

Human Dependability

HUDEP

Presented at HUDEP Tutorial Nov. 2017


J.P. Blanquart AIRBUS, Ph. Palanque IRIT, C. Preyssl ESA

Overview

This presentation

- Gives an introduction to **Human Dependability**
- Summarizes the ESA **Human Dependability Initiative**
- Introduces the ECSS **Human Dependability Handbook**



- **Human Dependability** 
- Human Dependability Initiative
- Human Dependability Handbook



Human Dependability

"Errare humanum est: to err is human, ..."* (Cicero, 1 century BC)

But other creatures do mistakes too:



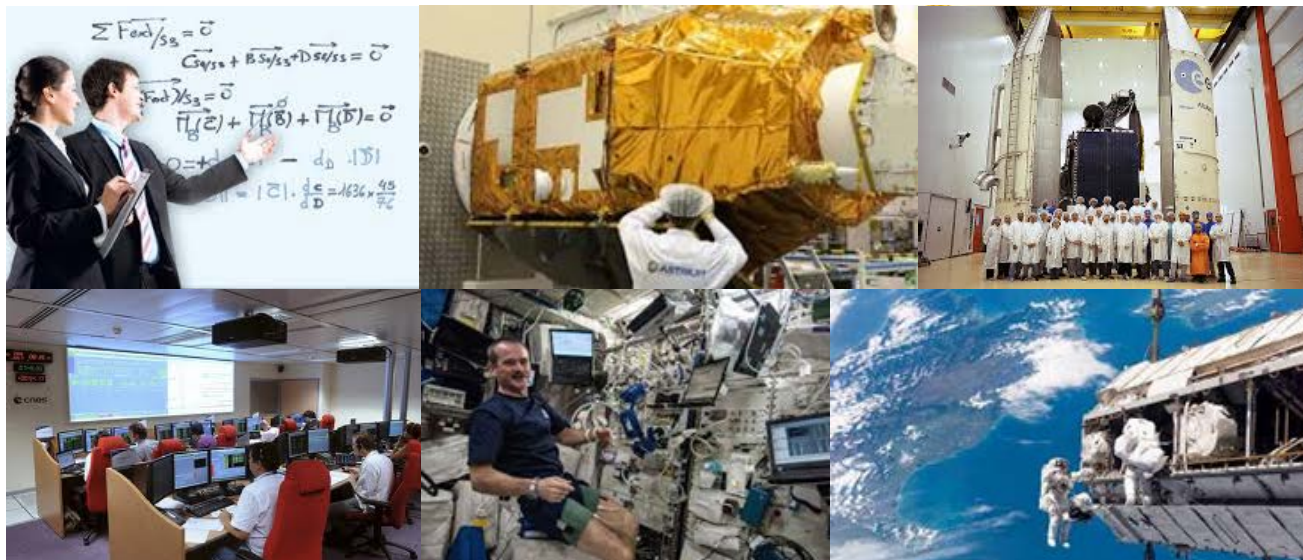
... it looks like there is even an error in this error-statement *

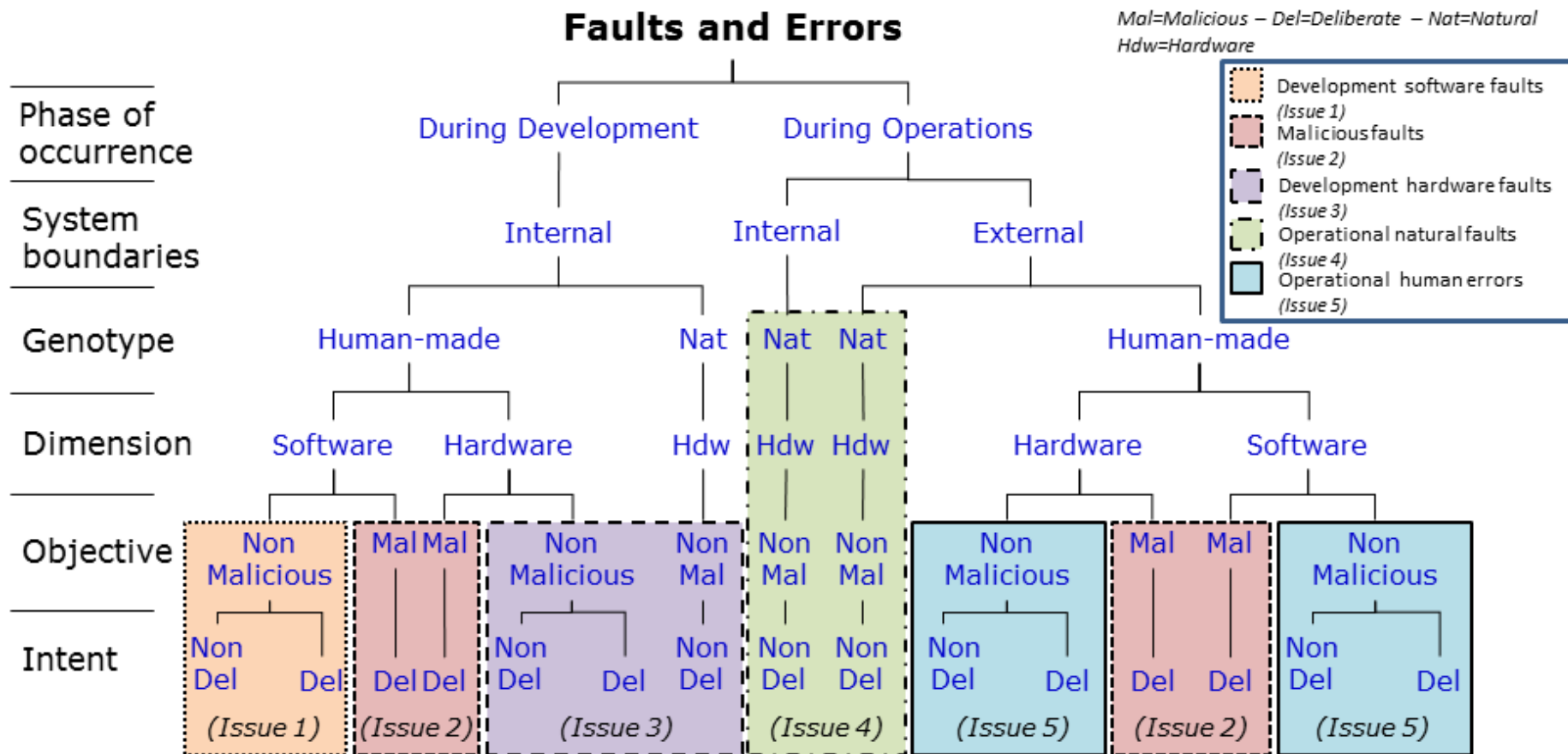
*** "... but to persevere in error is only the act of a fool"**

Human Dependability

All technical systems & projects have human in the loop:

- design engineers, test engineers, production staff, maintenance staff, ...
- operators in a control center, air traffic management, ...
- project team members, project managers, ...
- astronauts, pilots on board, ...





Adapted from: Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. In IEEE Trans. on Dependable and Secure Computing, vol.1, no.1, pp. 11- 33, Jan.-March 2004

Human Dependability

Human Dependability deals with the human in the system & project in a complementary way:

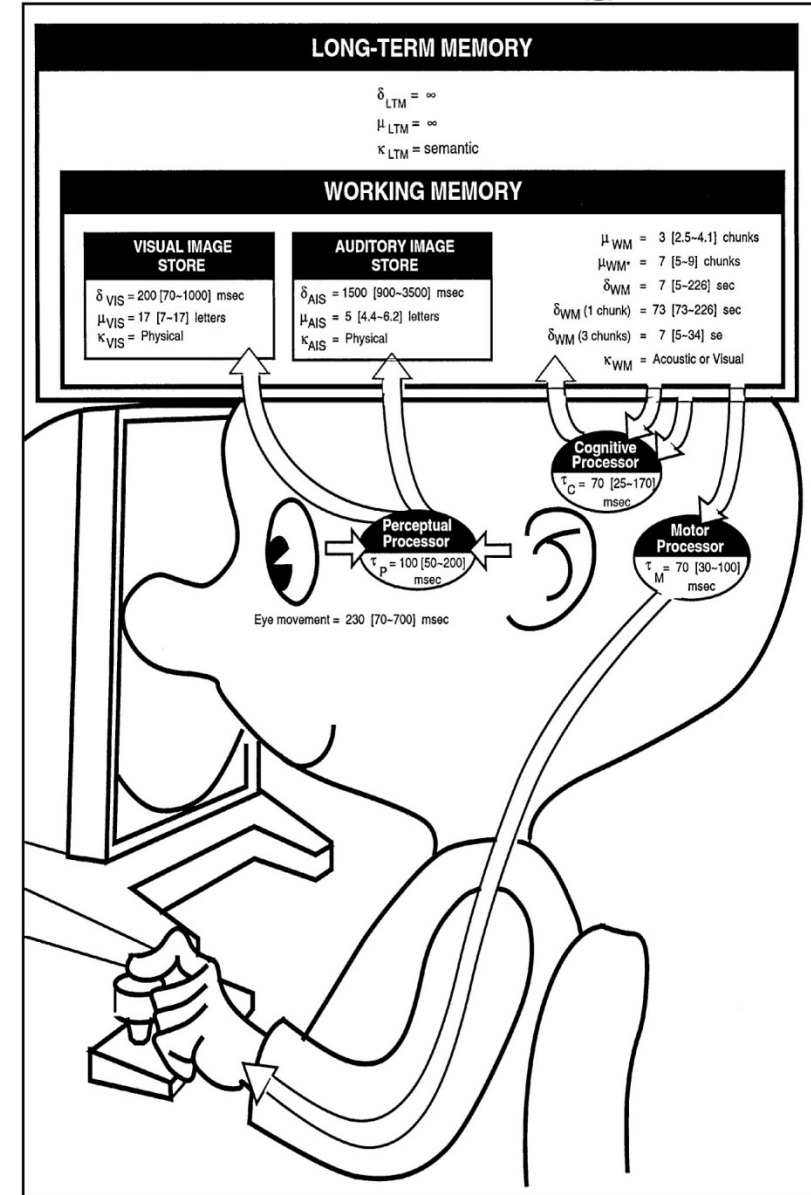
- “Human as Hazard” (human as source of failures), and
- “Human as Hero” (human as source of resilience).

Human performance is the key to safety & mission success !



