Rebecca Nauli (naulireb)

SafeSys Summary

Quizlet: https://quizlet.com/ch/1134781270/safesys-flash-cards/?i=dgqxd&x=1jqt

Contents

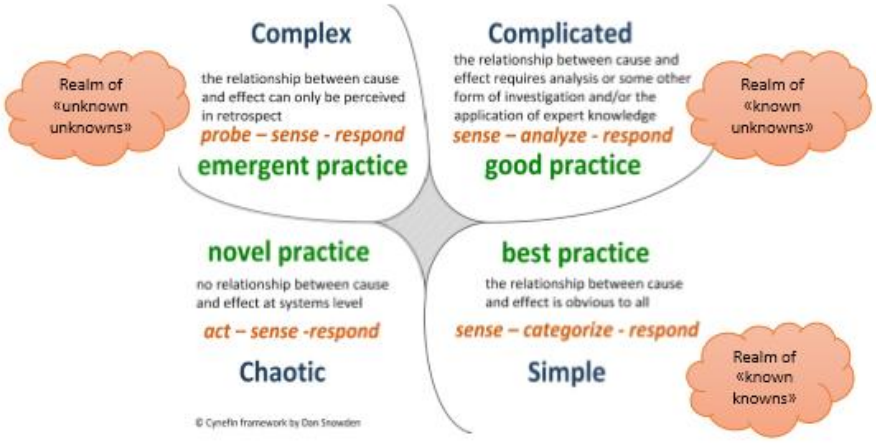
General Concepts

Safety Critical Systems Examples:

- Aerodynamics
- Structure
- Propulsion
- Avionics
- Electrical System
- Hydraulic System
- Flight Controls
- Reliability, Maintainability, Availability and Safety

Category	Typical Problems
Aerodynamics	• Aircraft performance (W&B calculations) • Estimation of basic static/dynamic forces • Estimation of complex aerodynamics interactions
Structure	• Withstand loads and be lightweight • Be fail safe (a component can fail but continued operations need to be safe) • Be stable from an aeroelastic point of view
Propulsion	• FOD (foreign object damage) • Rotor Burst • Fire Protection
Avionics	• reliability (the more components, the less reliable but the more dependable)

Complexity



* Snowden, David J.; Boone, Mary E. (November 2007). "A Leader's Framework for Decision Making". Harvard Business Review, 69–76. PMID 18159787

Definitions

Safety-Critical	Failure or design error that could cause risk to human life MIL-HDBK-516B: a term applied to any condition, event, operation, process or item whose proper recognition, control, performance, or tolerance is essential to safe system operation.
Flight Safety Critical	Flight Safety Critical indicates that a defect mode of the equipment can cause a hazard, i.e. a situation which threatens the safety of the crew and/or the aircraft when the aircraft is operated within its design limits.
Safety Critical System	A system (or one of a collection of systems) of the aeroplane in which a disturbance (or combination of disturbances) could result in a direct hazard to the aeroplane, aircrew, people or property on the ground. (FDEF-STAN-00-970)

Three major hazards:

1. Loss of line in flight

2. Collision of AC

3. Kill so. on ground/infrastructure damage

Example of complex systems:

- aileron
- flaps
- slats
- speed brakes
- roll spoilers
- lift dumpers
- rudder
- elevator
- trimmable horizontal stabilizer
- = reversible flight controls

Examples of catastrophic failures

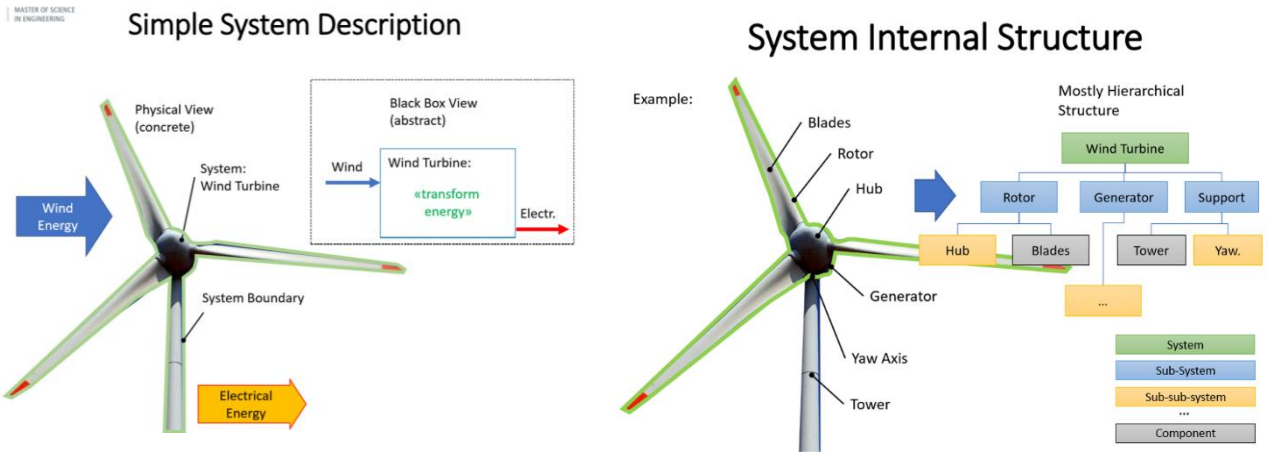
Loss of control	Erroneous Control
• loss of roll control • loss of pitch control • loss of yaw control • loss of thrust control • loss of breaking/steering control on ground	• erroneous roll output • erroneous pitch output • erroneous yaw control • erroneous thrust control • erroneous steering control on ground • erroneous guidance • erroneous envelope protection

System Engineering Principles

Definition of System

Def:

- A system is a set of elements in interaction.
- A system is an integrated set of elements, subsystems, or assemblies that accomplish a defined objective.
- A system is a combination of interacting elements organizes to achieve one or more stated purposes.
- A system is the combination of elements that function together to produce the capability required to meet a need.

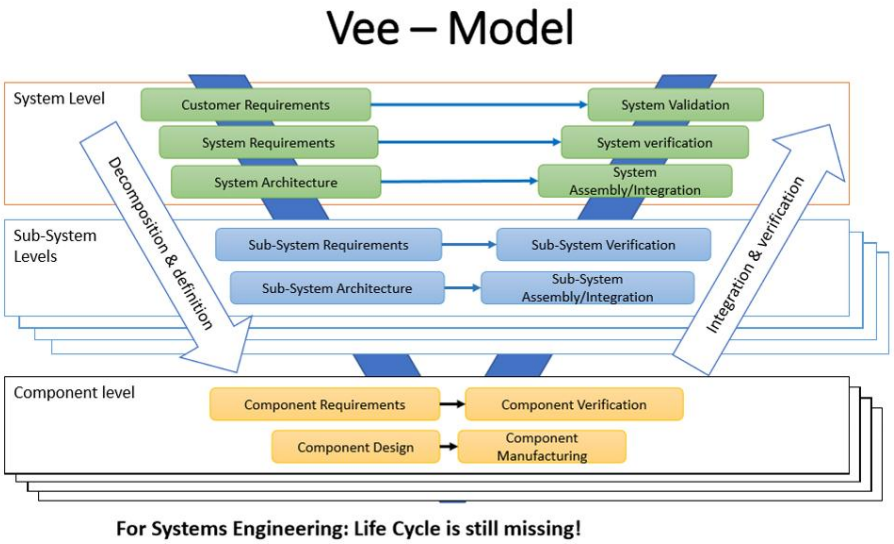


Systems Engineering Considerations

1. System exists in a “context” or environment e.g. operational environment, interaction with other/competing systems
2. System consists of elements that interact with each other and/or the external context E.g. hardware, software, people, organisations, … Interactions include exchange of information, energy, resources …
3. System has “system-level properties”, i.e. these are attributed to the system as a whole, not to individual elements
4. A system has the following:
    - Life cycle
    - Function
    - Structure, incl.
        - Boundary
        - Set of parts
        - Set of relations between parts and across the boundary
    - Behaviour, incl. state change and change of information, energy & resources

- Performance characteristics

5. A system changes and adapts to its environment, when deployed
6. System contains multiple feedback loops with various time constants → cause effect relationships not immediately obvious



Life-Cycle Models

System life cycle typically consists of

- Idea & Concept phase
- Development phase
- Production phase
- Utilisation phase

Stakeholders

A stakeholder is any entity (individual or organization) with a legitimate interest in the system. When nominating stakeholders, take into account all those who may be affected by or able to influence the system:

- users,
- operators,
- organization decision makers,
- parties to the agreement,
- regulatory bodies,
- developing agencies,
- support organizations,
- and society at large (within the context of the proposed solution)

Functional Architecture – Models

"A functional model in systems engineering and software engineering is a structured representation of the functions (activities, actions, processes, operations) within the modelled system or subject area." It shows relations between functions, inputs, outputs, resources etc.

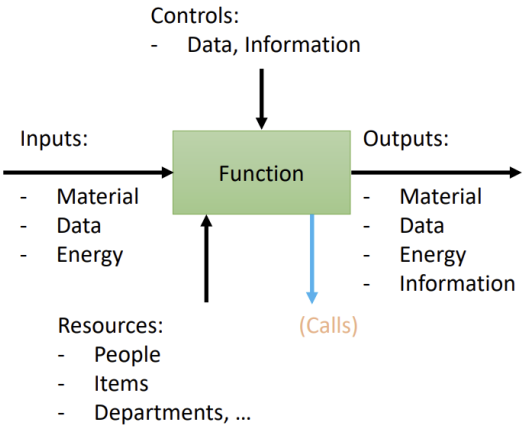
Typical:

- Boxes are functions
- Arrows are flow of material, data or energy
- Other specific elements

Functional Diagram

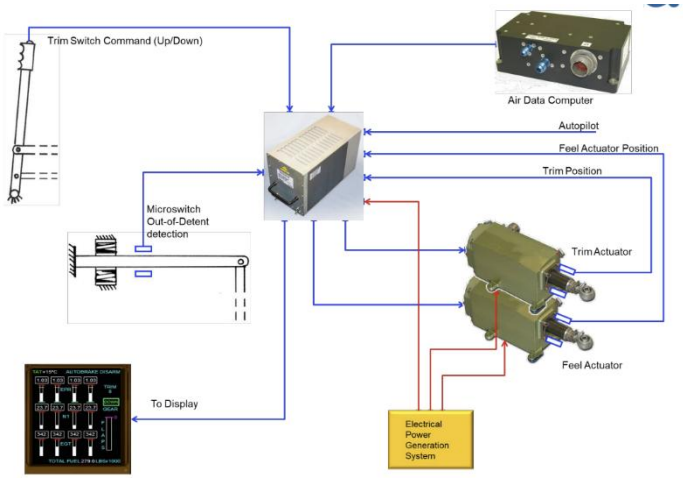
Functional Modelling method designed to model the decisions, actions, and activities of an organization or system.

- Function box is named with verb or verbed phrase
- Arrow locations important
- Each function block can be subdivided in function in a "child" diagram



Physical Architecture

Definition: A physical architecture is an arrangement of physical elements (system elements and physical interfaces) which provides the design solution for a product, service, or enterprise, and is intended to satisfy logical architecture elements and system requirements. It is implementable through technologies. (ISO/IEC 2010)



Functional vs. Physical Architecture

Functional Architecture (Process)	Physical Architecture (Form)
• Purpose of the system • Physical/Software solution free • Basis: Functional Requirements • Grouping and decomposing functions • Drives Value Proposition	• Physical/Software elements that deliver the function • Elements = technical solutions • Elements created top-down

	• Constraints & Non-Functional requirements need to be addressed

➔ Architect for both worst case and most likely case

Verification vs. Validation

Verification	Validation
• Done by the System Responsible • Test Environment • Answers the question: DID WE BUILD IT RIGHT, IN ACCORDANCE WITH REQUIREMENTS?	• Done by Developer • Systems real operational environment • Answers the question: ARE WE BUILDING THE RIGHT THING?

Verification Techniques

Inspection: visual or dimensional examination, non-destructive, often uses human senses, e.g. “green”, “loud”, “2kg”, “1.5m”

Analysis: uses analytical evidence based on models of reality, mathematics and logical reasoning, hardware is not necessary

Demonstration: used to show correct operation without using physical measurement, e.g. observations against predetermined responses

Test: a unit is built and subject to real conditions of operation, the results are compared against prediction with very concrete expectations of physical or software behaviour

Analogy or Similarity: based on previous experience with similar hardware and software under similar conditions - Handle with care!

Simulation: actually, a sub-set of analysis

Sampling: based on verification of characteristics based on samples (e.g. material properties), also considered as subset of testing

NASA (SE-Handbook):

Analysis:	analytical techniques based on mathematical or mock-up models, mostly when test is not (yet) available
Demonstration:	similar to test, used to show that requirement is basically met
Inspection:	visual examination of a product
Test:	based on verification of characteristics based on samples (e.g. material properties), also considered as subset of testing

ECSS: (ECSS-E-ST-10-02C R1, 2018)

Review of Design:	shall consist of using approved records or evidence that unambiguously show that the requirement is met
Analysis:	shall consist of performing theoretical or empirical evaluation using techniques agreed with the Customer.
Inspection:	shall consist of visual determination of physical characteristics.
Test:	shall consist of measure-ing product performance and functions under representative simulated environments.

Requirements – Writing, Verification, Validation & Testing

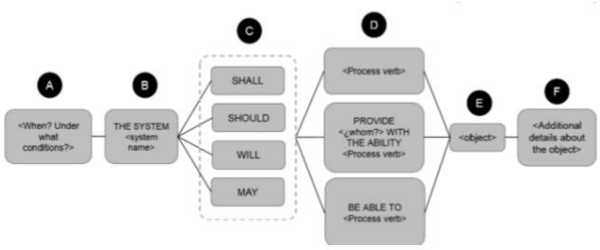
Writing – Documentation

Requirements Documentation:
Requirements must be **unambiguous, testable, complete, and consistent**. They can be expressed in **natural language**, **models** (UML, SysML, BPMN), or both.
A **glossary** helps avoid misinterpretations.

- **Unambiguous:** written in terms which only allow a single interpretation, aided, if necessary, by a definition.
- **Accurate:** written with the appropriate level of details
- **Complete:** it includes necessary, relevant requirements and/or descriptive material, responses are defined for the range of valid input data, figures used are labelled, and terms and units of measure are defined.
- **Verifiable:** it can be checked for correctness by a person or tool.
- **Consistent:** there are no conflicts within it.
- **Modifiable:** it is structured and has a style such that changes can be made completely, consistently, and correctly while retaining the structure.
- **Traceable:** the origin of its components can be determined.

Requirements Template

A requirements template is a blueprint that defines the structure of a single requirement sentence. The structure of the individual requirements is hence unified, and you can already tell at first glance whether or not important "components" are missing



(A) Conditions: condition or a set of conditions, usually optional. Example: "If", "as soon as", "after that".

(B) The System: The second space is the name of the system, the subsystem or component of the system that is specified for the requirement.

(C) Degree of Obligation: see later

D) Functional activity: typically: Autonomous requirement of the system, User interaction or Interface requirement
(not necessarily true for aviation)

(E) Object: the object for which the behavior specified in the requirement is performed.

(F) Object details: additional details (optional) about the object, the adjectives that qualify it or the characteristics that the object can possess.

