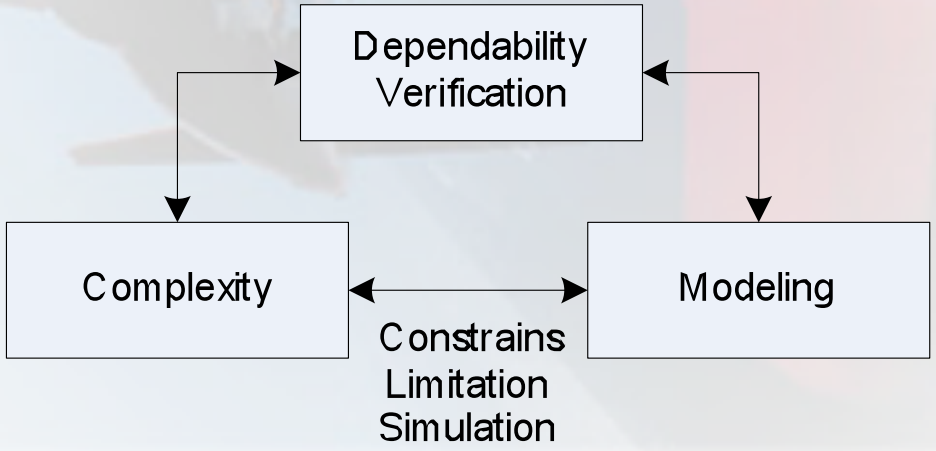
- Complexity raises from the interaction between two or more components of a system.
- Such interactions lead to a system behavior that is difficult to determine analyzing its components in isolation.
- The cause-effect relationship of problems are not evident.

Complexity x Safety – Challenges

- Traditional methods for safety analysis (FTA, FMEA, FMECA) are based on functional hierarchical decomposition.
- The interaction among components can lead to emergent misbehaviors which are a concern in complex systems.
- Coupled systems are prone to failure propagation.
- Interactivity and coupling are growing in modern systems.

Complexity x Modeling and Simulation

- Simulation may imply **simplification** in modeling removing the complexity that should be observed.
- To model a complex system, we have to impose constrains. But these constrains may lower the capability of Dependability Verification.



Complexity x Modeling and Simulation

- To deal with complexity: reduce/divide systems in domains "to represent" the complexity → how to define the sub-system boundaries?
- Timing in simulation must adequately represent the events in the application and system domain.
- Metrics that can adequately represent the complexity and how to use them to obtain the Target Level of Safety (TLS) or Mean Time to Unsafe Failures (MTTUF).

Safety Supported by Standards

Standards (as IEC61508 and EN5012x) recommend a huge number of techniques and measures to avoid and to control failures and, in this way, minimize the possibility of an impairment occurring as a result of an error during the lifecycle phases. But …

How to **quantitatively** evaluate the effectiveness of those techniques and measures **over the system safety level ??**

How to choose, based on **quantitative criteria**, the best set of techniques and measures to satisfy a required level of safety **??**

e.g.: IEC61508-3 recommends "**Defensive Programming**" to achieve the required SW safety integrity level. But, what is, quantitatively, the effectiveness of each technique over the system (application) safety level?

SECALL, J. ; CAMARGO JÚNIOR, J. B. . Comparative evaluation of defensive programming in safety critical applications. In: European safety and reliability conference, 2007, Stavanger. Risk, Reliability and Societal Safety. Leiden : Taylor & Francis/Balkema, 2007. v. 1. p. 655-661.

Safety Supported by Standards

How to **quantitatively** evaluate the software contribution **over the system safety level ??**

(Variations Application Domain/Hw Faults/Operational Faults/EMI/Sw Behaviour)

Safety Critical Systems

Safety Requirements

TLS - MTTUF

THANK YOU FOR YOUR ATTENTION

João Batista Camargo Junior
joao.camargo@poli.usp.br

Phone: +55 11 3091-5401
Fax: +55 11 3813-7415

Safety Analysis Group (GAS)
www.gas.pcs.poli.usp.br

Computer and Digital Systems Engineering Department (PCS)

Escola Politécnica da Universidade de São Paulo (Poli-USP)

São Paulo, Brazil