Human Loop

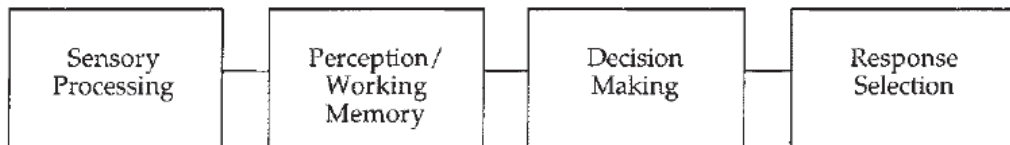
- **Perception** of information from the environment
- **Cognition**: processing (and storing) of information (from memory or from the environment)
 - **Analysis** of information
 - **Decision** how to react
- **Action**: motoric behavior of the human



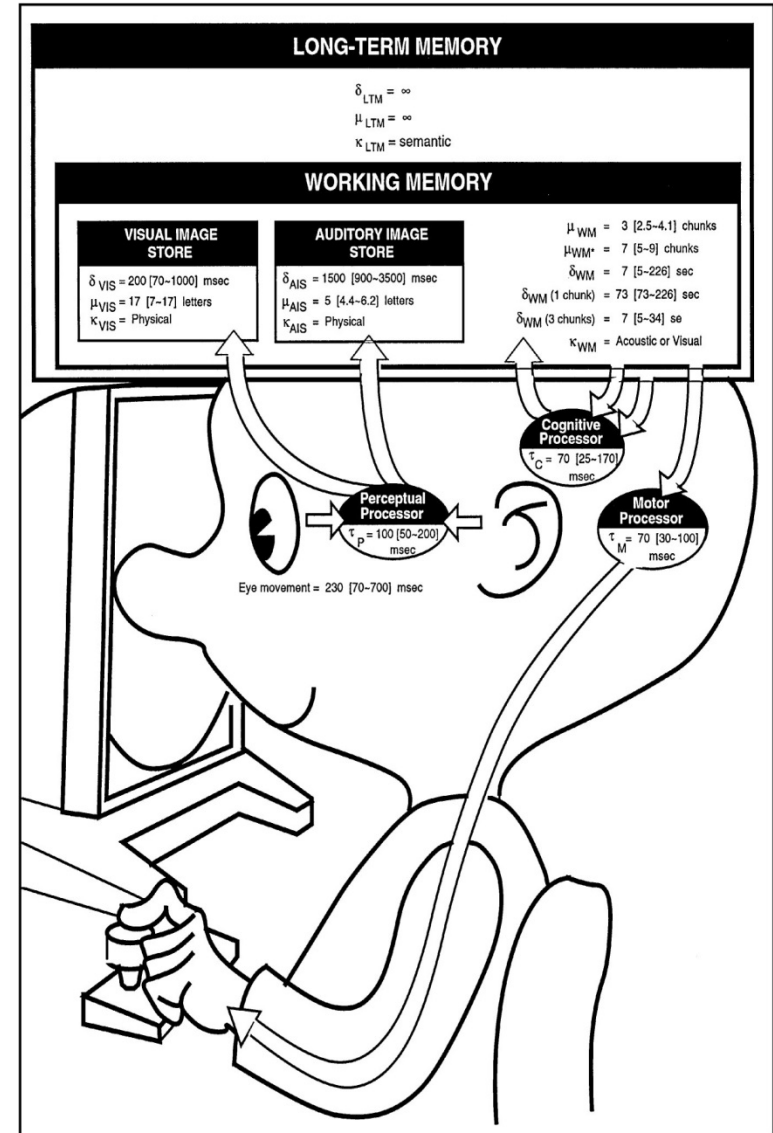
Card, S.K; Moran, T. P; and Newell, A. *The Model Human Processor: An Engineering Model of Human Performance*. In K. R. Boff, L. Kaufman, & J. P. Thomas (Eds.), **Handbook of Perception and Human Performance**. Vol. 2: Cognitive Processes and Performance, 1986, pages 1–35.

Human Loop

- **Perception** of information from the environment
- **Cognition**: processing (and storing) of information (from memory or from the environment)
 - **Analysis** of information
 - **Decision** how to react
- **Action**: motoric behavior of the human



Parasuraman, R.; Sheridan, T.B. & Wickens, C.D. "A model for types and levels of human interaction with automation" Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Trans. on, vol.30, no.3, pp.286-297, May 2000

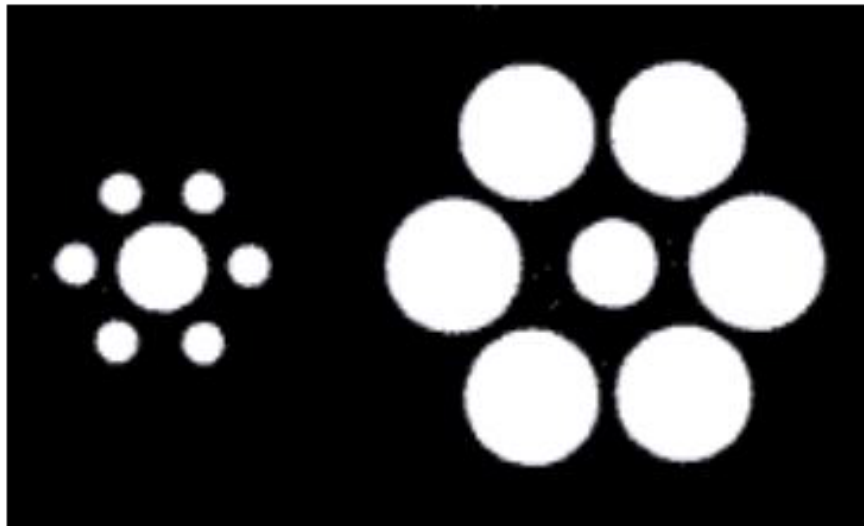


Human Dependability

“Human as Hazard” – Perception only (optical illusion)

Human error ...

... which (center left or center right is the biggest)

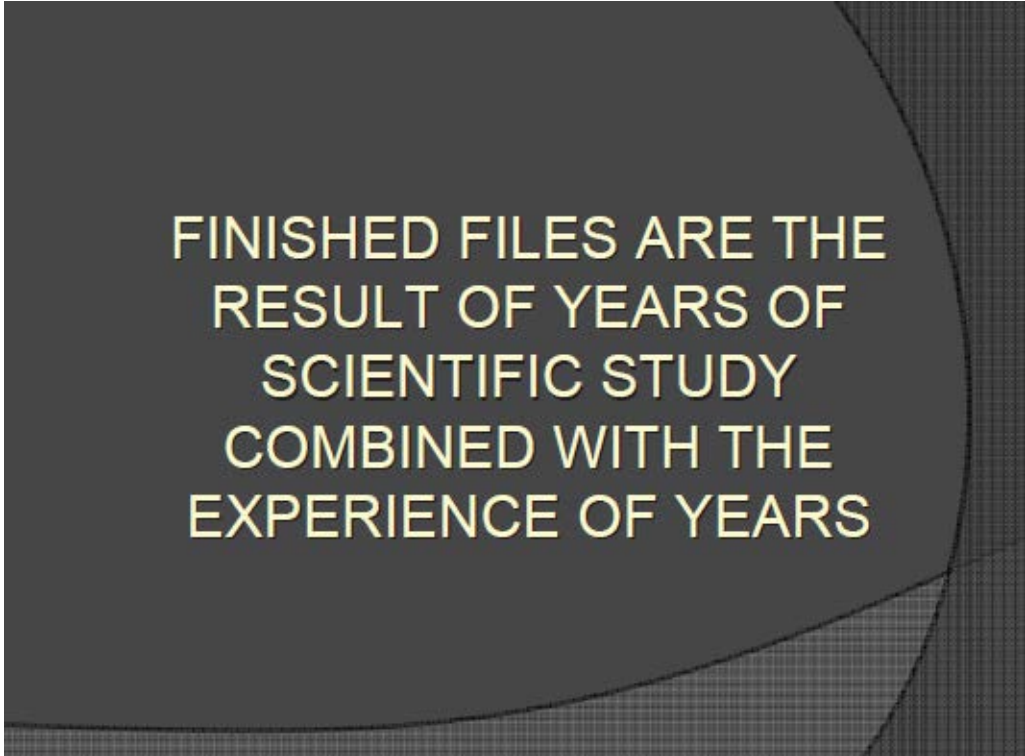


Human Dependability

“Human as Hazard” – Perception/cognition

Human error ...

... count the number of F
in 10 seconds



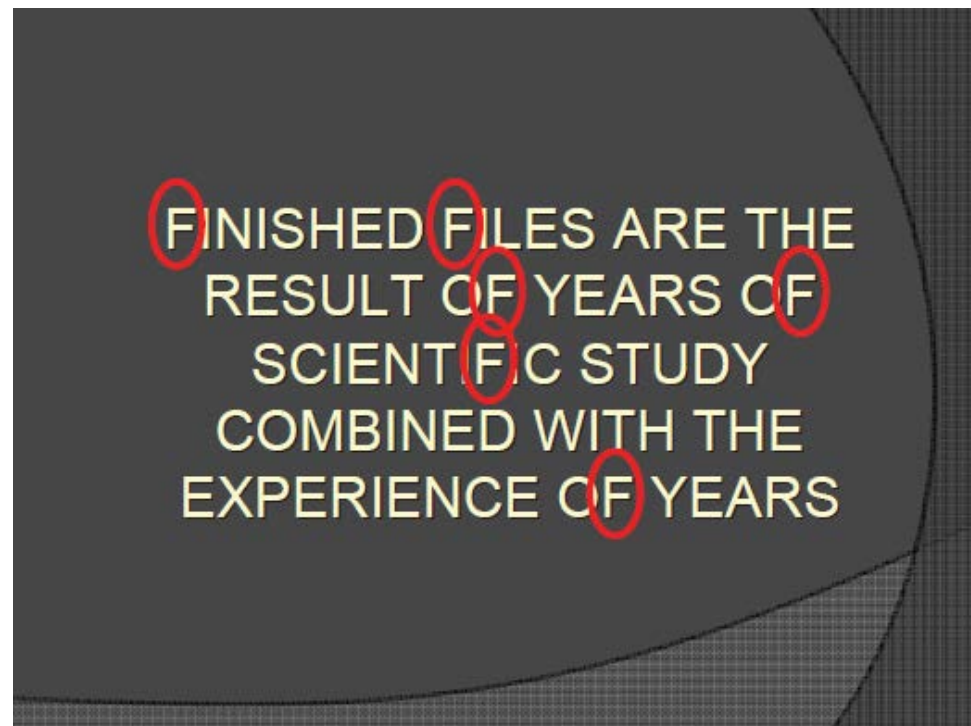
FINISHED FILES ARE THE
RESULT OF YEARS OF
SCIENTIFIC STUDY
COMBINED WITH THE
EXPERIENCE OF YEARS

Slide 11

Human Dependability

“Human as Hazard”

... there are 6 !



→ “Errare humanum est” !