Verb	Explanation
Shall	→a mandatory requirement Departure from such a requirement is not permitted without a formal agreement between the procuring activity and the supplier
Should	→ a recommendation or advice on implementing such a requirement. The procuring activity expects such recommendations or advice to be followed unless valid reasons are stated for not doing so
Will	→intention (design target) in connection with a requirement
May	→permissible practice of action It does not express a requirement of the specification
Must	→legislative or regulatory requirements (e.g. Health and Safety) with which both the Procuring Activity and the Supplier shall comply. e.g. certification

What we cannot test in-flight due to safety issues:

- fire
- engine failure
- rapid depressurisation
- structural integrity
- ground ops (parking brake, controls/steering on ground)

Validation & Verification

Validation: building the right thing

Verification: check req. and see if part fits the description

Validation & Consolidation:
Ensures stakeholder agreement using techniques like inspection, prototypes, or case studies.

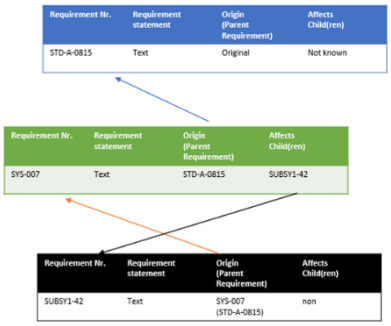
Management (Maintenance):
Involves **traceability**, **version control**, **requirement states**, and **lifecycle management**, often with tools like IBM DOORS.

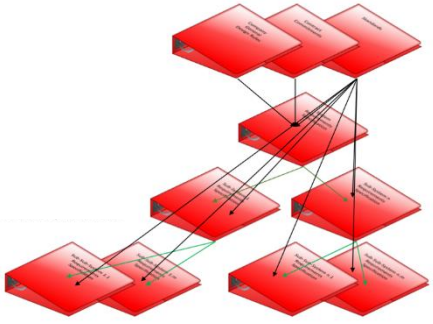
System Requirement Specification (SRS):
The baseline of all system requirements — clear, unique, consistent, stand-alone, traceable, non-redundant, and not biased (per INCOSE SE Handbook).

Requirement Hierarchy:
High-level → subsystem → sub-subsystem requirements.

Each requirement has:

- a unique number
- a parent requirement
- child requirement





Requirements can be

- qualitative (flown down); e.g. “All screws shall be stainless of quality 10.9”
- quantitative (broken down, decomposed); e.g. “The system mass shall be less then 10.5 kg”

➔ this is where discussions happen with the whole project team

Tools:

Simple (e.g. Excel)	Sophisticated (e.g. DOORS)

Pro’s
• Everybody can handle it
• Easy to adapt
• Easy to handle if:
  • number of requirements limited
  • Parent-child relations not so important
 	
Con’s
• Not useful for large systems
	Pro’s
	• All possibilities included
	• Programmed by professionals
	
	Con’s
	• Expensive
	• Only useful, if all sub-systems use it

Requirements may be **primary** (directly from system needs) or **derived** (from design decisions).

Traceability:

Every requirement must link to its origin and derived elements, avoiding gaps or orphan requirements.

We cannot accept:

➔ High level requirements that do not correspond to lower-level ones
➔ Lower-level requirements that do not correspond to higher level ones

Safety process – SAE-ARP-4761

Safety: Safety is a state in which risk is acceptable. (SAE ARP-4754A)

State: = implementation of the aircraft design

Risk: Estimation of the **seriousness** and the **likelihood of occurrence** of the **potential for harm**.

Risk must be acceptable to whom? The users of the aircraft (e.g. PAX), the general public.

Hazard: The potential for harm arising from an intrinsic property or disposition of something to cause detriment.

Probability: A measure or estimation of the likelihood of occurrence of an event.

Severity: The seriousness of something undesirable.

System Safety is (state in which risk is acceptable): the implementation of an aircraft design in which the seriousness and the likelihood of occurrence of the potential for harm to the passengers and the general public is acceptable!

Regulatory Framework:

Governed by **FAR/CS 1309 (now 2510)** — covering hazard prevention, safety analysis, and environmental conditions.

a. Prevention or mitigation of HAZARDS
b. Requires some analysis - SAFETY ASSESSMENT
c. Legacy Electrical
d. Environmental conditions/ external threats
e. What should not be covered by this requirement

Supported by **SAE ARP-4754A** (system development) and **SAE ARP-4761A** (safety assessment).

- **Failure Probability Categories:**
  - **Extremely Improbable** – $< 10^{-9}$
  - **Extremely Remote** – $< 10^{-7}$
  - **Improbable** – $< 10^{-5}$
  - **Probable** – $< 10^{-3}$

MSE | MASTER OF SCIENCE IN ENGINEERING

MSE SE.SCS: 1309

DESCRIPTIVE WORD	PERSONNEL INJURY/ILLNESS	IMPACT ON AIRCRAFT (SAFETY MARGIN)	FLIGHT CREW	FREQUENT	REASONABLY PROBABLE	REMOTE	EXTREMELY REMOTE	EXTREMELY IMPROBABLE
Catastrophic	Death of occupants	Loss of aircraft. Unable to continue safe flight and landing	Unable to respond or compensate for failure condition					
Hazardous	Adverse effects on occupants including serious or potentially fatal injuries to a small number of occupants	Large reduction in safety margin or functional capability	Significant increase in workload such that the crew cannot be relied upon to perform duties accurately or completely					
Major	Minor injury or discomfort to occupants	Significant reduction in safety margins or functional capability of the airplane	Significant increase in workload or in conditions impairing crew efficiency					
Minor	Physical effects but no injury to occupants	Slight reduction in safety margins or functional capability of the airplane	Slight increase in workload. Implementation of countermeasures (such as new flight plan)					
No Effect	None	No effect on safety or operational capability of the aircraft	No effect on crew workload					

Imperative to reduce risk to a lower level

Acceptable risk

17

MSE | MASTER OF SCIENCE IN ENGINEERING

MSE SE.SCS: 1309

Descriptive Word		Qualitative Definition
Extremely Improbable		Not anticipated to occur during the **entire operational life of all airplanes** of one type
Extremely Remote		Not anticipated to occur **in the life of a single airplane** but may occur at sometime during operational life of all airplanes of one type
Improbable		Not anticipated to occur in the life of a single airplane but **may occur occasionally** during operational life of all airplanes of one type
Probable		**Anticipated to occur** at sometime during the life of an airplane

18

Safety Assessment Methods

FHA – Functional Hazard Assessment

Top-down approach

Identifies and classifies potential failure conditions by severity (Catastrophic, Hazardous, Major, Minor, No Effect) and to describe them in functional and operational terms.

FHA should provide:

I. Identification of related Failure Condition(s)
II. Identification of the effects of the Failure Condition(s).
III. Classification of each Failure Condition based on the identified effects (Catastrophic, Hazardous, Major, Minor, or No Safety Effect) and assignment of the necessary safety objectives.
IV. A statement outlining what was considered and what assumptions were made when evaluating each Failure Condition (e.g., adverse operational or environmental conditions and phase of flight).

- loss of function:
  - total loss: the function cannot be performed anymore
  - partial loss: the function can still be performed somehow but: reduced effectiveness, increased difficulty and using alternative means.
    Focuses on *functions*, not *equipment*.
- Malfunction:
  - erroneous operation
  - function is performed incorrectly (erroneous indication of airspeed)

1 Function	2 Failure Condition (Hazard Description)	3 Phase	4 Effect of Failure Condition on Aircraft/Crew	5 Classification	6 Reference to Supporting Material	7 Verification
Decelerate Aircraft on the Ground	Loss of Deceleration Capability	Landing /RTO/ Taxi	See Below			
	a. Unannunciated loss of deceleration capability	Landing /RTO	Crew is unable to decelerate the aircraft, resulting in a high speed overrun.	Catastrophic		SI8 Aircraft Fault Tree
	b. Annunciated loss of deceleration capability	Landing	Crew selects a more suitable airport, notifies emergency ground support, and prepares occupants for landing overrun.	Hazardous	Emergency landing procedures in case of loss of stopping capability	SI8 Aircraft Fault Tree
	c. Unannunciated loss of deceleration capability	Taxi	Crew is unable to stop the aircraft on the taxi way or gate resulting in low speed contact with terminal, aircraft, or vehicles.	Major		
	d. Annunciated loss of deceleration capability	Taxi	Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs.	No Safety Effect		
	Inadvertent Deceleration after V1 (Takeoff/RTO decision speed)	Takeoff	Crew is unable to takeoff due to application of brakes at the same time as high thrust settings, resulting in a high speed overrun.	Catastrophic		SI8 Aircraft Fault Tree

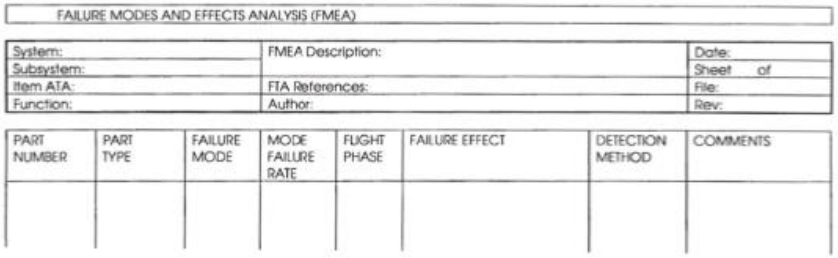
FMEA – Failure Modes and Effects Analysis

Bottom-up analysis identifying failure modes of a system, item and function and their system-level effects.

- **Functional FMEA** → analysis is performed at functional level
- **Piece Part FMEA** → analysis is performed at component level

Procedure

I. Tabulate all component parts of the equipment
II. Identify all foreseeable failure modes for each part
III. Identify the effects of each failure mode on the operation on the given level and at higher level
IV. Determine the detectability (failure indication or latency)



FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

System:	FMEA Description:	Date:
Subsystem:		Sheet of
Item ATA:	FTA References:	File:
Function:	Author:	Rev:

PART NUMBER	PART TYPE	FAILURE MODE	MODE FAILURE RATE	FLIGHT PHASE	FAILURE EFFECT	DETECTION METHOD	COMMENTS

Outputs:

- Helps in identify how the system is most likely to fail (especially single point of failure)
- Points to failures that are most difficult to detect
- List actions to prevent causes or to detect failure modes
- Allows to identify areas of the system that have the largest impact
- Provides a foundation for maintainability and logistics analyses
- Determines the MTBF (Mean Time Between Failure) and MTBCF (Mean Time Between Critical Failures)

FTA – Fault Tree Analysis

Top-down analysis starting from a system failure and tracing causes. Start with the failure condition, then determine causes of this event.

Qualitative: Minimal combinations of components failure resulting in system failure.

Quantitative: Probability or Frequency of the specific system failure

Qualitative	Quantitative
Minimal Cut sets Combination of component failures causing system failure	**Numeric probabilities** Probability of system and cut set failures
Qualitative Importance Qualitative ranking of contributions to system failures, direct cause vs. contributory via fail-safe	**Quantitative Importance** Quantitative ranking of contributions to system failure
Common Cause Potentials Minimal cut sets potentially susceptible to a single failure cause.	**Sensitivity Evaluations** Effects of changes in models and data errors determinations.

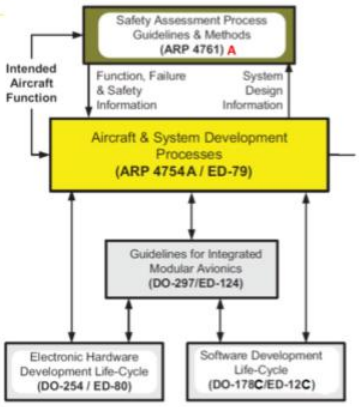
When do we have to carry out an FTA analysis?

(SAE ARP4761)

(*) Major Failure condition may be satisfactory analyzed also with less rigorous methods (e.g. FMEA with failure rates)

Rebecca Nauli (naulireb)

Development Assurance Level (DAL): SAE-ARP-4754A



SAE Society of Automotive Engineers

ARP Aerospace Recommended Practice

DAL: **Development Assurance Levels (DALs)** reduce the likelihood of design and development errors in aviation systems. Process based approach.

Failure Classification (FAR/CS 29)

Classification	**Effect**	**Example Probability**
No Effect	No effect on safety	$P \geq 10^{-3}$
Minor	Slight reduction in safety margin	$\leq 10^{-3}$
Major	Significant reduction in safety margins	$\leq 10^{-5}$
Hazardous	Large reduction in safety margins	$\leq 10^{-7}$
Catastrophic	Loss of rotorcraft	$\leq 10^{-9}$

Classification	Description	Safety Effects	Rotorcraft Capabilities	Workload	Transients	Probability	Probability
No Effect	NO EFFECT. Failure Conditions that would have no effect on safety; for example, Failure Conditions that would not affect the operational capability of the rotorcraft or increase crew workload, however, could result in an inconvenience to the occupants, excluding the flight crew.	No effect on safety	No effect on the operational capability of the rotorcraft	No increase in crew workload	Inconvenience to the occupants excluding flight crew	May be Frequent	$P \geq 10^{-3}$
Minor	MINOR. Failure conditions which would not significantly reduce rotorcraft safety, and which would involve crew actions that are well within their capabilities. Minor failure conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as, routine flight plan changes, or some physical discomfort to occupants.	No significant reduction in rotorcraft safety (slight reduction in safety margin)	Slight reduction in functional capabilities	Slight increase in crew workload such as routine flight plan changes. Required crew actions that are within their capabilities.	Some physical discomfort to occupants.	May be Reasonably probable	$P \leq 10^{-3}$
Major	MAJOR. Failure conditions which would reduce the capability of the rotorcraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew work load or in conditions impairing crew efficiency, physical distress to occupants, possibly including injuries, or physical discomfort to the flight crew.	Significant reduction in safety margins	Failure conditions which would reduce the capability of the rotorcraft, significant reduction in functional capabilities	Failure conditions which would reduce the ability of the crew to cope with adverse operating conditions. significant increase in crew workload or in conditions impairing crew efficiency	Physical distress to occupants, possibly including injuries, or physical discomfort to the flight crew.	Must be no more frequent than Remote	$P \leq 10^{-5}$
Hazardous	HAZARDOUS/SEVERE-MAJOR. Failure conditions which would reduce the capability of the rotorcraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be: (A) A large reduction in safety margins or functional capabilities; (B) Physical distress or excessive workload such that the flight crew's ability is impaired to where they could not be relied on to perform their tasks accurately or completely; or, (C) Possible serious or fatal injury to a passenger or a cabin crew member, excluding the flight crew. NOTE: Hazardous/Severe-Major failure conditions can include events that are manageable by the crew by use of proper procedures which, if not implemented correctly or in a timely manner, may result in a Catastrophic Event.	A large reduction in safety margins.	Failure conditions which would reduce the capability of the rotorcraft; large reduction in functional capabilities;	Failure conditions which would reduce the ability of the crew to cope with adverse operating conditions to the extent that there would be excessive workload such that the flight crew's ability is impaired to where they could not be relied on to perform their tasks accurately or completely	Physical distress such that the flight crew's ability is impaired to where they could not be relied on to perform their tasks accurately or completely. Possible serious or fatal injury to a passenger or a cabin crew member, excluding the flight crew.	Must be no more frequent than Extremely Remote	$P \leq 10^{-7}$
Catastrophic	CATASTROPHIC. Failure Conditions which would result in multiple fatalities to occupants, fatalities or incapacitation to the flight crew, or result in loss of rotorcraft.	Loss of rotorcraft	Loss of rotorcraft	Loss of rotorcraft	Multiple fatalities to occupants, fatalities or incapacitation to the flight crew.	Must be no more frequent than Extremely Improbable	$P \leq 10^{-9}$

Descriptive Word	Qualitative Definition	Proba-bility
Extremely Improbable	Not anticipated to occur during the entire operational life of all airplanes of one type	10^{-9}
Extremely Remote	Not anticipated to occur in the life of a single airplane but may occur at sometime during operational life of all airplanes of one type	10^{-7}
Improbable	Not anticipated to occur in the life of a single airplane but may occur occasionally during operational life of all airplanes of one type	10^{-5}
Probable	Anticipated to occur at sometime during the life of an airplane	10^{-3}

Development Assurance

The concept of DAL has been introduced to **minimize the number of errors** that will remain at **the end of the development of Software and Complex Electronic Hardware (Item DAL/IDAL)**. Recently, the DAL concept has **been extended to functions and overall system development (Function DAL/ FDAL).**

DAL Concept:

Ensures adequate rigor in development activities — higher safety risk ⇒ higher assurance level.