Human Dependability

"Human as Hazard" – Perception/cognition

Human error ...

... Say the words

VIOLET BLUE

BROWN

YELLOW

BLACK

YELLOW PINK

RED BLUE

VIOLET

BLACK

Stroop, John Ridley (1935). "Studies of interference in serial verbal reactions". *Journal of Experimental Psychology*. 18 (6): 643–662

Human Dependability

"Human as Hazard" – Perception/cognition

Human error ...

... Say the colors

PINK RED
 BLUE
 PINK BLACK
 ORANGE RED
 YELLOW GREEN BROWN
 RED

Stroop, John Ridley (1935). "Studies of interference in serial verbal reactions". *Journal of Experimental Psychology*. 18 (6): 643–662

Human Dependability

"Human as Hazard" – Cognition (only) cognitive bias (polarization)

Human error ...

... deduction

Baron, Jonathan
(2000), Thinking and
deciding (3rd ed.),
New York: Cambridge
University Press, ISBN
0-521-65030-5

The effect was demonstrated by an experiment that involved drawing a series of red and black balls from one of two concealed "bingo baskets". Subjects knew that one basket contained 60% black and 40% red balls; the other, 40% black and 60% red. The experimenters looked at what happened when balls of alternating color were drawn in turn, **a sequence that does not favor either basket**. After each ball was drawn, subjects in one group were asked to state out loud their judgments of the probability that the balls were being drawn from one or the other basket. These subjects tended to grow more confident with each successive draw—whether they initially thought the basket with 60% black balls or the one with 60% red balls was the more likely source, their estimate of the probability increased. Another group of subjects were asked to state probability estimates only at the end of a sequence of drawn balls, rather than after each ball. They did not show the polarization effect, suggesting that it does not necessarily occur when people simply hold opposing positions, but rather when they openly commit to them

Slide 15

Human Dependability

“Human as Hazard” – Motor (only)

- Human error ... A movement is not continuous but a series of micro movements (discrete)
- ... selection of target Micro-movement : 70 ms (basic cycle)
- Index of difficulty of selection of a target (Fitts law 54)

Paul M. Fitts (1954). The information capacity of the human motor system in controlling the amplitude of movement. Journal of Experimental Psychology, volume 47, number 6, June 1954, pp. 381-391

$$ID = \log_2 \left(\frac{D}{W} + 1 \right)$$

$$T = a + bID$$

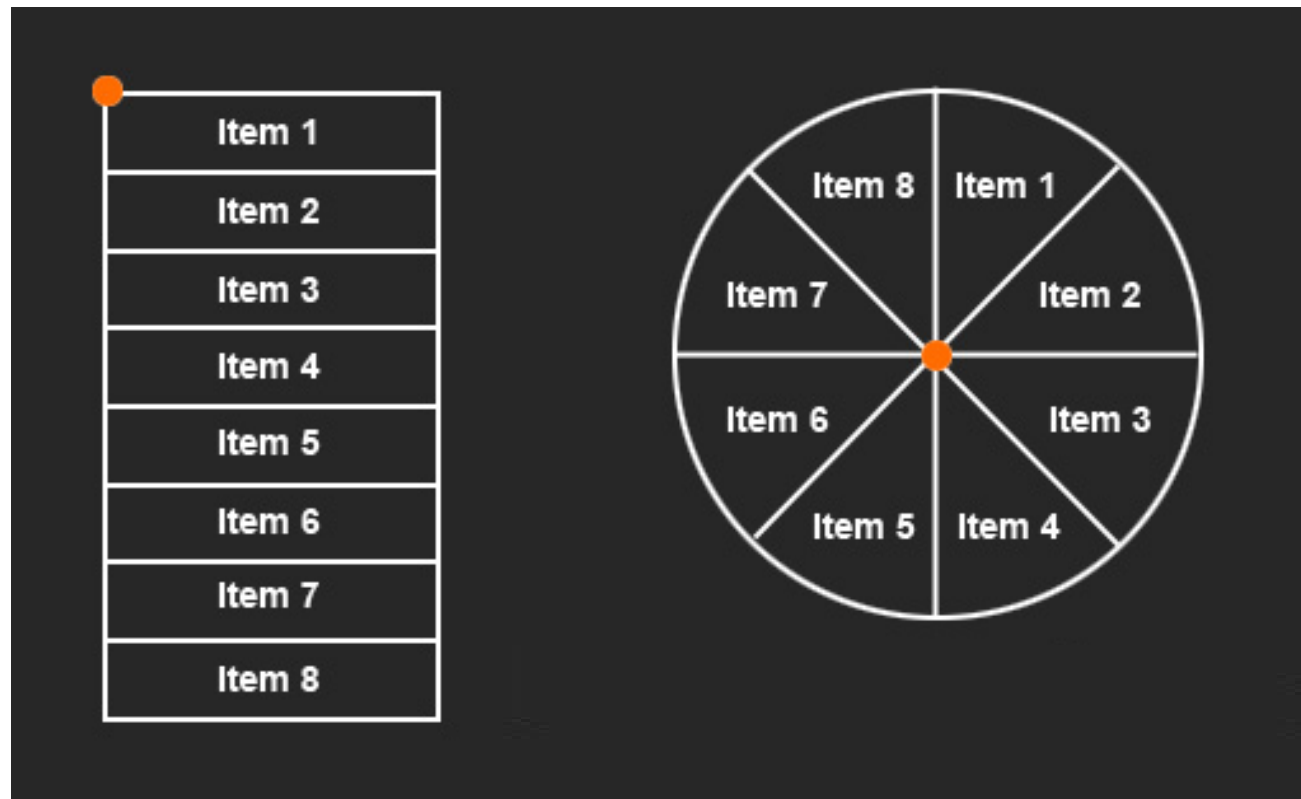
Human Dependability

“Human as Hazard” – Motor (only)

Human error ...

... selection of target

Paul M. Fitts (1954). The information capacity of the human motor system in controlling the amplitude of movement. *Journal of Experimental Psychology*, volume 47, number 6, June 1954, pp. 381-391



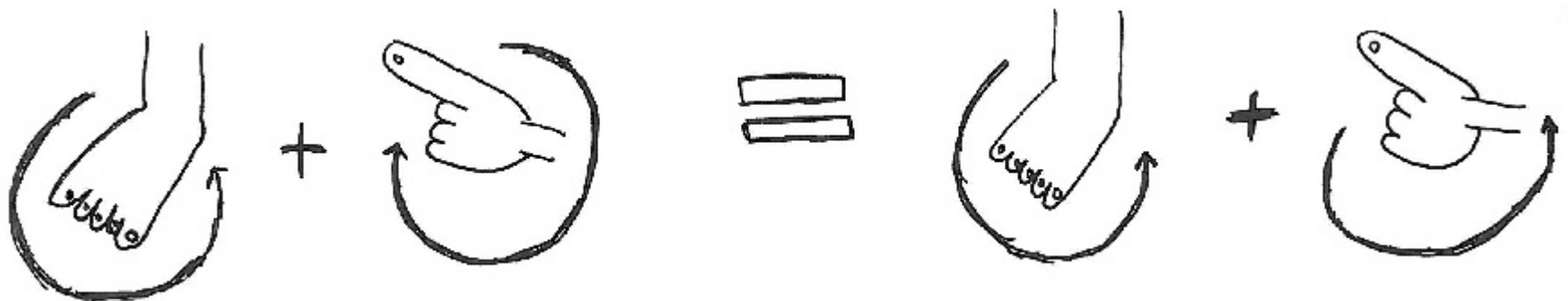
Human Dependability

"Human as Hazard" – Motor / cognition

Human error ...

... impossible movement (r/r)

Lift your right foot a few inches from the floor and then begin to move it in a **clockwise** direction. While you're doing this, use a finger your right index finger to draw a number 6 in the air. Your foot will turn in an **anticlockwise** direction and there's nothing you can do about it!



Human Dependability

"Human as Hazard"

Human error:

- tasks & stress level
- probability

Prof. Bubb TU-München

Kategorie	Probability of failure	MTBF
Easy, simple and often practised tasks with low stress level	$1 \cdot 10^{-3}$	33 min
Complex, difficult not often practised tasks with medium stress level	$1 \cdot 10^{-2}$	5 min
Complex, very difficult seldom practised tasks with high stress level	$1 \cdot 10^{-1}$	<30 sec

Human Dependability

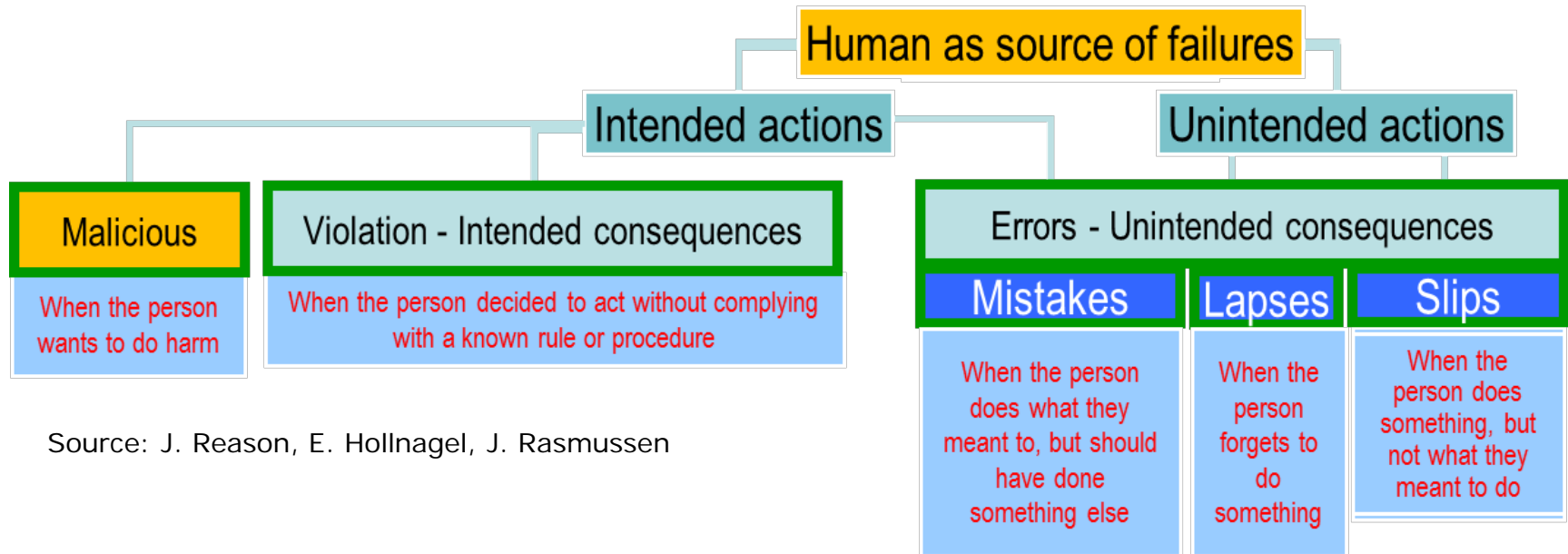
“Human as Hazard”

... when things go wrong



Human Dependability

"Human as Hazard"



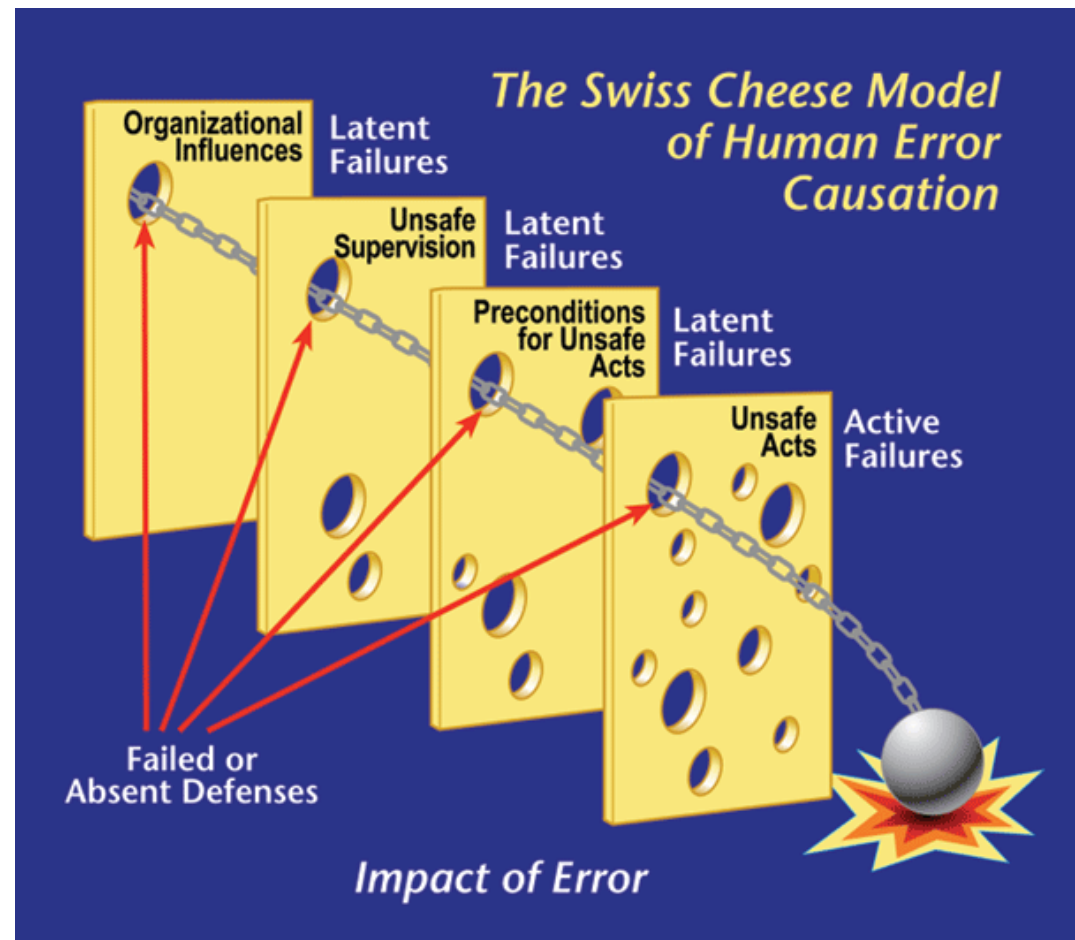
Source: J. Reason, E. Hollnagel, J. Rasmussen

Among the most dangerous human errors:
overconfidence, arrogance, ignorance ...

Human Dependability

"Human as Hazard"

Causes of human error and
barriers to prevent accidents:



Human Dependability

“Human as Hazard”

... when barriers fail ...



Human Dependability

“Human as a Hero”

Humans are a source of resilience !

Resilience is the ability to anticipate and adapt to the potential for “surprise and error” in complex sociotechnical systems, for example:

- resolve conflicts
- anticipate hazards
- accommodate variation and change
- cope with surprise
- close gaps between plans and real situations
- detect and recover from miscommunications and miss-assessment

Human Dependability

“Human as a Hero”

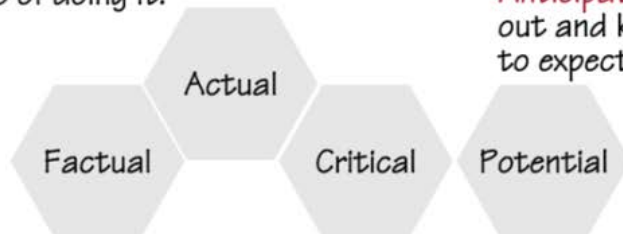


Designing for resilience



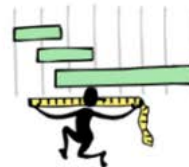
Responding: Knowing what to do, being capable of doing it.

Anticipating: Finding out and knowing what to expect



Learning: Knowing what has happened

Monitoring: Knowing what to look for (attention)



An increased availability and reliability of functioning on all levels will not only improve safety but also enhance **control**, hence the ability to **predict**, **plan**, and **produce**.

© Erik Hollnagel, 2008

Hollnagel E. FRAM: the functional resonance analysis method modelling complex socio-technical systems. Burlington, USA: Ashgate Publishing Company; 2012

Human Dependability

“Human as a Hero”

<https://www.youtube.com/watch?v=mjKEXxO2KNE>



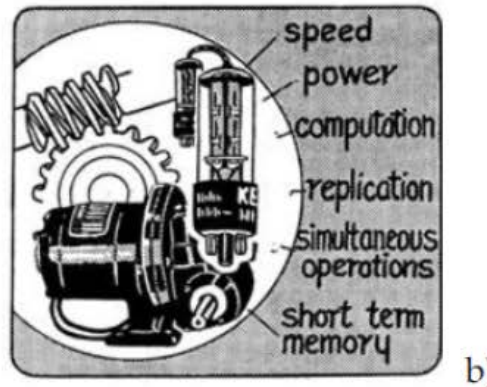
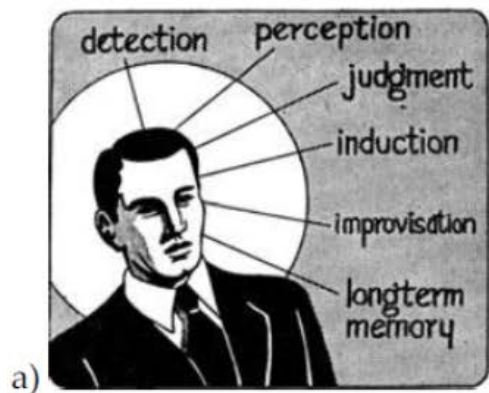
Human Dependability

Human in the System & Project

Systems & projects must be “human centered” to minimize failures due to “Human as Hazard” and recover from failures due to “Human as Hero”.

For example “Human Centered Design” means:

- Design according to goals
- Design taking into account user point of view
- Design for errors

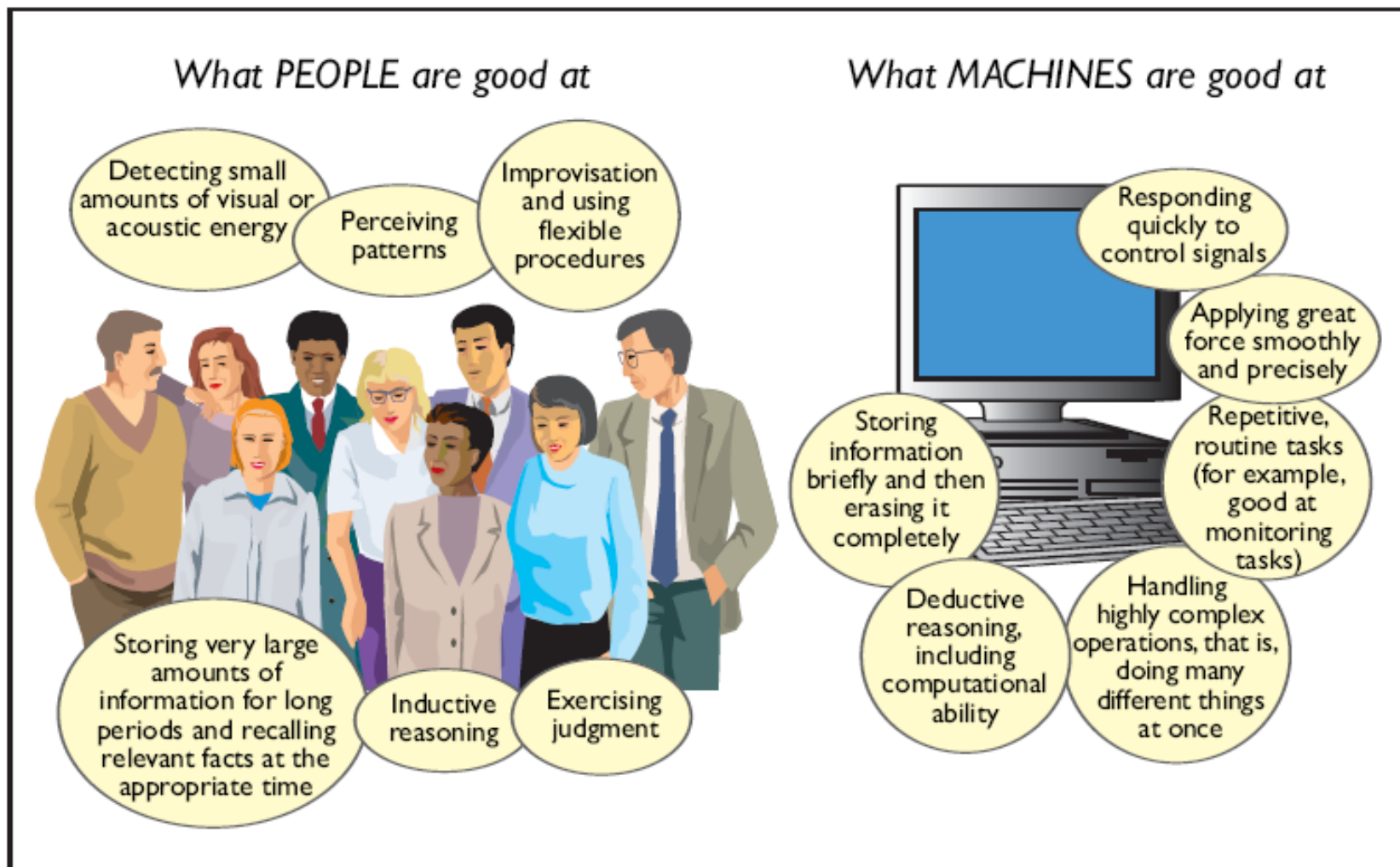


MABA – MABA
Men Are Better At – Machines Are Better At

●	Speed	●
●	Memory	●
●	Sensing	●
●	Perceiving	●
●	Reasoning	●
●	Consistency	●
●	Computation	●
●	Power Output	●
●	Information Capacity	●