DAL in numbers
General Principle for Large Transport Aircraft FAR/CS-25

- DAL A development gives confidence that the manifestation of a possible remaining error is compliant with an Extremely Improbable probability class defined as $P \leq 10^{-9}$ /fh.
- DAL B development gives confidence that the manifestation of a possible remaining error is at least compliant with the Extremely Remote probability class defined as 10^{-7} /fh$\geq P > 10^{-9}$ /fh.
- DAL C development gives confidence that the manifestation of a possible remaining error is at least compliant with the Remote probability class defined as 10^{-5} /fh $\geq P > 10^{-7}$ /fh.
- DAL D development gives confidence that the manifestation of a possible remaining error is at least compliant with the Probable probability class defined as 10^{-3} /fh $\geq P > 10^{-5}$ /fh.

- **Software DALs**: A (highest) → E (lowest)

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

Software: RTCA DO-178C - Software Consideration in Airborne System and Equipment Certification, mostly about project management and software engineering

Key Processes (DO-178C/DO-254):

- Planning,
- Development,
- Verification,
- Configuration Management,
- Quality Assurance, and
- Certification Liaison.

➔ **Fail-Safe Principle**

Common Cause Analysis (CCA):

The Common Cause Analysis provides the tools to verify:

1. Independence between functions, systems or items
2. Lack of independence is acceptable

CMA – Common Mode Analysis:

is performed to verify that failure events are independent in the actual implementation.

- performed throughout the safety assessment process
- qualitative analytical tool used to ensure the goodness of the design
- Design Experience is used to inspect integration of components
- scope and extend to be defined and agreed on before
- requirements verified should be in checklist for design review
- should be done early to avoid unnecessary discussions later
- detail of the checklists depends upon the degree of complexity or novelty of the technology or system

Candidates for CMA

a. Software development errors
b. Hardware development errors
c. Hardware failures
d. Production/repair flaw
e. Stress related events (e.g., abnormal flight conditions, abnormal system configurations)
f. Installation errors
g. Requirement errors
h. Environmental factors (e.g., temperature, vibration, humidity, etc.)
i. Cascading faults
j. Common external source faults

It should consider:

- Development
- Manufacturing
- Installation
- Maintenance
- Crew errors
- Failure of components

PRA – Particular Risk Analysis:

is performed to verify that events outside the system concerned do not violate failure independence claims. Particular risks are defined as those events outside the system(s)

that may violate failure independence claims Different analysis for different risks. There is no one-fits-all method! → e.g. lightning strike

- An assessment of possible multiple system and structure damages from a single source
- Not based on probability of occurrence as per 25.1309, but assumed to happen (Probability = 1)
- Analysis provides a damage status of the aircraft following the event and assesses the remaining capability of the aircraft.

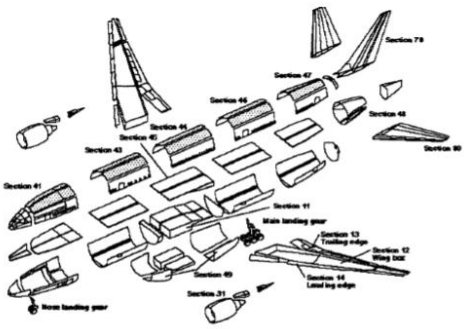
Example of Particular Risks

a. Fire
b. High Energy Devices (Engine Rotor Burst, APU, Fans)
c. Leaking Fluids
d. Hail, Ice, Snow
e. Bird Strike
f. Tread Separation from Tire
g. Wheel Rim Release
h. Lightning
i. High Intensity Radiated Fields
j. Flailing Shafts
k. Bulkhead Rupture

ZSA – Zonal Safety Analysis:

is performed on each zone of the aircraft to ensure that the installation meets the safety requirements with respect to:

- Basic Installation
- Interference Between Systems
- Maintenance Errors



Manned vs. Unmanned Systems

High Reliability Organisations (HRO)

An organisation that is able to:

Conduct relatively error free operations

- ➔ to achieve this, you need to care about failures
- Over a relatively long period of time
- making consistently good decisions

Conduct high quality and reliable operations

Create and sustain a mindful culture

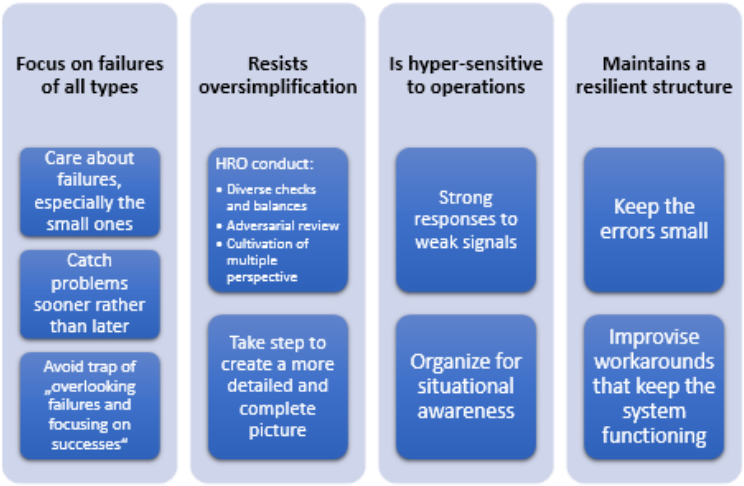
- ➔ catch errors before they occur or are fatal

What do they share in common? → Reliability

Common attributes

- Complexity
- Complex management
- Human life always at stake
- Multiple internal and external factors
- Fast moving and evolving situations

A mindful culture



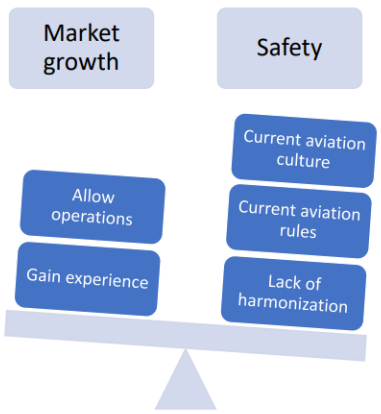
Few typical behaviours (by HROs)

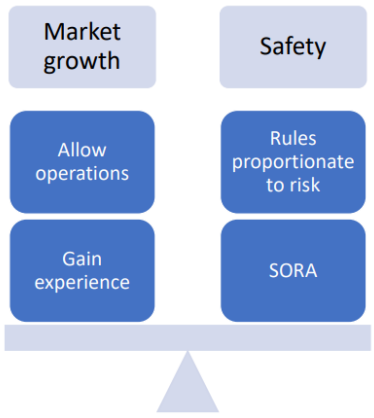
European Commission

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - COM(2014) 207 final

“An enabling legal framework would not only provide the rules to manufacture the air-craft, but also, even more importantly, gradually allow operations, starting from simple operations and growing in operational complexity. This would put operators in a position to gain valuable practical expertise and progressively develop their businesses”

“The regulatory framework should reflect the wide variety of aircraft and operations, keep rules proportionate to the potential risk and contain the administrative burden for industry and for the supervisory authorities”

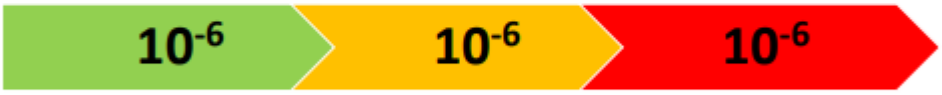


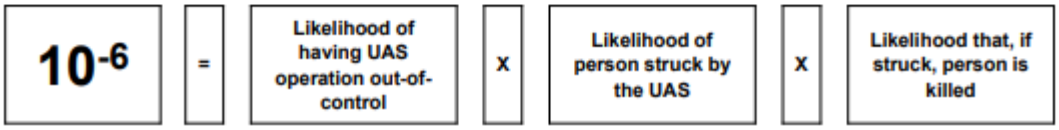


JARUS & EASA Airworthiness Categories

Open Category (A)	Specific Category (B)	Regulated Category (C)
• 3 operational Subcategories A1, A2, A3 • 5 UAV Categories C0-C4 • Within direct visual contact (VLOS) • Max. 120m AGL • No Flights over crowds • No UAV heavier than 25kg	Changes a lot, therefore "unknown"	• Traditional Type Certificate • Instructions for Continued Airworthiness • Standard Airworthiness Certificate
Represents very low risk operations. No/limited airworthiness regulations are envisaged and 1309 is not applicable.	Operations that would present a limited risk to people and property. Risk mitigation would be required, mainly through operational restrictions and limitations, but which may include 1309, depending on the type of operation and the nature of the risks.	Follows the traditional approach to aircraft regulation, including type-certification where compliance with 1309 would be mandatory.

Target Level of Safety
As numbers of fatal injuries on ground per flight hour





Specific operations

- Wide variety of operations, very difficult to categorize
- Wide range of expertise among applicants
  - Small start-ups (no money, no time, great people)
  - Photographers with NO aviation experience
  - Meteorologists with NO aviation experience
  - Military
- Wide range of RPAS
  - COTS (e.g. Phantom S-800)
  - Amateur built
  - Custom built for specific operation
- Huge economic potential if allowed to grow
- Human life not always at risk

Problem with current airspace

The current airspace was never designed for UAS.

- Very Low Level (VLL) Airspace was never thought to be navigable
- Current Airspace rely on See and Avoid
- UAS have very specific operation and equipment

Operators wishing to operate within manned airspace were required to do extensive airspace characterization and modelling to prove that it was safe to fly the UAS with an acceptable MAC risk rate.

MAC = Mid Air Collision

- ➔ Air-SORA tries to simplify/alleviate the amount of work required to the operator to demonstrate to CAA that a reasonable level of safety can be achieved for the UAS MAC Risk Rates with manned aircraft
- ➔ The approach is qualitative

Detect and Avoid

Gliders and Paragliders both operate below 500 ft AGL, how to avoid collision? → See and avoid

Detect and Avoid (DAA): The capability to see, sense or detect conflicting traffic and take the appropriate action. 'Detect and Avoid' is the combination of 'Separation Assurance' and 'Collision Avoidance'

Vigilance is also necessary to avoid collisions

Safety in manned aviation

Airworthiness

Measure of an aircraft's suitability for safe flight (design, manufacturing, operation and maintenance).

An operation is sufficiently safe to accept the risk when:

- ✓ The Organization behind the Operation is approved to accepted standards
- ✓ They use a crew, which is approved to accepted standards
- ✓ They use aircrafts which design, production & maintenance as well as the organizations behind are approved to accepted standards

SORA process

SORA: Specific Operations Risk Assessment

Air Risk Model

The purpose of the Air Risk Model for the Specific Operation Risk Assessment (Air-SORA) is to propose a method for the collision risk assessment and means of compliance for small UAS to:

- ICAO Annex 2 section 3.2
- 14 CFR 91.113
- SERA 3201
- additional requirements by different states.

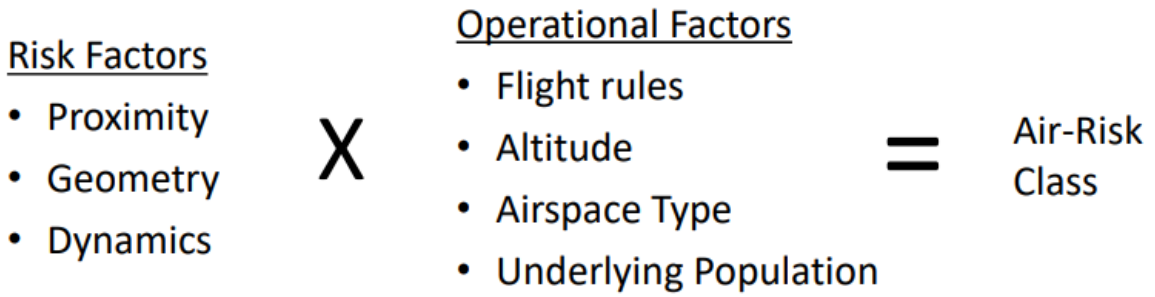
SORA Air Risk Model (Air-SORA):

- Provide a holistic DAA model that should guide both the operator and the CAA in establishing whether an operation can be conducted in a safe manner under the requirements in ICAO Annex 2, Section 3.2.

- It is not a checklist
- Does not provide answers to all the challenges of DAA.
- Designed to help the operator and CAA in determining the UAS risk of collision and to develop a means to determine mitigations required for safe operations for UAS which fall under the EASA "specific" category
- It does not contain prescriptive requirements but rather objectives to be met at various levels of robustness.

CAA = Civil Aviation Authorities

Qualitative Approach to Air Risk



1. **Proximity** - The more aircraft in the airspace, the higher the rate of proximity, the greater the risk of collision.
2. **Geometry** - An airspace which sets or allows aircraft on collision courses increases risk of collision.
3. **Dynamics** - The faster the speed of the aircraft in the airspace the higher the rate of proximity, the greater the risk of collision.