MABA-MABA for computers

*Carver & Turoff March 2007/Vol. 50,
No. 3 comm. of the acm (from Fitts 51)*

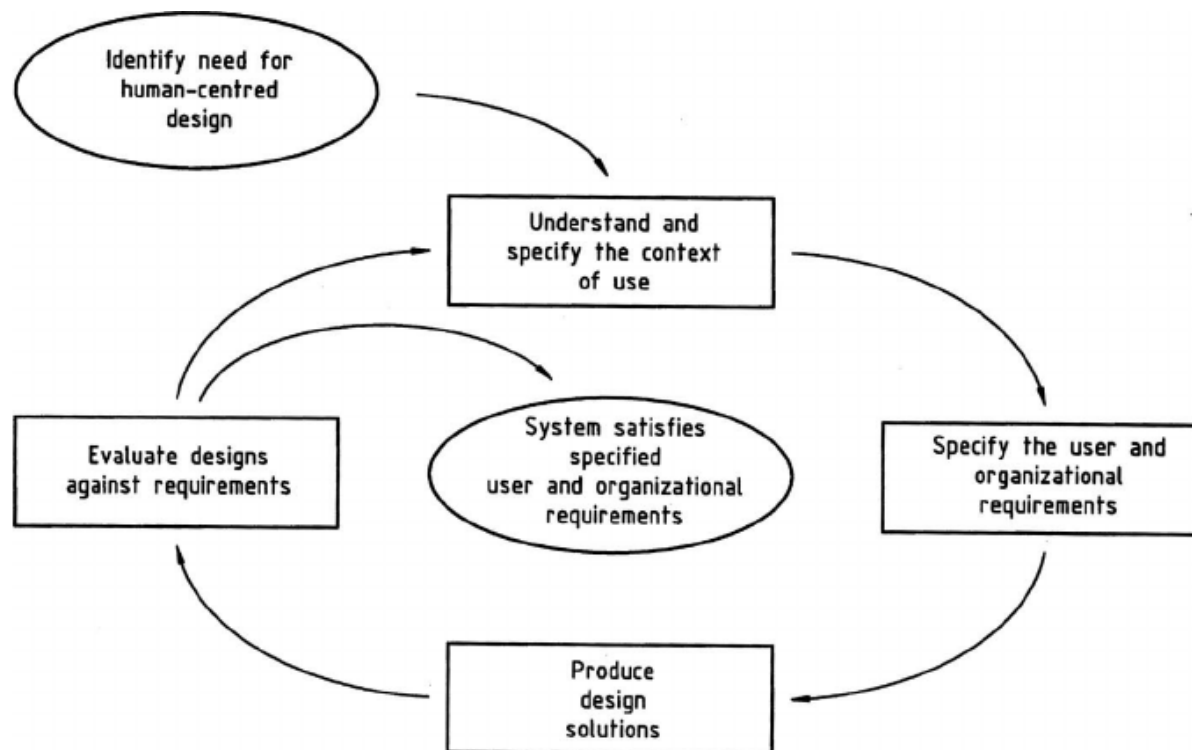


Human Dependability

Human in the System & Project

User Centered Design is an ISO standard

ISO 13407 now integrated in ISO 9241 (on Usability) – part 11

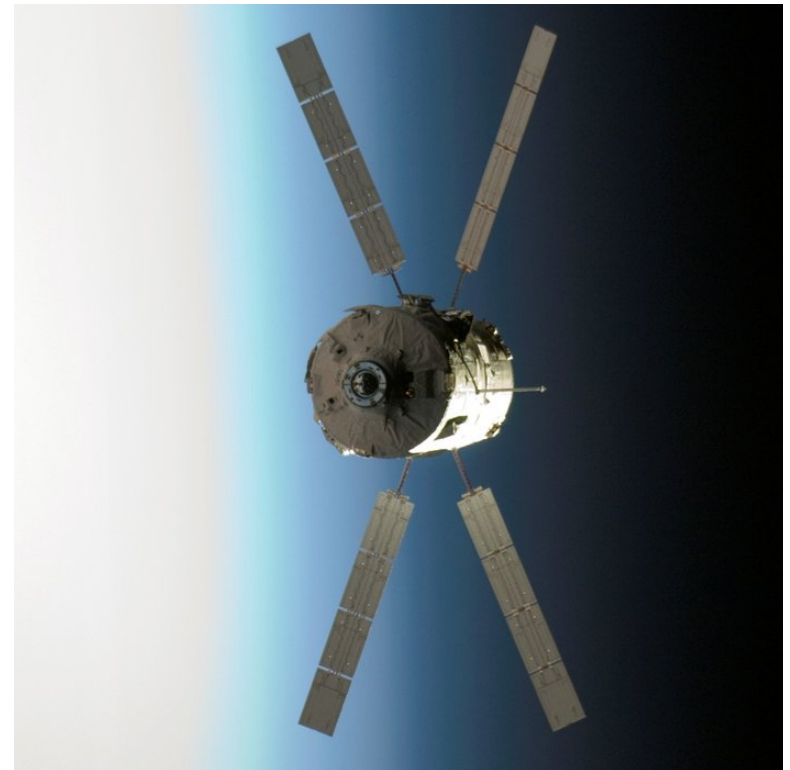


Human Dependability

“Human Centered Design”

Example from the past for the need of “Human Centered Design”:

Since its first voyage in April 2008 until its last in 2015, the ESA Automated Transfer Vehicles (ATV) were very successful supply ships to the Space Station.



Human Dependability

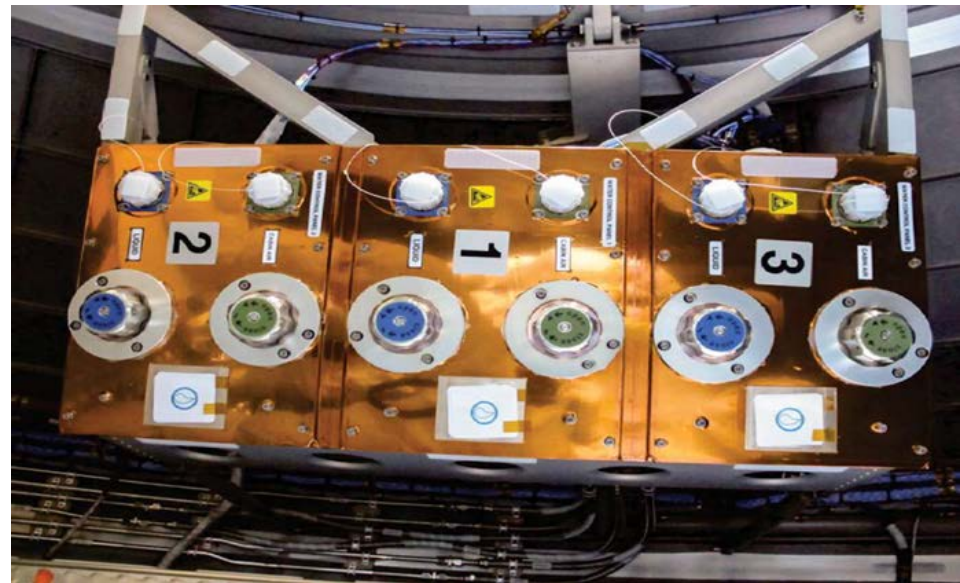
“Human Centered Design”

ATV Water Control Panels:

Astronauts are supposed to open/close valves to transfer water, fuel, etc.

- much more robust design than automatic valves
- crews have no problem doing it, but...

the three valves were in the wrong order causing incidents moving the wrong valve.



Source: Essential Elements to Ensure Human Dependability Onboard Spacecraft - P. Duque ESA / HUDEP 2015.

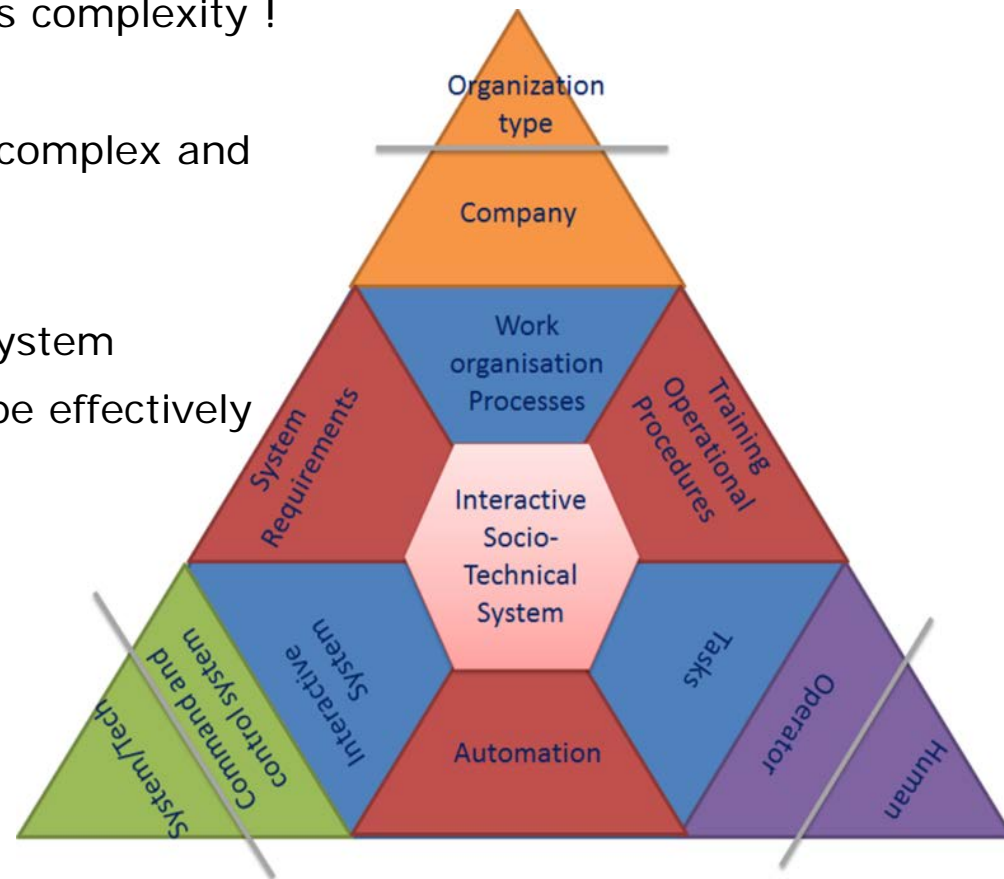
Human Dependability

“Technology-Centered Design”

“Technology-Centered Design” increases complexity !