Ground Risk Model

The approach is to reach a specific Target level of safety (TLS). TLS = A generic term representing the level of risk which is considered acceptable in particular circumstances. Main elements of the Ground Risk Model:

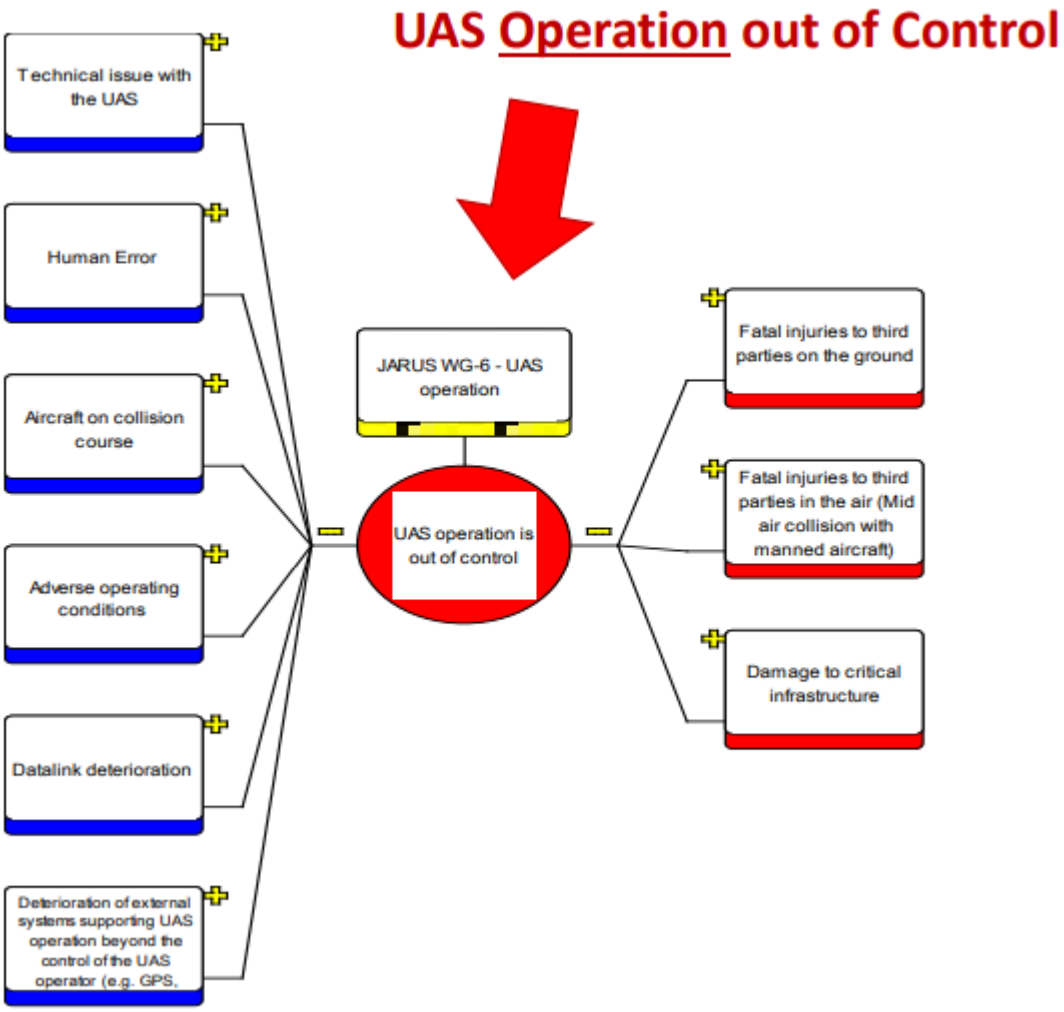
- Population density
- Shelter Effects
- Impact Area
- Factor for Casualties

Elements of an operational authorization

- Description of the intended mission
- Total Hazard and Risk Assessment
- Safety Concept for every risk
- Emergency concept for when all safety barriers fail
- Realization of the safety barriers

- Documentation

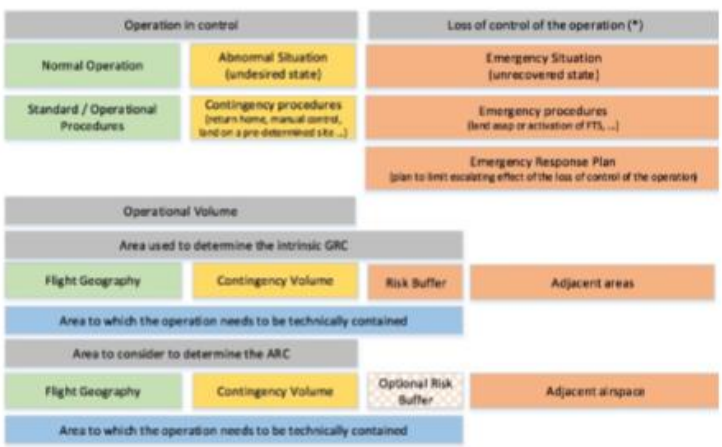
Holistic Risk Model

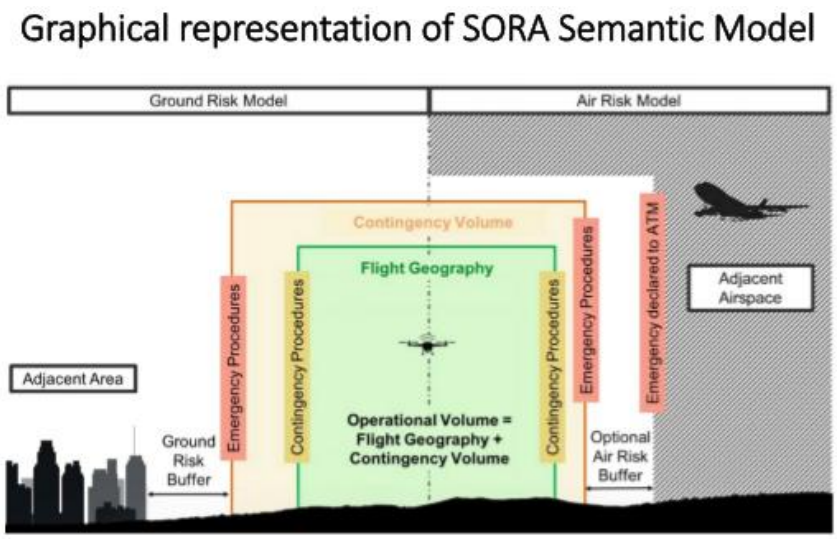


Semantic Model

The Loss of control of operation corresponds to situations:

- Where the outcome of the situation highly relies on providence; or
- Which could not be handled by a contingency procedure; or
- When there is grave and imminent danger of fatalities



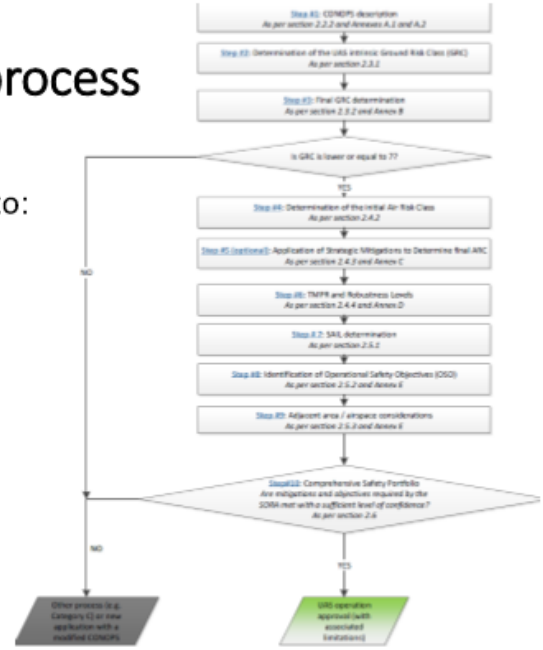


MSE MASTER OF SCIENCE IN ENGINEERING

The SORA process

A 10-step feedback approach into:

- defining an operation (ConOps)
- Assessing the risk
- Mitigating the risk
- Address residual risk
- Creating the documentation

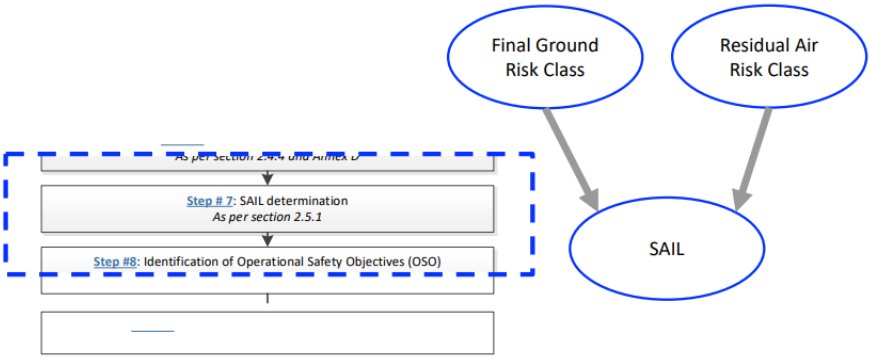


SAIL

SAIL – Specific Assurance and Integrity Level

Assurance: The planned and systematic actions necessary to provide adequate confidence that a product or process satisfies given requirements.

Integrity: Attribute of a system or an item indicating that it can be relied upon to work correctly on demand.



What is robustness in SORA?

ROBUSTNESS = INTEGRITY + ASSURANCE

INTEGRITY = SAFETY GAIN

How useful is the barrier to improve the safety of the operation?

ASSURANCE = PROOF Is the claimed safety gain proven?

The SAIL will define the associated objectives to be met in order to establish a sufficient level of confidence that the likelihood of losing control of the UAS operation is commensurate with the proposed ConOps. The SAIL represents the level of confidence that the UAS operation will stay under control.

The level of confidence represented by the SAIL is not quantitative but instead corresponds to:

a. Objectives to be complied with
b. Description of activities that might support the compliance with those objectives
c. Evidence to indicate the objectives have been satisfied.

A SAIL is assigned to the ConOps using Table 5

SAIL Determination				
	Residual ARC			
Final GRC	a	b	c	d
≤2	I	II	IV	VI
3	II	II	IV	VI
4	III	III	IV	VI
5	IV	IV	IV	VI
6	V	V	V	VI
7	VI	VI	VI	VI
>7	Category C operation			

Table 5 – SAIL determination

Applying SAIL

OSO = Operational Safety Objectives

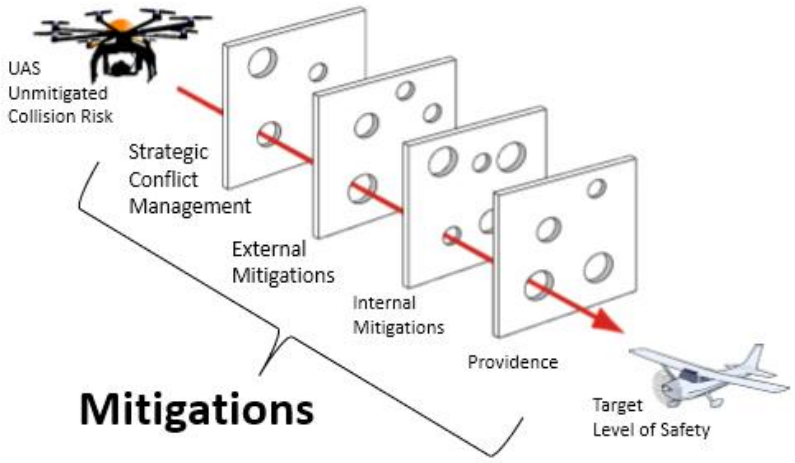
TECHNICAL ISSUE WITH THE UAS		LEVEL of INTEGRITY		
		Low (SAIL III)	Medium (SAIL IV)	High (SAIL V & VI)
OSO #05 **UAS is designed considering system safety and reliability**	Criterion	The equipment, systems, and installations are designed to minimize[1] hazards[2] in the event of a probable[3] failure of the UAS or of any external system supporting the operation.	Same as Low. In addition, the strategy for detection, alerting and management of any failure or combination thereof, which would lead to a hazard is available.	• Major Failure Conditions are not more frequent than Remote[4]; • Hazardous Failure Conditions are not more frequent than Extremely Remote[4]; • Catastrophic Failure Conditions are not more frequent than Extremely Improbable[4]; • No single failure can lead to a Catastrophic Failure Condition; • Software (SW) and Airborne Electronic Hardware (AEH) whose development error(s) may cause or contribute to hazardous or catastrophic failure conditions are developed to an industry-standard or a methodology considered adequate by the competent authority and/or in accordance with means of compliance acceptable to that authority[5].
	Comments	*[1] The minimization of hazard criterion correlates to the contribution of the UAS and of any external system supporting the operation to the loss of control of the operation rate, thus the SAIL of the operation. As an example, at SAIL III, the contribution of the UAS and of any external system supporting the operation to the loss of control of the operation rate could be 10-4/FH assuming a traditional 10% contribution of the technical aspects to the safety of an operation.* *[2] For the purpose of this assessment, the term "hazard" should be interpreted as a failure condition that relates to major and hazardous (the term "Catastrophic" is intentionally not included since the TLOS is considered met for SAIL I to IV operations with the provision of Note 1 above and, if applicable M2 requirements in Annex B).* *[3] For the purpose of this assessment, the term "probable" should be interpreted in a qualitative way as, "Anticipated to occur one or more times during the entire operational life of a UAS".*	*N/A*	*[4] Safety objectives may be derived from JARUS AMC RPAS.1309 Issue 2 Table 3 depending on the UAS class or an equivalent risk-based methodology acceptable to the competent authority.* *[5] Development Assurance Levels (DALs) for SW/AEH may be derived from JARUS AMC RPAS.1309 Issue 2 Table 3 depending on the UAS class or an equivalent risk-based methodology acceptable to the competent authority.*

TECHNICAL ISSUE WITH THE UAS		LEVEL of ASSURANCE		
		Low (SAIL III)	Medium (SAIL IV)	High (SAIL V & VI)
OSO #05 UAS is designed considering system safety and reliability	Criterion	A Functional Hazard Assessment[1/2] and a design and installation appraisal[3] that shows hazards are minimized are available.	Same as Low. In addition: • Safety assessment are conducted in line with standards considered adequate by the competent authority and/or in accordance with a means of compliance acceptable to that authority. • A strategy for the detection of single failures of concern includes pre-flight checks.	Same as Medium. In addition, safety assessment and development assurance activities are validated by a competent third party.
	Comments	*[1] Severity of failure conditions (No Safety Effect, Minor, Major, Hazardous and Catastrophic) should be determined according to the definitions provided in JARUS AMC RPAS.1309 Issue 2.* *[2] UK CAA CAP 722A Volume 2 section 2.4 named "Section 3 – Safety features of the UAS" or Eurocae ED-280 "Guidelines for UAS safety analysis for the specific category (low and medium levels of robustness)" may be considered by the applicant to support compliance with this criterion (FHA).* *For SAIL III and IV, Eurocae ED-280 "Guidelines for UAS safety analysis for the specific category (low and medium levels of robustness)" may be considered acceptable by the competent authority to support compliance with this criterion (FHA).* *[3] A simple written justification from the operator including functional diagrams and a description of how the system works explaining why the integrity claim is met is an acceptable means of compliance.*	*For SAIL IV, Eurocae ED-280 "Guidelines for UAS safety analysis for the specific category (low and medium levels of robustness)" may be considered acceptable by the competent authority to support compliance with this criterion.*	*N/A*

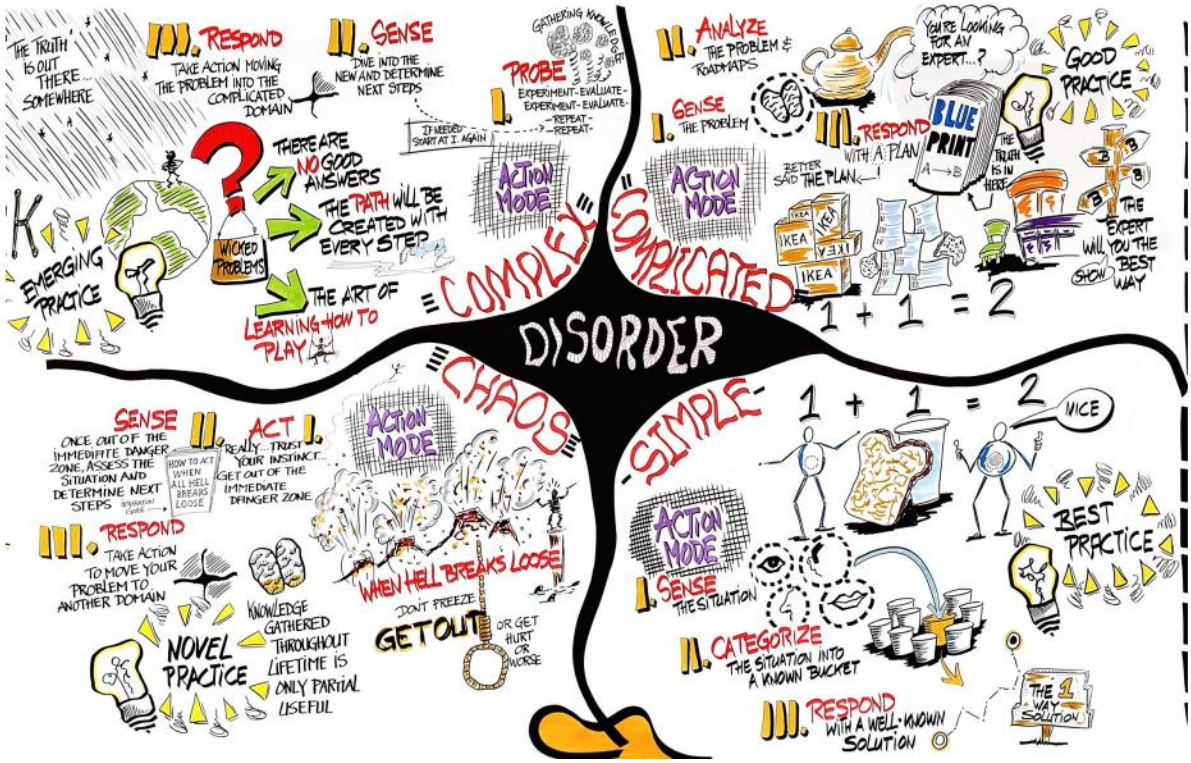
MSE MASTER OF SCIENCE IN ENGINEERING

zh aw

Reason mitigation model (Swiss Cheese)



Complexity, Byzantine Problems, Robustness, Redundancy, Dissimilarity



Complexity

Cambridge dictionary: The state of having many parts and being difficult to understand or find an answer to.

Oxford dictionary: The state or quality of being intricate or complicated.

B. Edmonds(*): Complexity is that property of a model which makes it difficult to formulate its overall behaviour in a given language, even when given reasonably complete information about its atomic components and their interrelations.

System Complexity

SAE-ARP-4754A - Guidelines for Development of Civil Aircraft and Systems

COMPLEXITY: An attribute of functions, systems or items, which makes their operation, failure modes, or failure effects difficult to comprehend without the aid of analytical methods.

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

COMPLEXITY: An attribute of systems or items which makes their operation difficult to comprehend. Increased system complexity is often caused by such items as sophisticated components and multiple interrelationships.

The Byzantine Generals Problem

A type of failure - described in some literature as a story about Byzantine-era generals trying to coordinate an attack, with possible traitors among the generals and/or their messengers. The point of this story is mutual agreement - agreement wins, disagreement looses. "Byzantine" is not synonymous with "bizarre".

"Byzantine" has a precise meaning which deals with failure behaviour that works against reaching agreement.

Safecomp 2003:

- Byzantine fault: any fault that presents different symptoms to different observers.

- Byzantine failure: the loss of a system agreement service due to a Byzantine fault

Byzantine Failure

The Byzantine Generals Problem

- Generals = processors
- Messengers = data network communication

→ Any operational data link between redundant devices must exist for some type of agreement.

→Even asynchronous systems without voting need "equalization" to prevent divergence.

→ It is nearly impossible to create a highly dependable system without Byzantine Fault tolerance.

Random and Systematic Failures

SAE-ARP-4761

FAILURE: A loss of function or a malfunction of a system or a part thereof.

COMMON MODE FAILURE: An event which affects a number of elements otherwise considered to be independent.

Random Failures: A failure that can happen at any given time during the lifetime of the equipment, e.g. degradation of parts of hardware.

Systematic Failures: A failure that is the results of an error in the design process, manufacturing process, etc.; e.g. software design errors, hardware design errors, requirement specification errors and other operational procedures.

Robustness

ROBUSTNESS: The ability of a system to tolerate variations in system parameters without undue degradation in performance.

- Which system parameters?

In practice any parameter that defines the operating condition of my system around which I make my design.

Aviation generic: Airspeed, Dynamic Pressure, Outside Temperature, Acceleration, Electromagnetic Interference, High Intensity Radiated Field, etc.

System specific: Hydraulic Pressure, Electromagnetic Compatibility, Modelling Error, Wear, etc.

- How large should the variations be?

Example 1: Temperature range in cockpit for cabin equipment

Example 2: Aircraft load factor response to longitudinal stick input

→ It is always difficult to foresee which are the plausible variations in system parameters

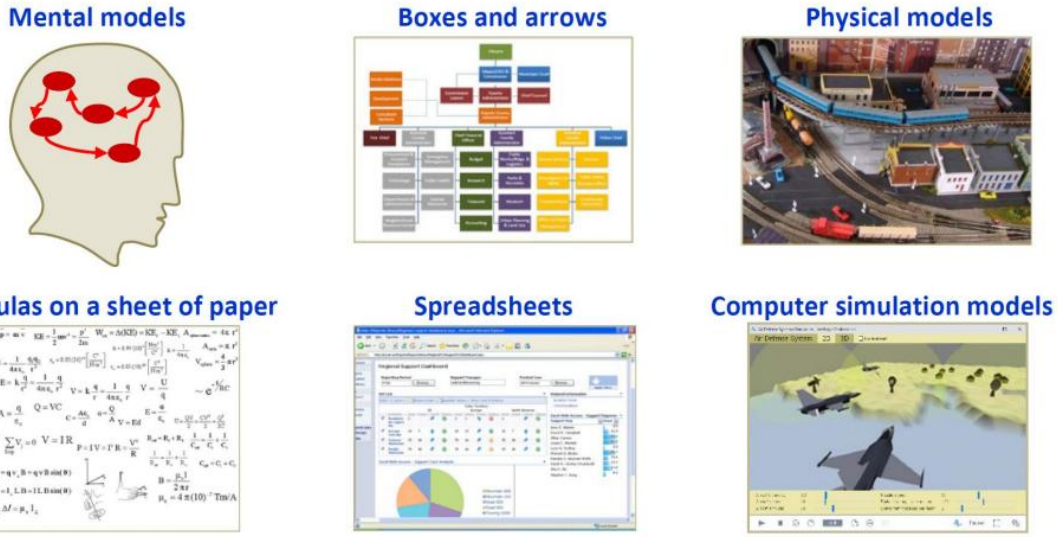
- How degraded can the performance be?

As a general statement: the aircraft in the most degraded condition must be able to perform safe flight and landing. The words ‘continued safe flight and landing’, according to AMC 25.1309, mean the capability for continued controlled flight and landing, possibly using emergency procedures, but without requiring exceptional pilot skill or strength. Some aircraft damage may be associated with a failure condition, during flight or upon landing.

Modelling, Simulation and Testing of SCS

Modelling

Modelling is one of the ways to solve problems that appear in the real world. In many cases we cannot afford finding the right solutions by experimenting with real objects. We build a model of a real system → This process assumes abstraction: we throw away the details that (we think) are irrelevant to the problem we are trying to solve and keep what we think is important. The model is always less complex than the original system.



Types of Simulation

- **Stand-Alone Simulation**: running on a single computer / machine / workstation
- **Parallel Simulation**: simulation load is distributed over different processors
- **Distributed Simulation**: running on multiple computers / machines / work-stations
- **Continuous**: Equations representing the models are written in continuous time and integrated accordingly using specific integration methods. e.g. Water Tank →$WaterInTank = \int_0^t WaterFlow(t)dt$
- **Discrete**: Equations representing the model are written in discrete time domain. e.g. Counter → $c_{k+1} = c_k + 1$; e.g. Water Tank → $WaterInTank_{k+1} = WaterInTank_k + WaterFlow_k \cdot \Delta T$
- **Multi-Rate**: The model is Discrete and contains sub-parts running at different time increments. e.g. Network of computers communicating on a digital bus.
- **Hybrid**: Model is composed of part that are continuous and parts that are discrete. e.g. Flight Control Computer closing the loop on a Hydraulic Actuator → FCC Discrete + HydAct Continuous
- **Off-Line**: Simulation time is not related to solar time. e.g. response of the aircraft model to a gust

- **Real-Time**: Simulation time correspond with solar time
- **Soft-Real-Time**: Real-Time simulation performed with non-real-time operating systems such as: Standard Linux or Windows.
- **Pilot-In-The-Loop**: Human (pilot) interacts with simulation (that should be real-time) e.g. response of the aircraft to a pilot input
- **Hardware-in-The-Loop**: Some parts of the system are not simulated but actually interfaced with the model itself. e.g. displays are feed by data generated by the simulation model

Analytical vs. Simulation Modelling

There is a large class of problems where the analytic solution does not exist (or is extremely complicated to find).

Dynamic Systems:

- Non-linear behaviour
- States ("Memory")
- Non-intuitive influences between variables
- Time and causal dependencies
- All above combined with uncertainty and large number of parameters

Level of Abstraction

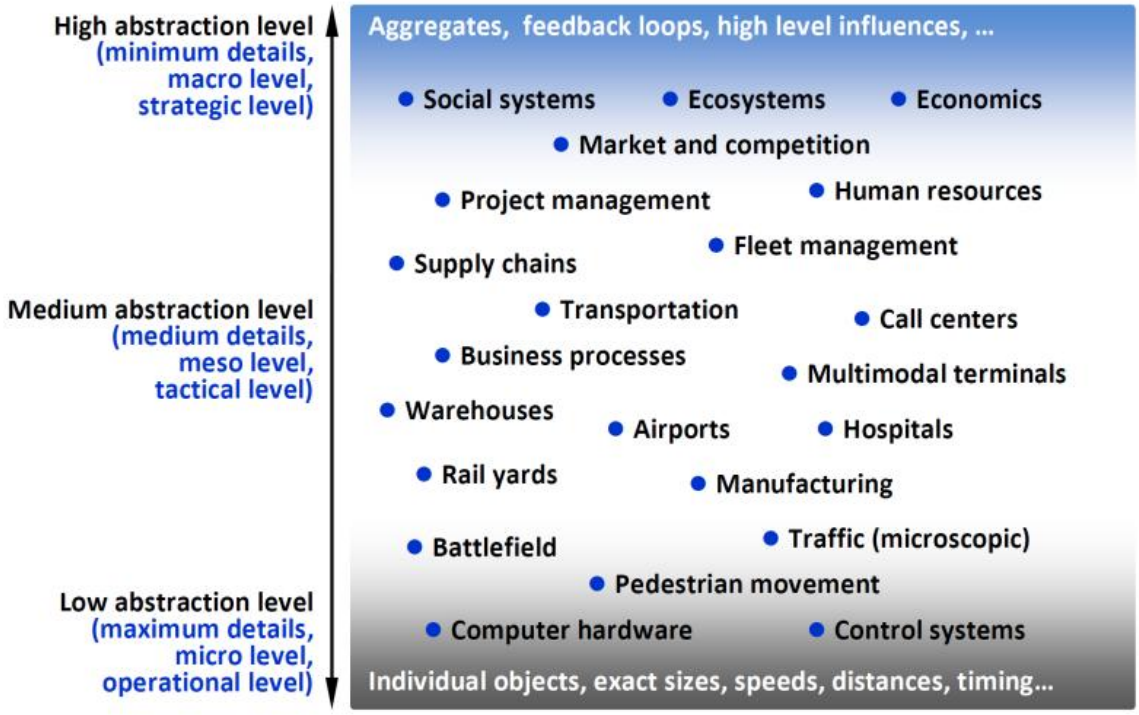


Figure 1.8 Applications of simulation

- Choosing the right abstraction level is critical to the success of the modelling project. Once you have decided what do you include in the model and what is

left below the level of abstraction, the choice of the modelling method and the actual "coding" of the model is quite straightforward.
- In the model development process, it is normal and even desirable to periodically reconsider the abstraction level. Typically, you would start with high abstraction and add details as they are needed.

Methods

Method or General Framework for mapping a real-world system to its model:

• **System Dynamics**: approach to understand the nonlinear behaviour of complex systems over time using stocks, flows, internal feedback loops, table functions and time delays. https://web.mit.edu/sysdyn/sd-intro/

• **Discrete Event Modelling**: A discrete-event simulation (DES) models the operation of a system as a (discrete) sequence of events in time. https://en.wikipedia.org/wiki/Discrete-event_simulation

• **Agent-Based Modelling**: In agent-based modelling (ABM), a system is modelled as a collection of autonomous decision-making entities called agents. https://www.pnas.org/content/99/suppl_3/7280

Modelling for AC/ AC systems design

- Modelling requirements for aircraft / aircraft system design and verification embody requirements from several disciplines
- Analyses and investigations to be conducted during the different phases of the design require different levels of detail
- Maximum level of accuracy is used throughout the process of verification
- Development and verification need some sub-modules to be exported from the simulation model to other simulation/analysis tools (such as real-time simulators, specific design tools, Iron Bird, etc.) and vice versa
- The need to fulfil such tasks by the same tool leads to the creation of highly versatile simulation models

→ "Model requirements" is no longer addressed only to mathematical modelling, but also to the structure and the flexibility of the simulation model

→Available simulation environment will strongly drive the design process and affect the timetable and the costs

→Modelling of the various items that form a modern aircraft shall be carried out taking care of the implications of approximations

Modelling for design

Challenges:

- Aerodynamic data analysis & validation (aircraft stability and control analysis, aerodynamic tables and build-up implementation, parameters identification, etc.)
- Systems architecture design (such as sensors, actuators, data filtering and processing)
- Mathematical modelling of aircraft motion, aerodynamics data set, servos, sensors, engine, hydraulic system, etc.

→ Validation of models through analysis and comparison

Modelling Environment

Commercial Code / Freeware: Aerodynamics:

- VSAERO: 3D Aerodynamic Analysis
- Ansys Fluent: fluid simulation software
- …

Structures:

- Nastran: Finite Element Analysis Program (with Aerolastic)
- …

Mechanical Engineering:

- ADAMS: Multibody Dynamics Simulation Solution
- CATIA: Computer Aided Design
- …

Flight Mechanics / Systems:

- Matlab / Simulink
- MATRIXx / SystemBuild
- Scilab / Scicos
- Dymola
- …

Software Development:

- SCADE: model-based development environment for critical embedded software
- Matlab / Simulink
- …

Custom Developed:

- C / C++
- Fortran
- Python
- ...

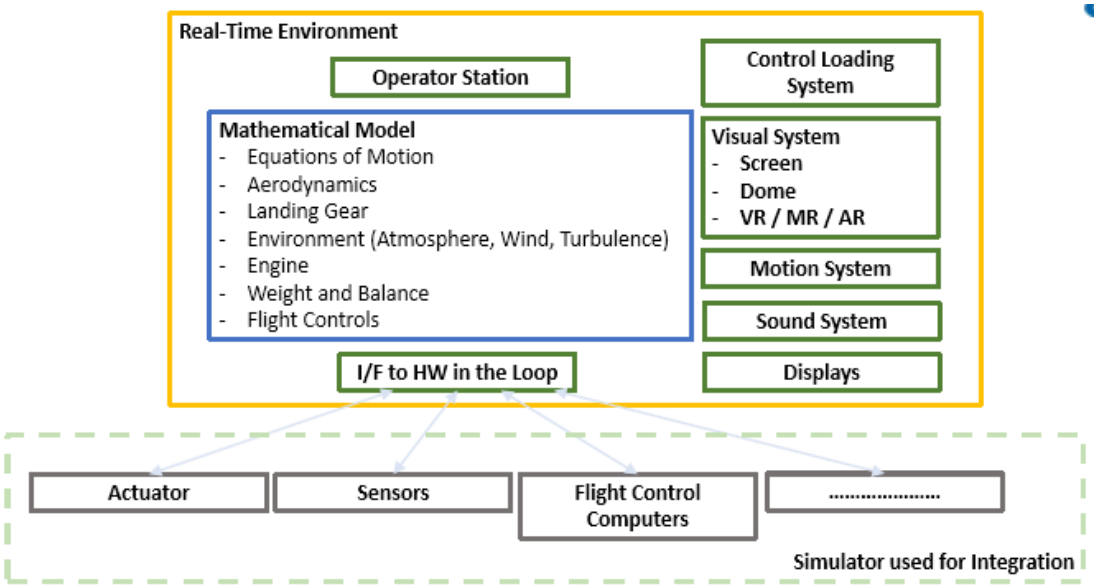
→ Need to somehow integrate these items to create a simulation model

Modelling of Dynamic Systems

1. Understanding the Real System
   The first and the most important step is always to gain a very good understanding of the system that we want to model
2. Writing the Equations
   Once the system is well understood the EOM can be written on the basis of the physical relationship that exist between the input, the states and the outputs
3. Layout of the Simulation Model
   The Layout of the model is an important phase where we decide how to iteratively solve the EOM
4. Initialization & Simulation
   Simulation of the model can be achieved by numerical integration, but we must define a starting point.