Today’s systems become more & more complex and unpredictable in their behavior:

“Interactive-Complexity Failures” in a system represent the “temporal inability to cope effectively with complexity”.



Exercise : Analysis of Kegworth Aircraft Accident

An industrial example of all this happened in the cockpit of the B737 that crashed at Kegworth in 1989.

http://en.wikipedia.org/wiki/Kegworth_air_disaster

The crew throttled back one engine that was suspected to vibrate. Very shortly after that, the vibration level decreased on that engine, leading the crew to believe that they had diagnosed the problem right.



Exercise : Analysis of Kegworth Aircraft Accident

An industrial ex
B737 that cra

<http://en.wikipedia>

The crew thrott
Very shortly
engine, leadi
problem righ



cockpit of the

er

ected to vibrate.
eased on that
ad diagnosed the

Human Dependability

“Technology-Centered Design”

It is common to hear that “Automation” will:

- reduce human workload
- simplify tasks performed by humans
- reduce training requirements
- reduce human error

But insight from e.g. aviation shows that “Automation” often:

- changes human tasks to increased complexity (from action to supervision)
- moves tasks from control to monitoring without being simpler
- increases training needs due to more complicated systems
- decreases the operator/controller system state awareness



Source: Designing for
Human Reliability:

Human Factors at NASA

Dr. C.H. Null NASA / HUDEP 2015

Slide 35

Human Dependability

Models & Simulation

Be aware that models, simulation, “models of models of models ...” used to predict system behavior and system automation up to the use of artificial intelligence (*) even further increase:

- system complexity
- the potential for “Interactive-Complexity Failures”
- uncertainties in safety, security & mission success.



Mikhail Kalashnikov:

“When a young man, I read somewhere the following: God the Almighty said, ‘All that is too complex is unnecessary, and it is simple that is needed’ ... So this has been my lifetime motto – I have been creating weapons to defend the borders of my fatherland, to be simple and reliable.”

* artificial intelligence: “an area of computer science that deals with giving machines the ability to seem like they have human intelligence” / “the power of a machine to copy intelligent human behavior” Source: Merriam-Webster's Learner's Dictionary

- Human Dependability
- **Human Dependability Initiative** ←
- Human Dependability Handbook



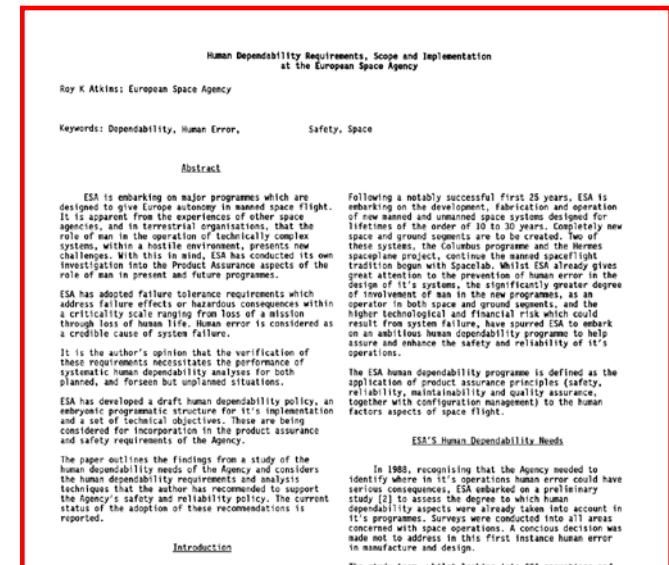
Human Dependability Initiative

At ESA Human Dependability is part of Dependability & Safety.

The discipline of Human Reliability was introduced at ESA more than 20 years ago.

See for example:

- Roy Atkins - Human Dependability Requirements, Scope and Implementation at the European Space Agency - 1990 Proceedings Annual Reliability and Maintainability Symposium
- Alenia Spazio (1994) Human Dependability Tools, Techniques and Guidelines: Human Error Avoidance Design Guidelines and Root Cause Analysis Method (SD-TUN-AI-351, -353, -351). Noordwijk: ESTEC

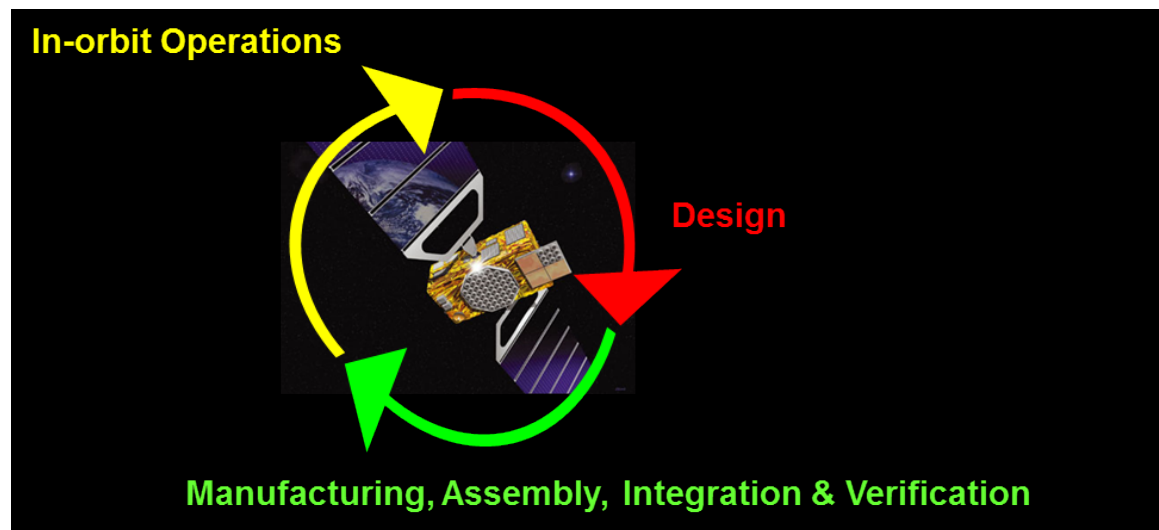


Human Dependability Initiative

ESA created the Human Dependability Initiative as part of an overall ESA initiative to enhance System Dependability & Safety during:

- Design
- Verification
- Operations

in an iterative and integrated way.



Human Dependability Initiative

The ESA Human Dependability Initiative HUDEP includes:

- organization of HUDEP Workshops
- HUDEP Research & Development Studies
- development of a HUDEP Handbook
- HUDEP training

and is supported by a HUDEP steering group comprising ESA, CNES and DLR.



Human Dependability Initiative

HUDEP Workshops

The first HUDEP Workshop in 2009 confirmed the need to re-establish the discipline of Human Dependability at ESA.

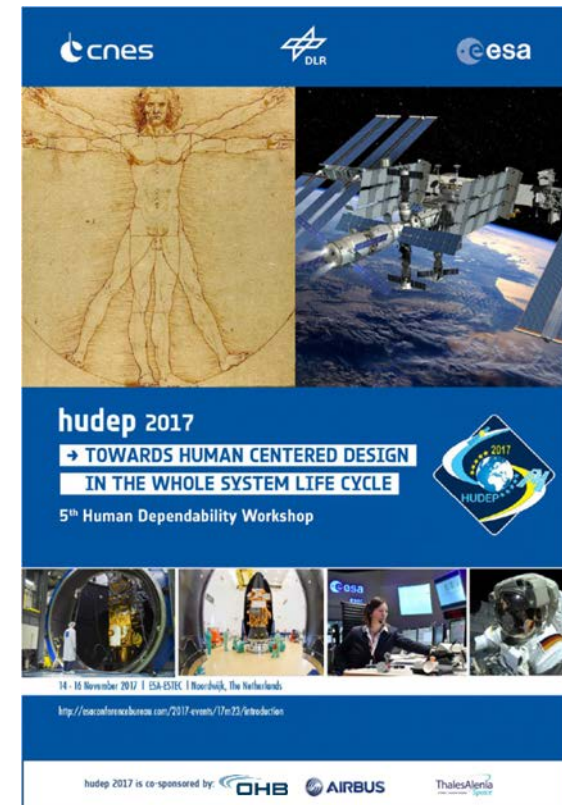
Based on the conclusions of the second HUDEP Workshop in 2011 an ECSS handbook on Human Dependability was developed. Following the third HUDEP Workshop in 2013 the HUDEP Steering Group for coordinated continuation of the HUDEP Initiative was created. The handbook was presented at the fourth HUDEP Workshop in 2015 and the focus was on space operations.



Human Dependability Initiative

The HUDEP Steering Group decided to hold the fifth Human Dependability Workshop HUDEP 2017 at ESTEC and to focus on “Human Centered Design”.

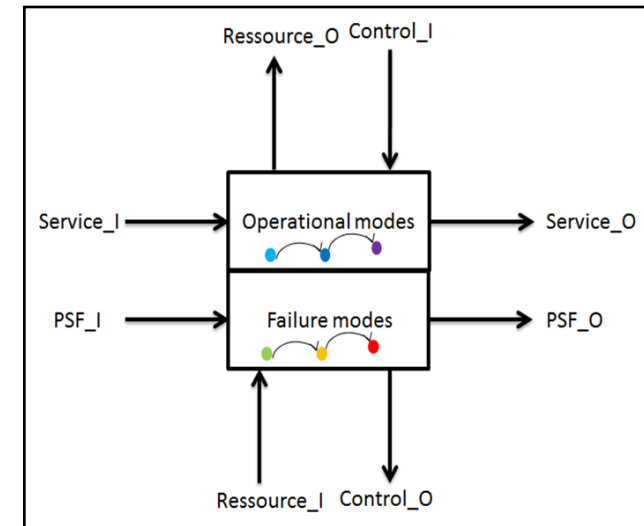
HUDEP 2017 marks 10 years of HUDEP !



Human Dependability Initiative

HUDEP Research & Development Studies include:

- IFA study on Integrated Failure Analysis to deal with “Interactive Complexity Failures”
- CFDA - Catalogue of Failure Data for Safety and Dependability Analysis



- Human Dependability
- Human Dependability Initiative
- **Human Dependability Handbook**



Human Dependability Handbook

The Human Dependability Handbook is the ECSS (*) document ECSS-Q-HB-30-03A published in 2015.

Download your copy of the handbook at:

<http://www.ecss.nl/>

* European Cooperation for Space Standardization



Human Dependability Handbook

The Handbook was written by an ECSS Working Group.