Simulation

Simulator Components



Training vs. R&D flight simulator

Training simulator	R&D flight simulator
• used for operational training	• no certification required* • main goals

• qualified according to (Europe) EASA CS-FSTD(A)
• Four categories
  ○ Full Flight Simulator (FSS)
  ○ Flight Training Device (FTD)
  ○ Flight Navigation Procedures Trainer (FNPT)
  ○ Basic Instrument Training Device (BITD)
• Depending on categories, flight hours can be booked as in a real aircraft
• cost effective training environment
	○ study of human-machine interaction
	○ evaluation of Handling qualities
	○ Development of AC and Its Systems
	• Used by AC manufacturers and research Institutes

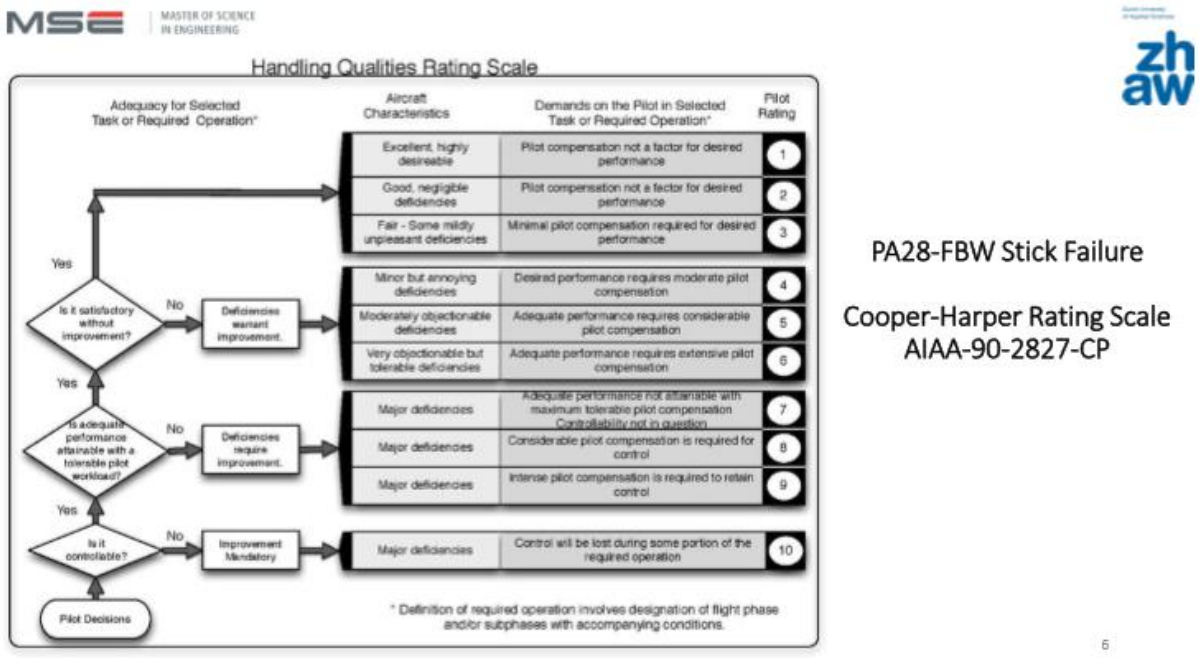
**Development models do not require certification but validation if certification credits is sought*

From Design to Test

Design: Requirement capture, design choices, interface definition, identification of relevant parameters, etc.

Development: model validation, system development support, function development, etc.

Test: compute expected results, run test with H/W in the loop and/or Pilot-in-the-loop

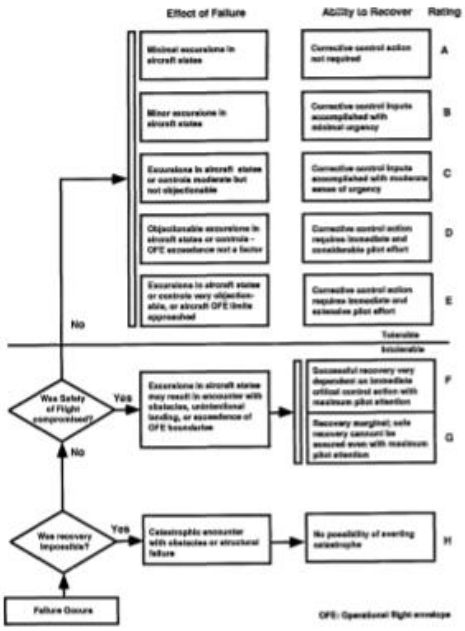


MSE | MASTER OF SCIENCE IN ENGINEERING

zh aw

PA28-FBW Stick Failure

Failure/Recovery Rating Scale
AIAA-90-2827-CP



Human Aspects in Engineering – Safety Critical Systems

Human in the System

Networks within Organisations

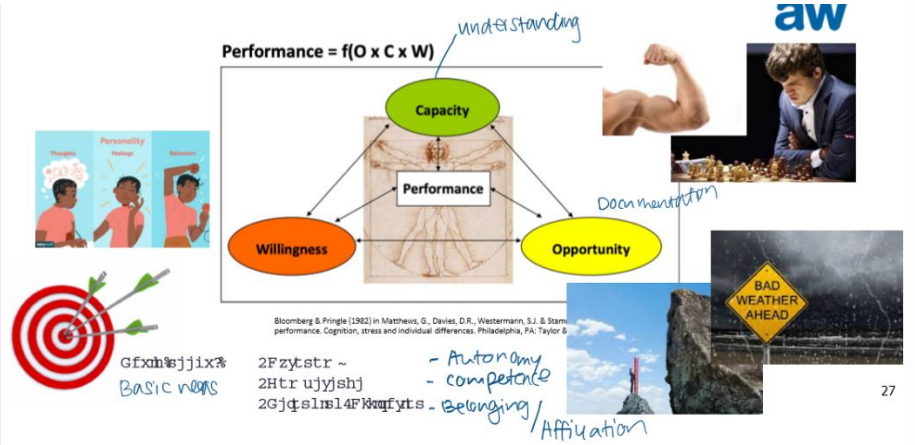
- Technical
- Structural
- Social

Human Performance Limitations (HPL)

How Humans manage threats:

- A beginner's traps: lack of experience
- an experts' trap. overgeneralisation
- inconspicuous threats: first of a kind incident
- fixed mindset: error due to misinterpretation
  - goal-serving interpretation
  - confirmation bias: I see what I expect
- complacency and learning history with routine threats
  - situation awareness
  - behaviour
  - group dynamic

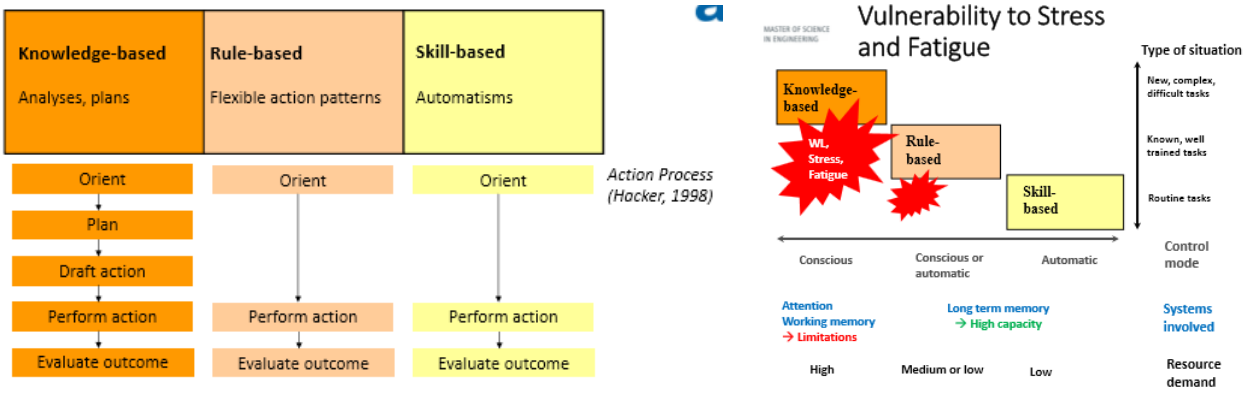
Performance Determinants

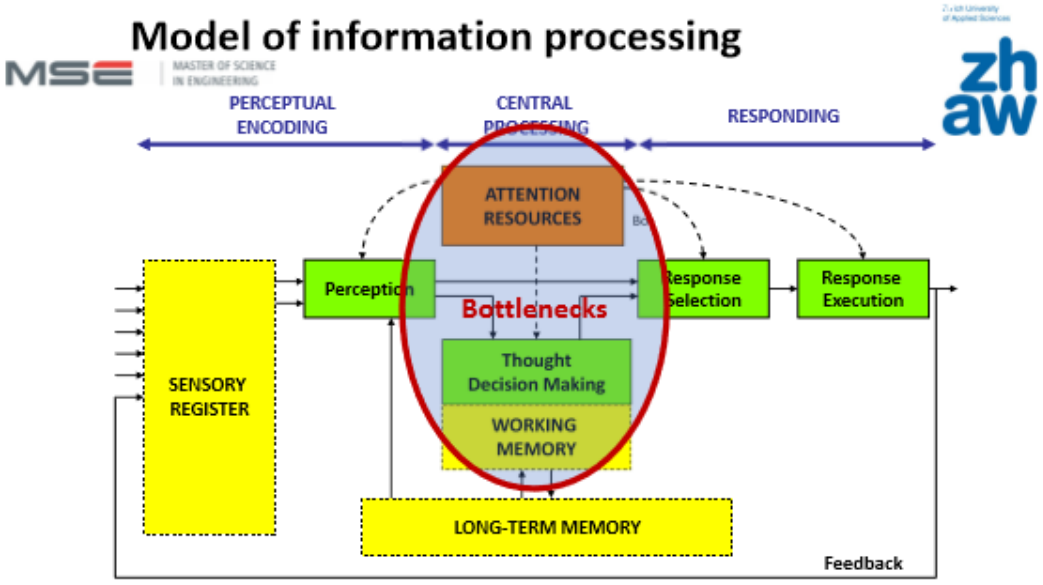


Adaptation: in psychology, adaptation corresponds to a process by which individuals or groups make necessary or desirable adjustments (cognitive, behavioural or affective) – in response to new environmental

conditions or requirements, to meet their basic needs or functions and to achieve a good quality of life.

Modes of Action Control



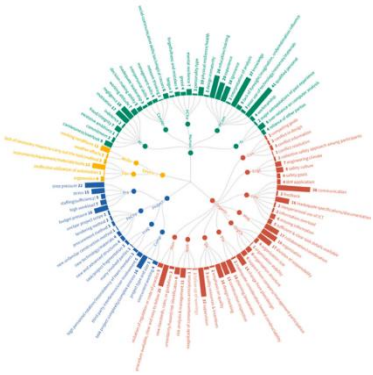


20.10.2025 Wickens, C. D., Gordon, S. E., & Liu, Y. (1998). An introduction to human factors engineering (p. 147). New York (etc.): Longman. 32

Model of Skills for Social Interaction

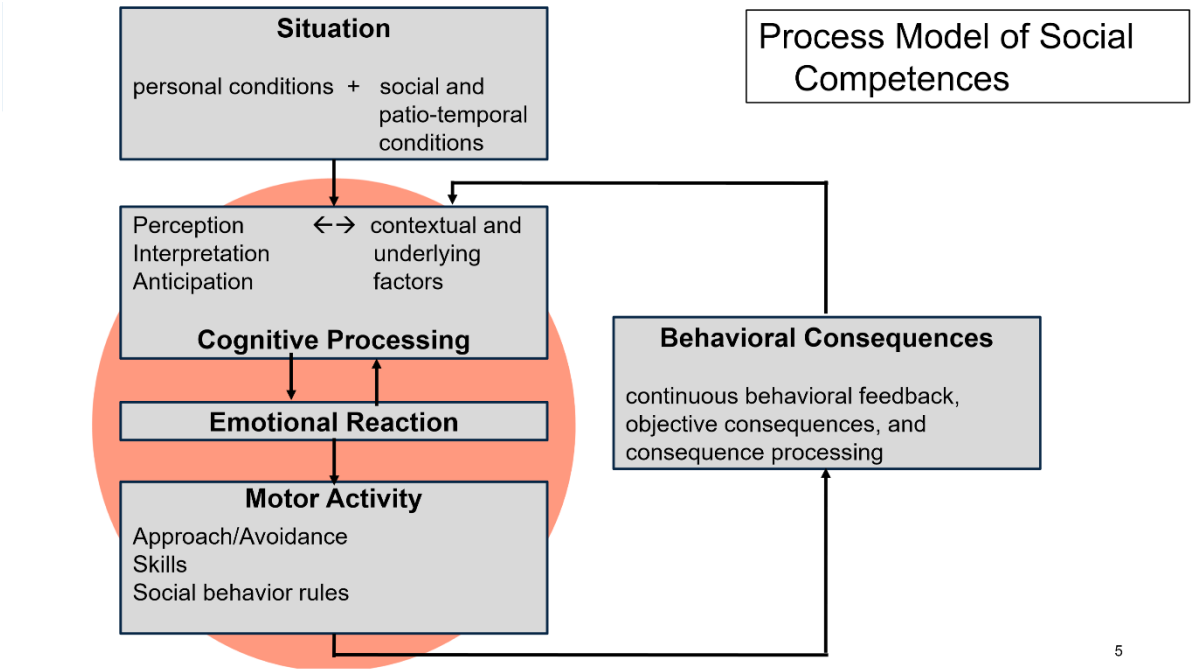
Human and Organisational Factors Affecting Safety

- **Human**:
  - Qualified personal (41)
  - Knowledge (37)
  - Education/training (26)
- **Organisational**:
  - Communication (38)
  - Supervision (33)
  - Procedure (25)



- **Project-related**:
  - Time pressure (22)
  - Budget pressure (16)
  - Task project complexity (16)
- **Environmental**:
  - Instruments/equipment (15)
  - Working conditions (11)
  - Ergonomics (4)

2



5

Item	Additional Explanation
Situational Aspects	personal conditions: • My own plans, • intentions, • interests, • moods and needs social and patio-temporal conditions: • People involved: number, age, sex, behaviour, distribution of roles. • Rules and conventions specific to situation • Cultural and societal background • Time of day • Characteristics of the location

Cognitive Processing	Attention control and social perception →Requirement and task nature
Emotional Reaction	e.g., helplessness, anger, fear, courage and determination
Motor Activity	• Perceive task (do not avoid it) • Combination of behaviours to cope with task • Rules in social context
Behavioural Consequences	Adapt to reaction of environment Short-term vs. long-term consequences* Internal processing of consequences: (a) Experience as a success/failure (b) Reinforce myself positively/rebuke oneself * C+ present: positive reinforcement with a reward (◊ healthy behaviour) C- present: punishment with a negative consequence C+ eliminated: extinction C- eliminated: negative reinforcement with avoiding something aversive (◊ unhealthy behaviour)

Personality

Motivation

Motivation — is the internal process that initiates, guides, and sustains goal-directed behaviour. It is what drives a person to act, whether it's achieving a goal, fulfilling a need, or responding to an external stimulus. Motivation can be **intrinsic** (coming from within, like personal interest, satisfaction or curiosity) or **extrinsic** (coming from external factors, like rewards, recognition, or avoiding punishment).