Working Group members:

AGENCIES

ESA:	C. Preyssl (convenor), M. Gabel, S. Buckle
CNES:	A. Sylvestre-Baron, D. Seguela
DLR:	A. Codazzi

INDUSTRIES

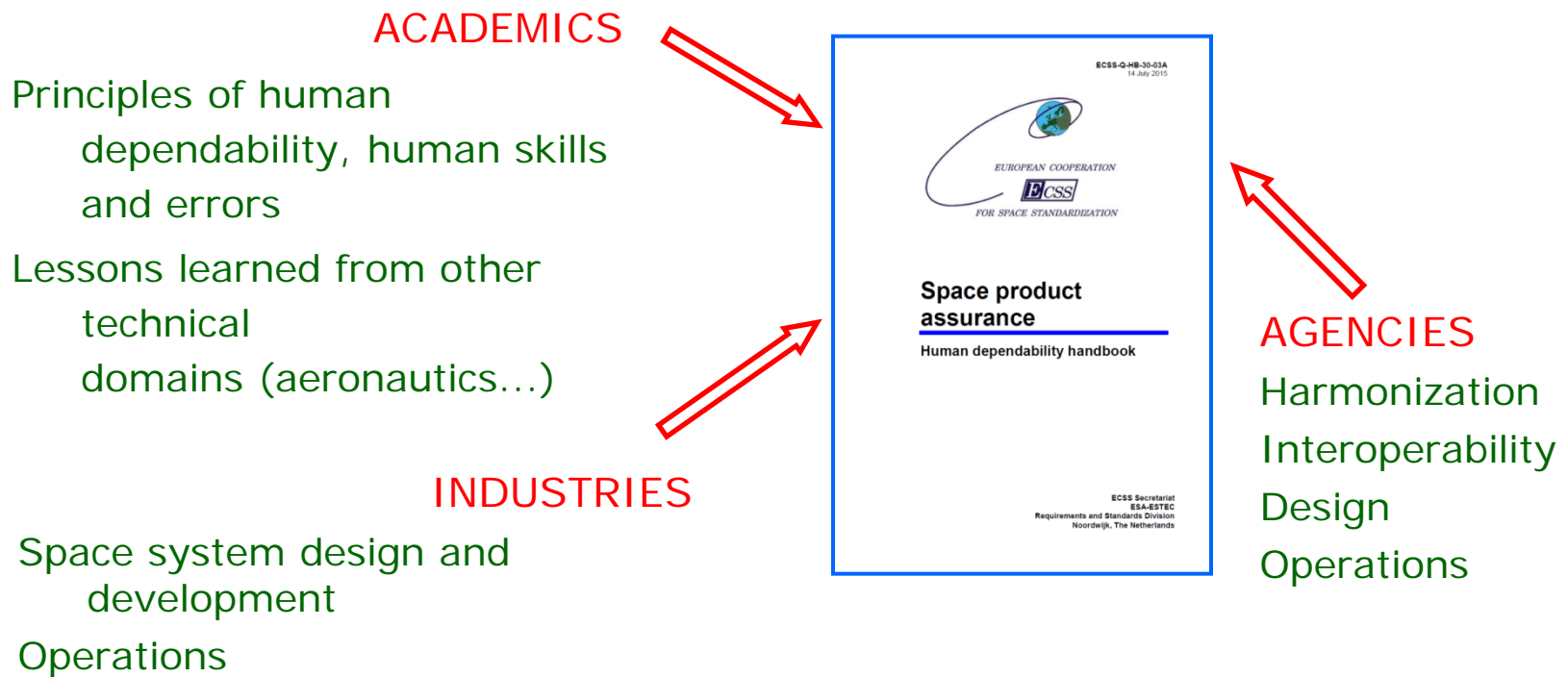
Airbus (AST):	J.-P. Blanquart
Airbus (AST):	P. Scheffers
GMV-Madrid:	A. Atencia
OHB-Bremen:	R.A. Knauer, T. Pohl
TAS-Roma:	M. Sarno, R. Accossato

ACADEMICS

IRIT:	Ph. Palanque
VTT-Espoo:	H. Koskinen

Human Dependability Handbook

The Handbook provides different points of view.



Human Dependability Handbook

The Contents & Structure of ECSS-Q-HB-30-03A:

1. Scope and objectives
2. References
3. Terms, definitions and abbreviated terms
4. Objectives of human dependability
5. Principles of human dependability
 - Human dependability concept
 - Introduction
 - Failure scenario integrating human errors
 - Human error and error type
 - Error precursors and error mitigators
 - Human role in the system
 - Overview
 - Human contribution to safety and mission success
 - Fundamental principles driving function allocation
 - Some principles driving user interfaces design
 - Automated processes and operator tasks in space systems

Human Dependability Handbook

The Contents & Structure of ECSS-Q-HB-30-03A:

6. Human dependability processes

- General
- Human error analysis
 - Objectives of human error analysis
 - Principles of human error analysis
 - Human error analysis process
- Human error reporting and investigation
 - Objectives of human error reporting and investigation
 - Principles of human error reporting and investigation
 - Human error reporting and investigation process

7. Implementation of human dependability in system life cycle

- General
- Human dependability activities in project phases
 - Overview
 - Phase A: Feasibility
 - Phase B: Preliminary Definition
 - Phase C: Detailed Definition
 - Phase D: Qualification and Production
 - Phases: E Operations/Utilization and F Disposal

Human Dependability Handbook

The Contents & Structure of ECSS-Q-HB-30-03A:

- Overview
- Examples of the Evolution of PSFs
- Examples of Human Error Scenario Data

Annex B (informative) Human error analysis documentation

Annex C (informative) Human error analysis example questions

- Examples of questions to support a risk analysis on anomalies and human error during operations

Annex D (informative) Human dependability in various domains

- Human dependability in industrial sectors

Bibliography

Human Dependability Handbook

Scope & Objectives

The handbook:

- provides a familiarization with Human Dependability
- supports the application of Human Dependability such as Human Error Analysis as part of System Safety & Dependability

Human Dependability Handbook

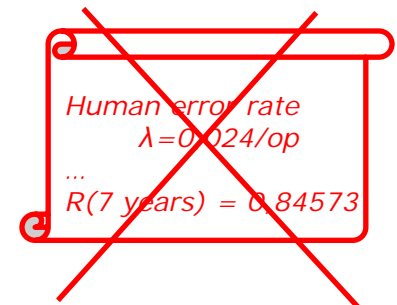
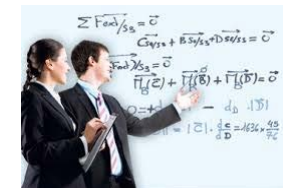
Scope & Objectives

Included:

- Positive (recovery by human) and negative (human error) impact
- Space and ground operations during AIT, launch preparation, space mission
- Qualitative analysis
- Accidental errors

Excluded:

- Design errors
- Quantitative analysis
- Intentional attacks, security



Human Dependability Handbook

Principles of Human Dependability

Human dependability concept:

- The notion of human error, human fault and associated error types
- The commonalities between system, human and organizational faults
- The influencing factors

- Performance Shaping Factors

- Workload (O&M)
- Level of supervision (O&M)
- Work pressure (O&M)
- Training (Job)
- Usability of user interfaces (Job)
- Complexity of the task (Job)
- Fatigue (internal)
- Physical condition (internal)
- Motivation (internal)

Human Dependability Handbook

Principles of Human Dependability

▪ Levels of Human Performance

- Skill
- Rule
- Knowledge

Performance Level		Error Type		
Skill-based level		Slips and lapses		
Rule-base level		Rule based mistakes		
Knowledge-based level		Knowledge-based mistakes		

Control Modes Situations	Control Modes		
	Conscious	Mixed	Automatic
Routine			Skill based
Trained for problems		Rule based	
Novel problems	Knowledge based		

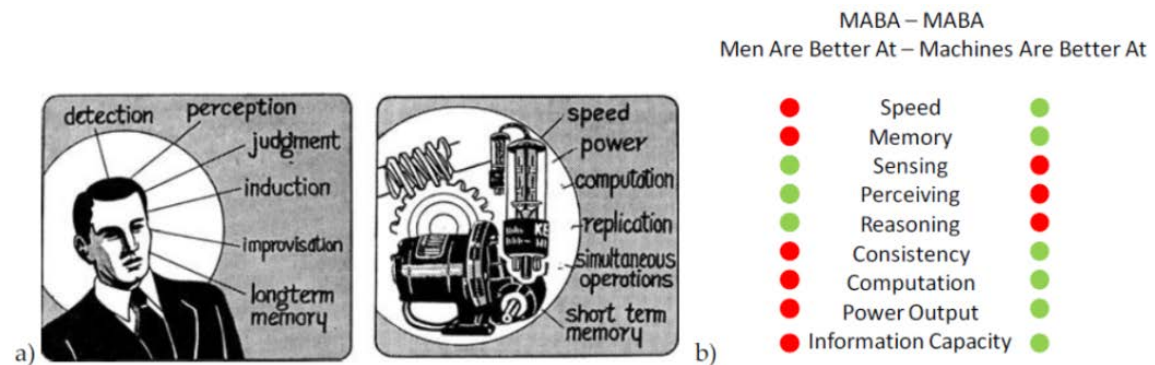
Slide 54

Human Dependability Handbook

Principles of Human Dependability

➤ Human role in the system

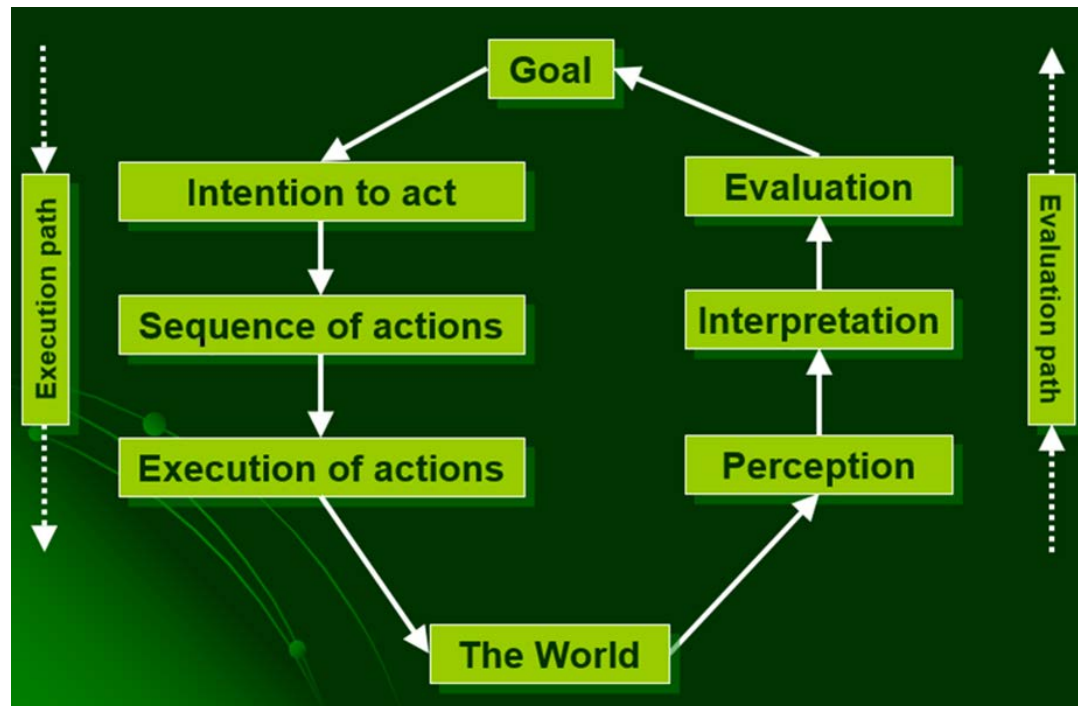
- Human as hazard AND human as hero (work variability)
- Function allocation
 - Temporal allocation (for the same operator)
 - Operator allocation (for a team of operators)
 - Automation (between operators and system)