Key Aspects of Motivation

- Activation (& direction): the decision to start a certain behaviour.
- Intensity: the level of effort put into the behaviour.
- Persistence: continuing the behaviour over time despite obstacles.

Motivators

In psychology, needs and motives are central to understanding why people act.

Needs: Needs are essential **conditions for survival, psychological growth, and wellbeing**. They are more universal and fundamental. E.g., Maslow's hierarchy of needs [1]: from physiological to self-actualization needs.

Deci and Ryan (1985; 2000) reframed motivation by proposing that all humans share **three innate psychological needs** that are essential for **optimal functioning and self-determination**.

- **Autonomy:** the experience of volition and psychological freedom in one's actions. → Feeling the behaviour is self-chosen, not controlled
- **Competence**: the experience of effectiveness and mastery in interacting with the environment. → Feeling capable of achieving desired outcomes.
- **Relatedness:** the experience of belonging to a group and of connection with others → Feeling cared for and connected.

Motives: Motives are more specific energizing states that drive behaviour toward certain goals, often shaped by individual experiences and context. E.g., competition will attract achievement motivated individuals.

- Power motive (Machtmotiv)
- Achievement motive (Leistungsmotiv)
- Affiliative motive (Zugehörigkeitsmotiv)

Creating intrinsic motivation

Doing something for inherent enjoyment or interest is enhanced, when …

- basic needs (autonomy, competence, relatedness) are satisfied,
- … and formerly extrinsic motivation is internalized (taking on external goals as personally meaningful).

The frustration of the basic needs' leads to …

- controlled motivation (acting due to pressure or obligation) or
- amotivation (a lack of motivation).

Experts spend 4 h/d for ~ 10 years (10'000 h) in …

- intensive, deliberate practice (gezieltes Üben)
- improving/correcting errors/finding out

This allows them to …

- recognize underlying patterns (having an eye for something)
- reflect on intuition (why it works/doesn't work)
- Practice and use a refined repertoire of „hard wired" skills (fast and automatic)

Attitudes & Behaviours

Attitude: An attitude is a relatively enduring and general **evaluation of an object, person, group, issue, or concept** on a dimension ranging from negative to positive.

- Affective component: feelings and emotions toward the objective (e.g., enjoying jazz music)
- Behavioural component: Actions or intentions related to the object (e.g., attending jazz concerts; playing piano)
- Cognitive component: Beliefs and thoughts about the object (e.g., jazz music is intellectually stimulating)

Attitudes provide summary evaluations of target objects and are assumed to be derived from specific beliefs, emotions, and past behaviours associated with those objects [1]. Example: attitude towards cleaning – differences in expectations regarding cleaning rules in a shared apartment.

Attitudes are like conclusions from the past that work as procedures for the future.

Attitudes …

- … are learned
- …. automated thought processes providing a judgement about some object/matter
- … lead to automatic reactions in the situation
- … instead of processing information (perception)
- … prevent re-evaluation of the situation

Change of attitude by awareness and reflection

Reflection of (automatic) thinking underlying the „old“ attitude:

- how does it feel for me? (as if someone …)
- what experience do I link to this?
- what are my thoughts about this?
- what emotions get triggered by these thoughts?
- in what situations do they occur? What triggers them?

What can be changed?

- in my perception (what to focus on/look for)?
- in my thoughts? (how do I interpret …)
- about my feelings? (what could be good about it)
- about my goals? (is this really important?)
- in my behaviour? (what (else) can I do?

Mindset drives behaviour

Mindset Type	Core Belief	Behavior / Outcome
Fixed Mindset	"Intelligence is something you're born with."	Avoid challenges Fear failure Give up easily
Growth Mindset	"Intelligence can be developed through effort and learning."	Embrace challenges Persist after setbacks Improve over time

Learning Goal vs. Mastery Goal Orientation

Performance-Goal Orientation:
Focus on demonstrating competence relative to others — the goal is to look competent and gain favorable judgments.

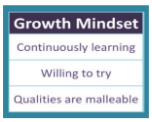
E.g., study maths to score highest in class or to exercising to avoid looking "dumb" in class.

- Belief in **giftedness, aptitude**
- Are competitive → win-lose

Mastery/Learning-Goal Orientation: Focus on developing competence, improving skills, and understanding – the goal is personal growth and mastery of a task.

E.g., study math problems not just to get a good grade, but to deeply understand the concepts or for the enjoyment of problem solving.

- Belief in **ability to learn, self-motivation**
- Cooperation/support → win-win



This can also be seen in practice: praise for effort not for result.

When teachers framed effort as the path to mastery – emphasizing learning, strategy, and persistence – students' motivation and performance improved significantly [1].

Praise for effort («you worked hard on this») lead to **resilience**, whereas **praise for intelligence** («you are so smart») **led to fragility**, as students avoided challenges to protect their «smart» identity. Praise for …

- Effort
- Strategy
- Endurance

Development of Personality

Personality: Personality refers to the characteristics and qualities that form a person's distinctive character, including physical, mental, emotional, and social characteristics of a person.

»The unique, relatively enduring internal and external aspects of a person's character that influence behaviour in different situations» (Schultz & Schultz, 2017, p. 6) such as

- Action-orientation vs. position-orientation in decision-making
- Extravert vs. introvert in relationships
- Optimistic vs. pessimistic attitude towards life

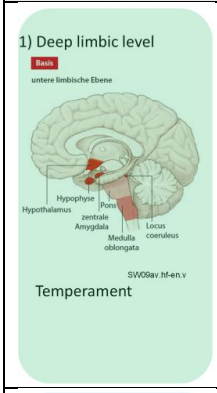
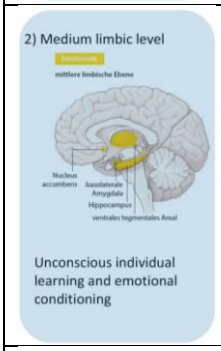
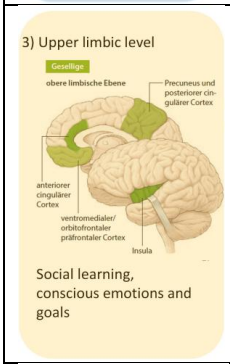
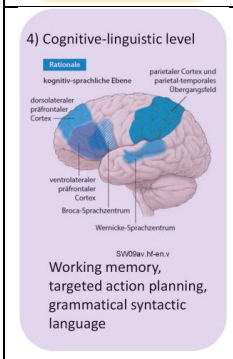
The heredity of personality is h2 = 0,5: 50%, i.e. 50% is determined by genetic factors

Personality is a matter of life-long learning:

- Social competences
- Self competences

The Big Five Personality Traits

1. Openness to experience (inventive/curious vs. consistent/cautious)
2. Conscientiousness (efficient/organized vs. extravagant/careless)
3. Extraversion (outgoing/energetic vs. solitary/reserved)
4. Agreeableness (friendly/compassionate vs. critical/rational)
5. Neuroticism (sensitive/nervous vs. resilient/confident)

Developmental Stages of Personality	Description
	Basic Pattern • Temperament, regulation of vegetative functions and innate behaviours relevant for survival are genetically determined. • Level 1 develops before birth, is minimally influenced by experience and education
	Individuality • Is based on unconscious emotional conditioning • Connects elementary emotions (fear, happiness, contempt, disgust, curiosity, hope, delusion etc.) with events of individual life. • Level 2 develops in first months and years after birth.
	Identity • Consists of conscious emotional-social learning: Pursuit for success, power, profit, recognition of fame, friendship, love, acceptance, moral and ethics. • Functions as social control of egoistic impulses from deep and lower limbic level • Functions as attention control. • Level 3 develops in late childhood and adolescence by socioemotional experience.
	Integrity • Feelings and motives* created in limbic levels are verbalized, thoughts are structured and put into order, behavioural goals internally mapped and maintained, compared with each other and with models. • Reflects how we like to see ourselves and like to be seen by others. • Level 4 develops over the entire life span. * Target classes we emotionally react to (e.g., belonging to a group, being first/best, ...)

Character Strengths that Catalyse Competences

Executive functions:

- Organizing and prioritizing
- Focusing on tasks
- Sustaining effort

- Managing frustration and emotions
- Accessing memory and recall
- Self-regulating actions

24 Character Strengths:

- Wisdom: creativity, curiosity, judgment, love of learning, perspective
- Courage: bravery, perseverance (grid), honesty, zest (enthusiasm)
- Humanity: love, kindness, social intelligence
- Justice: teamwork, fairness, leadership
- Temperance: forgiveness, humility, prudence, self-regulation (self-control)
- Transcendence: appreciation of beauty and excellence, gratitude, hope (optimism), humour, spirituality

The seven yellow-marked character strengths are considered game changers for success and happiness.

Interpersonal Skills

Situation Type	Social Skill	Goals	Manifestation
Enforcing Rights (Type R)	• You have a right to enforce your legitimate demands due to your role/position (e.g., buyer, boss, .regulator, etc.) • E.g., manager must confront an employee about their shortcomings and set consequences.	**Assertion** – self-confident behaviour, with skills such as maintaining eye contact, speaking loudly and clearly, and avoiding unnecessary apologies	Before: – Positive instruction: «I will make it», «It's my right» Speak loud and clear: – Keep eye contact. – Take a relaxed position. – Express your demands, wishes and feelings with I-message («Ich-Botschaft»). – First say what you want and then why. – Don't apologize. – Do not get aggressive, stay calm and determined. – Do not devalue your partner («you did it again»). – Express your understanding for partner's position.

Relationships (Type B)	– You have no legal authority, and you want to maintain or improve the relationship as you need to establish consensus by reaching an agreement. Expressing one's own feeling is personal and not debatable – as compared to any legitimization (that is not appropriate/according to standards). – E.g., A friend sells me his old car (Volvo cabriolet) as a "super model" for 6T CHF. Nevertheless, I need to invest a lot of money to get repairs done. I want to confront him and to reach a fair deal.	**Feelings** • Express one's feelings and needs and show understanding for the partner's feelings and needs • Express insecurities openly	• Before: – Be conscious about what you feel (anger, joy, etc.). – Think about what event triggered the feelings. – Use positive self-instruction («my feelings matter») Speak calmly: – Directly address your feelings «I am now …». – Describe the specific event that triggered your feelings from your own perspective «today, you … ». Avoid generalizations («you are always …», «you did it again») – Try to understand your partners feelings. – Express your wishes and needs how your partner should behave in this situation in future. – Express also positive feelings (authentically)

Seeking sympathy (Type S)	• No legitimate claim for one's own demands, they can only be met, if the person waives their own rights or a positive relationship can be established. • E.g., convincing a police officer not to issue a parking fine; networking for successful sales	**Flexible persuasion** • Present yourself as a likable person and motivate others to do a favour. • React flexibly to other's behaviour and situational conditions	Before: – Positive instruction: «I must try at least; I can't lose anything» – Establish contact Focus on creating a good conversation and atmosphere: – Reinforcement of others (show interest, listen, ask, give compliments and smile friendly. – Focus on situation and what/how things are said or done. – Keep eye contact. – Mirror your partner. – Talk about yourself, admit errors, weaknesses, insecurities.

Attribution of the cause

The attribution process refers to the way people explain the causes of behaviour and events — both their own and others'. It involves assigning causes to actions, often distinguishing between …

– internal (dispositional) factors, such as personality or motivation, and

– external (situational) factors, such as environment or luck.

Through this process, individuals try to make sense of why things happen, which influences how they perceive others, react emotionally, and behave socially.

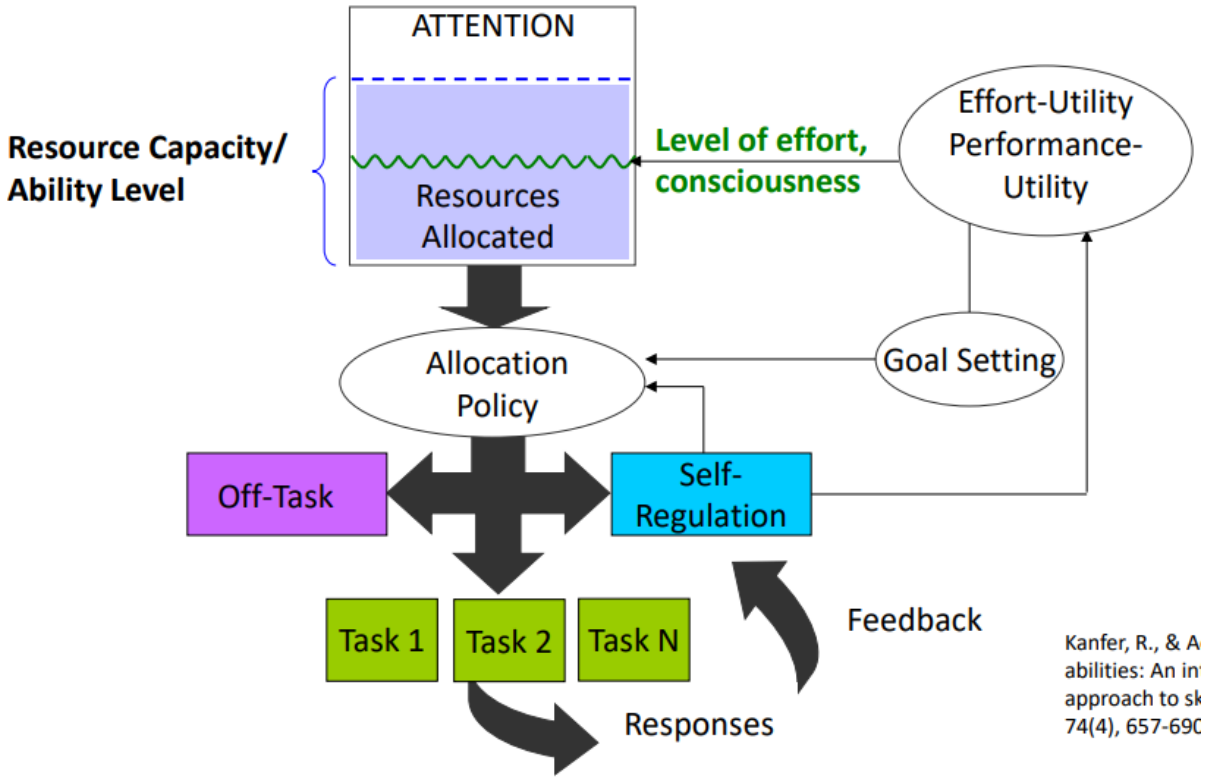
Stress and resilience

Workload

Workload: Workload is defined as ...

- Costs for executing tasks
- Energy consumption during task execution
- Competition for limited mental resourced
- Felt need to restrain from continuing work, need to recover.
- Experience of challenge
- Feeling of satisfaction

Capacity Model of Attention



Stress

Stress: Stress is an anxious state of tension triggered by anticipated negative outcomes and consequences:

• Perception of a substantial imbalance: physiological and psychological demands > capability to respond adequately

• The consequences of the (anticipated) failure to meet demands are relevant/severe.

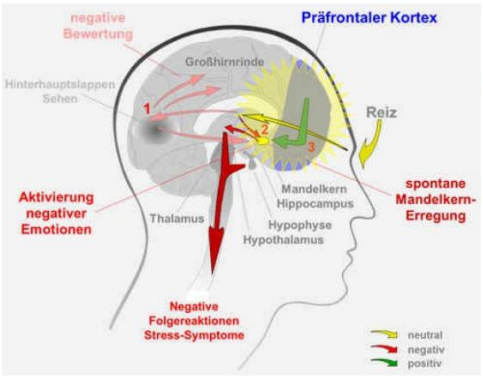
Stress is subjective

- cf. speaking in front of an audience

Workload vs. Stress

Workload	Stress
Challenge	Overload
Energy mobilisation is useful	… is ineffective
Effort increase & strategy change	FFF Fight, Flight, Freeze reaction
Rest, contentment, skills enhancement	no recovery, problem rumination

Information processing



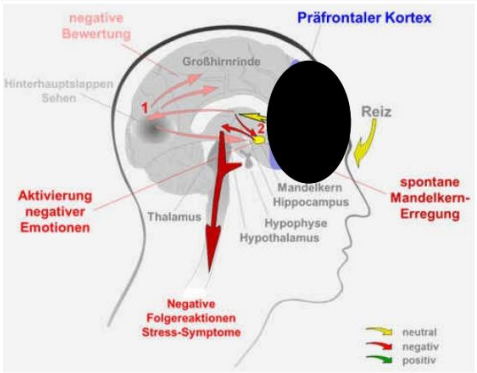
1. step: visual information processing

2. step: amygdala
   - Emotional activation

0: Challenge reaction
1: Threat reaction

3. step: PFC functions:
   - Emotional control
   - Reasoning
   - Judgement
   - Planning
   - Decision making

Risk-assessment
Re-evaluation



http://www.kriechbaum.eu/PKS.html

1. step: visual information processing

2. step: amygdala
   - Emotional activation

0: Challenge reaction
1: Threat reaction

3. Strong negative emotions inhibit prefrontal lobe (PFK) functions

   Under this condition stress makes you do stupid things!

X

~~Risk-assessment~~
~~Re-evaluation~~

Internal Drivers for Stress

- “Be perfect!”
- “Hurry up!”
- “Do your best / put your back into it!”
- “Please others!”
- “Be strong!”

Attitudes that make life hard(er)

- Everything has to be perfect.
- I have to be performant in any way.
- Everything has to be as I want it.
- I must be loved by everybody.
- Life must be easy.
- Absolute claims («must»)

Resilience

Resilience:	Resilience is the ability to bounce back from challenging and even stressful conditions.

Team

How to avoid them:

1. build trust
2. address conflicts/divergence in interests
3. generate commitment
4. have accountability for results among team members
5. attention to results

Trust

Concept	Definition	Explanation
Trust Invulnerability	Trust is choosing to be vulnerable and take risks	Trust builds on perception of **Ability**: individual strengths and weaknesses **Benevolence**: spend time, face-to-face, care about others **Integrity**: do what you say (walk the talk)
Psychological safety	Psychological safety is a sense of confidence the team will not embarrass, reject, or punish someone for speaking up.	1. build relationship first 2. dare to ask "stupid" questions/reward brave questions 3. give everyone a voice Beware of traps: expert halo and dominance by extraverts and senior team members

Bring up conflicts

Artificial harmony!

- Acknowledge that conflict is required for productive meetings
- Rules for engaging in conflict
- Hold people responsible to bring up and discuss conflicting information (no gossiping)
- Address problems and issues quickly (non-verbal signs)

- Get everyone's' perspective and opinion
- Weigh differences as important

Agreement is not required, acknowledgment is necessary.

Rules of Handling Conflicts

- Be respectful
    - not personal
    - very specific
    - show appreciation
- I feel … (I-Messages)
    - For me the consequences are …
- Listen actively + paraphrase
    - mirror emotion
- care + empathy

Life constantly disturbs the balance of our brain: Perception and anticipation of discrepancies, disappointment and disrespect can create emotions and tension.

Selective interpretation of information: bad intentions, mean motives, difficult personality.

- These feelings and corresponding thoughts/assumptions create a perspective and a tendency for certain goals and actions that lead to … separation, self-protection, attack for resistance
- Can create "concept of the enemy"

What is Necessary to Connect / Stay Connected to Others

Theory of mind (ToM) is about how we attribute mental states of ourselves and others. Having a theory of mind allows us to understand that others have unique beliefs and desires that are different from our own ones, enabling us to engage in daily social interaction as we interpret the mental states and infer the behaviours of those around us (Premack & Woodruff, 1978)

- What do we expect others to believe and feel and how will this possibly affect their behaviour?
- How adequately do expected intentions match with other people's actual intentions?

Lack of differentiation in ToM: Columbian ex-terrorists' moral judgement of another person's error is guided by the outcome instead of integrating intention and outcome (social cognition): the man is dead → intention was evil

Perspective Taking, Empathy and Connecting

Social experience is the fundament.

Example: Compassionate rats

Social experience drives helping behavior

Conclusion: familiarity matters

… availability of memories

… similarity … (cf. principles of memory organization)

The art of being connected is based on interpersonal skills, relationship building and is crucial for the capability to positively deal with conflicts.

Culture of Addressing Conflicts starts with Relationship building

- Needs first relationship building and trust → being connected
- Acknowledges basic needs of everybody Self-determination theory: competence, autonomy, affiliation
- Is aware of prior experience/conditioning: … conditioning of Athenian vs. Trojan toddlers on trusting others
- Can be changed Robert Sapolsky: baboon colony switches from hierarchical culture with strong rivalry to culture of affiliation

"Level 4-Thinking" for Empathy (Accurate ToM) Find explanations for annoying behaviours of others / ask questions

- „S/he is just like me sometimes"…
    - Sometimes not paying attention, not being aware of
    - Being in a hurry
    - Being fed up
- "S/he is bothered because her/his goals can't be met"
- "S/he is probably afraid of losing …"
    - Face
    - Position/Status
    - Control
    - Self-Confidence (Souveränität)

Commitment

Anti: Ambiguity

- Passive, no buy-in, therefore continue discussions again and again due to hidden conflicts Clarity and Buy-in →alignment on team objectives
- Clarity on direction and priorities: avoid assumptions and ambiguity

- High engagement of team members
- Clarify what was been agreed upon in meetings
- Keep record about commitments
- Commitment does not require consensus (suitable solution, sufficiently safe, no harm expected)

Solution oriented Interaction

Focus:

- What keeps the problem alive?
- What resources do we have to change this?

Assumptions:

- Circularity of behaviours (e.g. drinking – blaming – drinking - ...)
- Constructivism: interpretation in the context of subjective experiences
- Cybernetics: systems behave dynamically

Tasks:

• Initiate, maintain and guide process to find options to solve problem ◊ questioning

• Create commitment → contracting

Finding Options

- What might be helpful to achieve ...?
- How should it look like for you in order to make sense?
- Do you remember examples from the past, where it worked well? What would someone else say, what you did differently at that time?
- What do you think, when you get started doing it differently: how do I recognize, that you are ...?
- If you want to start ... in x weeks, what do you first need to do/learn in order to successfully master that step?
- How would your work situation change, if you received full support and positive feedback on your next step/task accomplishment/presentation?
- If I asked a colleague about your strengths, what would he or she say? What is the cause for you to think, your colleagues would say this?

Create Commitment

- What would show that it actually happens/the solution gets realized?
- What would be an example of successful accomplishment? What? Where? When? How often? With whom?
- Who else could recognize the change? How would he/she recognize?

- On a scale from 1 to 10 (10 = expectations fulfilled and 1 = none of them fulfilled), …
    - Where are we right now?
    - Where do we like to be?
    - What would show us, we are there?
    - What would rise the probability that this would happen?
    - How? When? How often? With whom?
- Suppose the goal would be achieved,
    - what would you do differently compared to now?
    - What needs would be fulfilled?
    - What would be the consequences?

Accountability for Contributions

Anti: Low standards

- Problem: Passive, no buy-in, revisited discussions again and again

Therefore do …

- regularly compare performance with goals and standards
- provide authentic feedback to improve performance
- apply the same standards to everybody

Providing Personal Feedback and Establish Learning Culture

Providing Feedback

- About progress
    - What did improve?
    - What changed?
- Discrepancy
    - Compared to expectations and what was committed
    - What did not meet the expectations?
- Initiation of next steps

Feedback and Debriefing

Asking the right questions

Questions

- what, how, when, where
- not why

… to analyse

- performance on a global level

- performance in specific detail

Self-Debriefing Method Example

The project meeting turned out to be a .... success/failure.

- How satisfied are you with this meeting? ... with specific aspects e.g. quality of the contributions to the concept/plan, quality of the interaction, openness to new aspects/problems, ...?
- How did you feel in your role as ... (e.g. moderator)?
- Who has contributed to the result and how was it generated?
- What was good about it, what didn't work well?
- What made you think your plan could work? Is there a discrepancy between the plan for and result of the meeting?
- What can you improve next time and how?
- What could possibly have happened/gone wrong if additional challenges occurred?
- ...

Self-Debriefing vs. Instruction

Instruction is useful for beginners to build up standard repertoire for handling the tasks. Self-Debriefing does not instruct how to do things. It is interested in the process that has led to the performance result. What made people think their approach was good? It helps people detect specific aspects that trigger and drove their behaviour. It gives them control over learning process.

Enhancing metacognitive strategies (think focused on the process of problem solving, not the problem itself)

Enhancing Learning Culture

Fixed mindset: competitiveness → win-lose

Fixed Mindset	Growth Mindset
Must be perfect	Continuously learning
Fear of failure	Willing to try
Qualities set in stone	Qualities are malleable

Growth mindset: cooperation/support → win-win

Effective Praise in Training

Fixed Mindset Students

Believe	Intelligence is set
Goal	To look smart
Mistakes	Proof they have lost their giftedness
Challenge	Fearful: To try and fail = no longer smart
Difficult Task	Give up
Praised for	Being intelligent

Growth Mindset Students

Believe	Brain is like a muscle
Goal	To learn
Mistakes	Problem to be solved
Challenge	Excited: See as opportunity to learn
Difficult Task	Work harder
Praised for	Effort, process, persistence

Practice Your Feedback Skills!

• It all starts with having agreed on the solution (commitment)

• What will be done, how and why

• Challenge your teammates perception and judgement of accomplishment

• On a scale from … how well did you do? How much of the goal is achieved?

• What is the reason for discrepancies?

• How could this be changed?

• Next steps

Attention to Results

Anti: Status and ego

• Collective results should get more important than ego-driven aspects (status, career aspiration)

• Focus: Potential of collective achievements

• Support objectives that help achieve overall goal

Degree of Participation Example: Ecological Turnaround in Samsö, DK

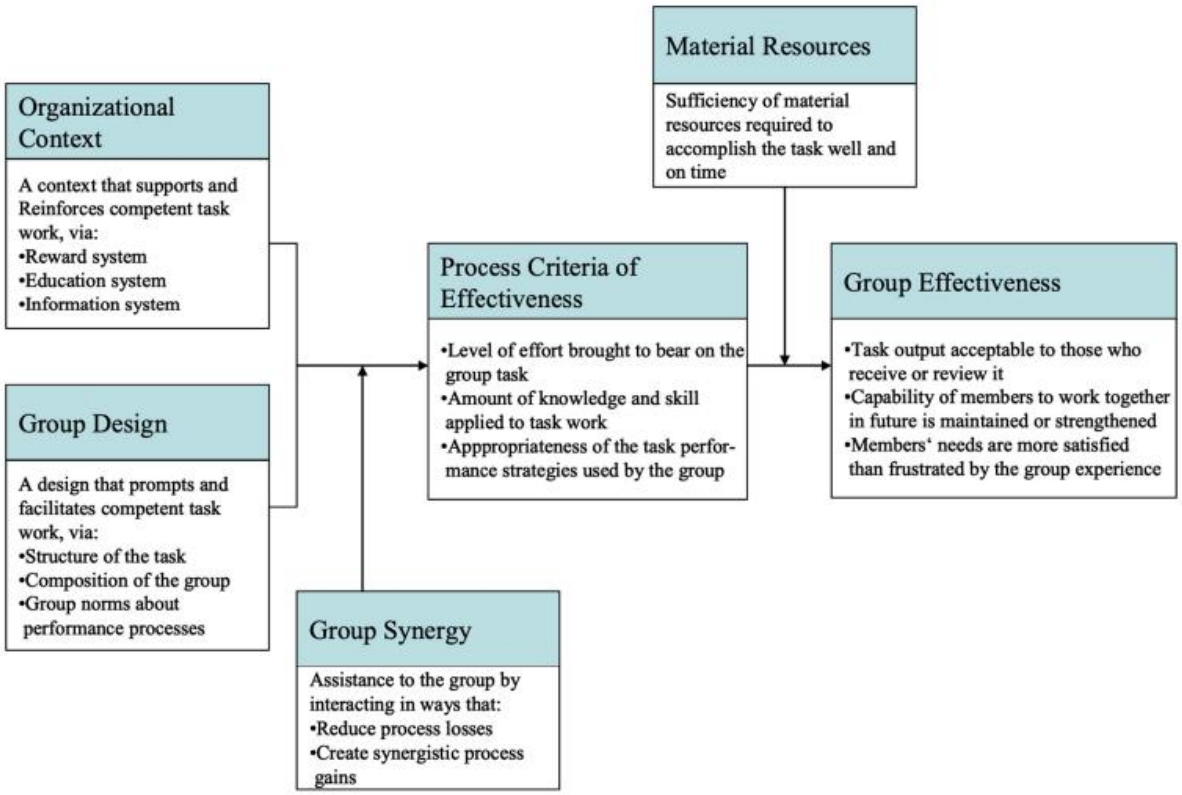
1. "Law and order" not by decree not for idealistic reasons only
2. Incentives "Agree and be silent, so you get something out of it for yourself"

3. Involvement on the basis of individual needs autonomy (control and self-direct-edness, also financial) competence (development of skills, jobs, innovations, …) affiliation (part of the community, of the innovators/"super(wo)men") → shared interest in (financial) success and reputation

Team Process Criteria

Normative Model of Team Effectiveness (Hackman,1983):

- Level of effort
- Amount of knowledge and skills applied
- Appropriateness of strategy



Summary

Topic	Standard / Focus	Purpose
Safety-Critical Systems & General Concepts	Safety-critical systems, hazard concepts	Introduce safety-critical systems, typical hazards, catastrophic failures, and complexity in aviation systems
Systems Engineering Fundamentals	INCOSE, Systems Engineering principles	Define systems, system context, lifecycle, stakeholders, and core systems engineering concepts
Requirements Engineering	DO-178C, INCOSE SE Handbook	Define, document, verify, validate, and manage system and software requirements with traceability
Safety Process	SAE ARP-4761, FAR/CS-1309	Identify, assess, and mitigate functional hazards and ensure acceptable risk levels
Development Assurance	SAE ARP-4754A, DO-254, DO-178C	Ensure appropriate design rigor and independence according to failure severity (DAL concept)
Human in the System	Human Factors, Safety-Critical Systems	Understand human performance limitations, behaviour, cognition, and their impact on system safety
Personality & Interpersonal Skills	Psychology, Human Factors	Improve interaction, communication, motivation, and social behaviour in safety-critical environments
Stress & Resilience	Human Performance, Workload Models	Analyse stress, workload, coping strategies, and resilience to maintain safe performance
Team & Organizational Factors	High Reliability Organizations (HRO)	Build trust, psychological safety, conflict management, accountability, and effective teamwork
Safety Assessment Methods	FHA, FMEA, FTA	Apply qualitative and quantitative safety analysis methods to identify and mitigate failures

Topic	Standard / Focus	Purpose
Common Cause & Independence Analysis	CCA, CMA, PRA, ZSA	Ensure independence of systems and protection against common-cause and external hazards
Complexity & Robustness	ARP-4754A, ARP-4761	Address system complexity, Byzantine failures, robustness, redundancy, and failure tolerance
Modelling, Simulation & Testing	Model-based design, HIL/PIL	Support design, verification, and validation using appropriate abstraction, simulation, and testing
Manned vs. Unmanned Systems & SORA	EASA, JARUS, SORA, SAIL	Assess air and ground risk for UAS operations and define acceptable operational safety levels