Human Dependability Handbook

Principles of Human Dependability

➤ User Centered Design



Human Dependability Handbook

Human Error Analysis

Human Error Analysis supports the implementation of Human Dependability in line with the objectives and scope for each specific application:

- Failure Tolerance requirements
- Single point failures
- Investigation of failure scenarios

Applicability:

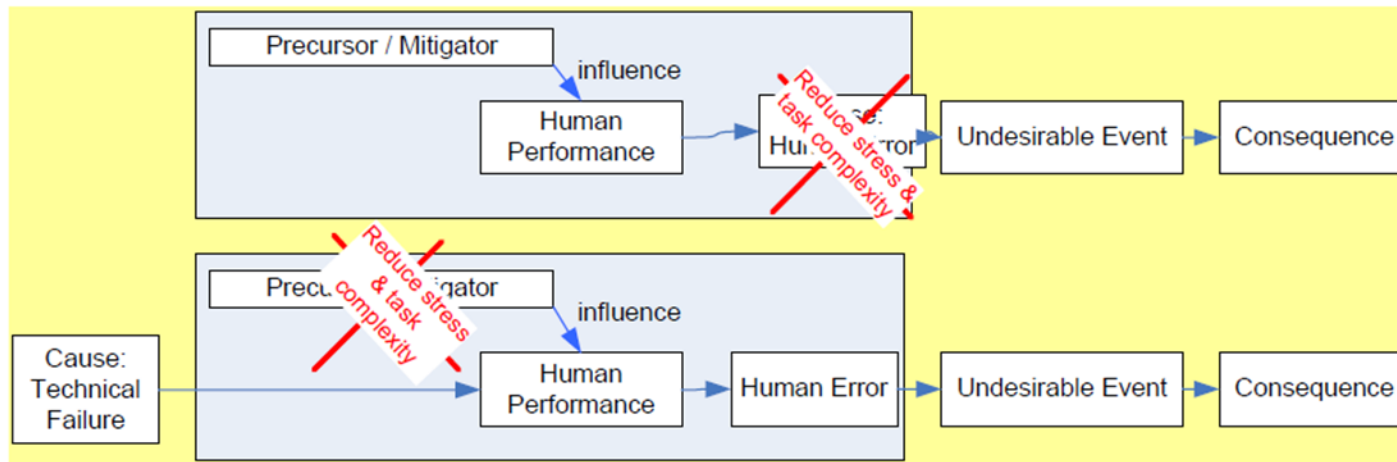
- Functions implemented involving human operators
- Design and operation involving human operators
- Support to the development of operation procedures

Human Dependability Handbook

Human Error Analysis

Human error analysis is the systematic and documented process of identification and assessment of human errors, and analysis activities supporting the reduction of human errors achieved by:

- elimination of existing or potential conditions for human errors
- minimization and control of these conditions
- addressing external and internal Performance Shaping Factors



Human Dependability Handbook

Human Error Analysis

Human error analysis interfaces with:

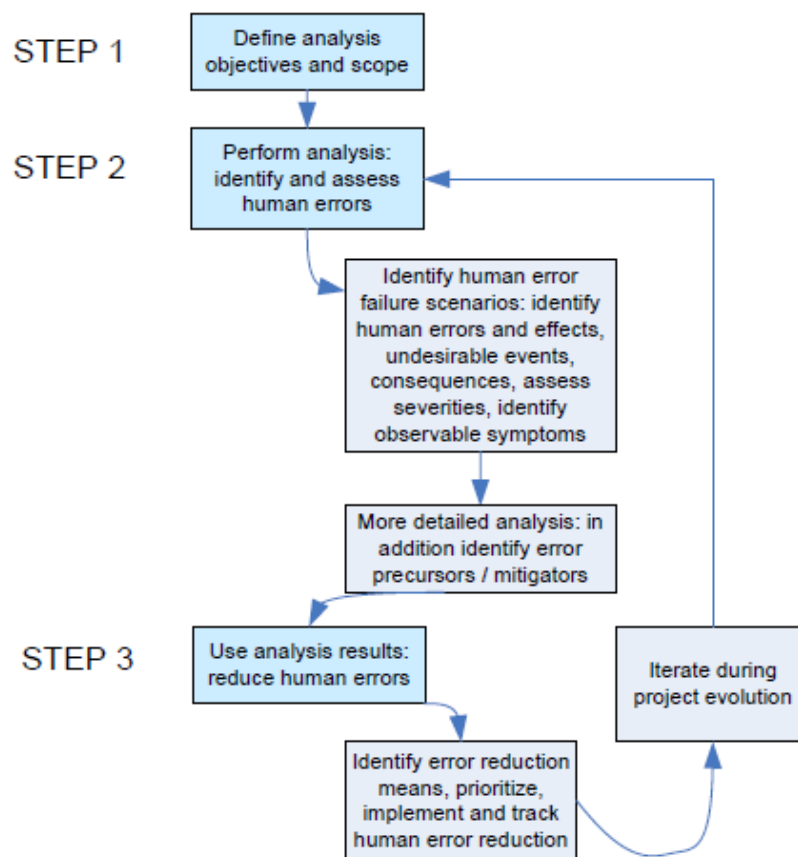
- ECSS Safety & Dependability Standards in Q series
- Hazard analysis, fault tree analysis and FMECA with consideration of human error events
- Common Cause analysis
- Task Analysis
- Staffing and qualification analysis

Human Dependability Handbook

Human Error Analysis

Human error analysis steps:

Iterative process:



Human Dependability Handbook

Human Error Analysis

Table B-1: Example of an “Human Error Analysis Form sheet”

HUMAN ERROR ANALYSIS										Page
Document Reference:					Issue:		Prepared by:			
Project:					Operation:		Ref.:			
Approved by:										
Ref.:	1. Operation Step & Task	2. Failure scenario involving human errors			3. Severity & Requirements	4. Precursor, Mitigator & Reduction measure: PSFs	5. Observable Symptom	6. Links & Interface	7. Error Reduction Recommend ation	8. Implementation, Verification, Status, Remarks
		Cause & Human Error	Effect & Undesirable Event	Consequence						
S1.1	Selection of file	Slip: operator selects wrong file	Wrong file sent to spacecraft leading to safe mode	Service interruption	3	Routine, night shift	Flag	Task analysis	Peer review of files	Now part of normal practice, procedure reviewed, closed

Human Dependability Handbook

Human Error Reporting & Investigation

Operational Phase of Life Cycle

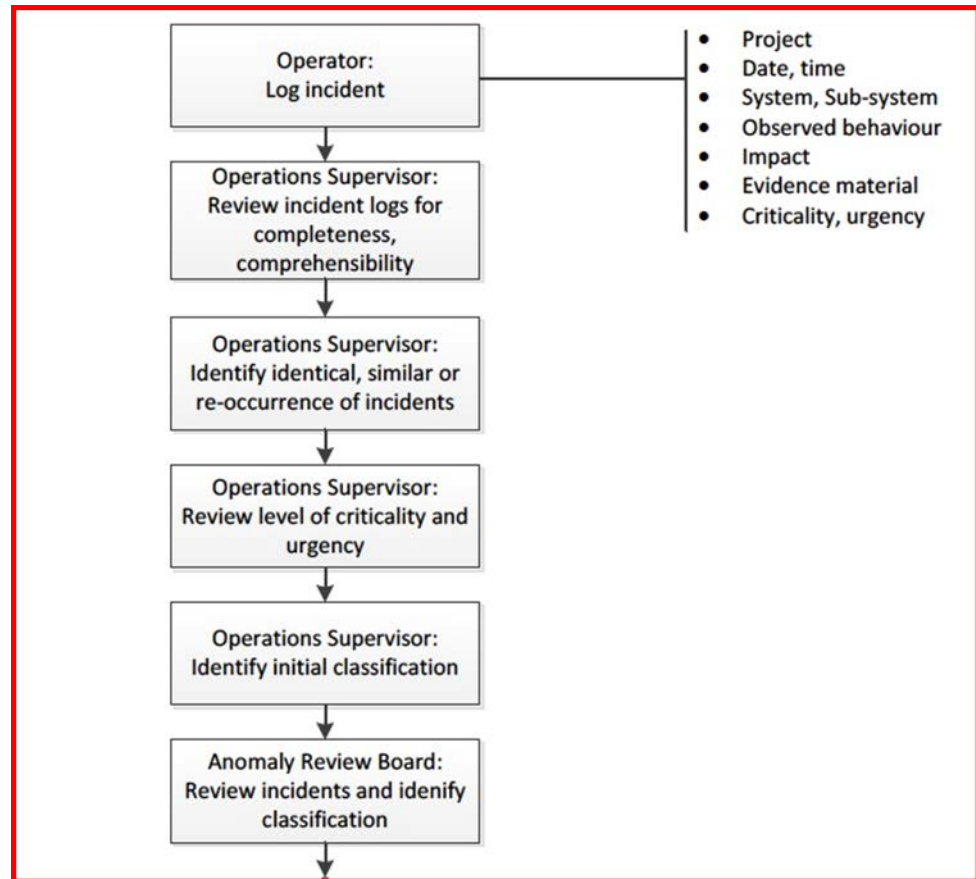
Objectives of Human Error Reporting & Investigation:

- Collect data on human performance
- Identify root causes and contributing factors (e.g. PSFs)
- Feed insights into project life cycle

Human Dependability Handbook

Human Error Reporting & Investigation

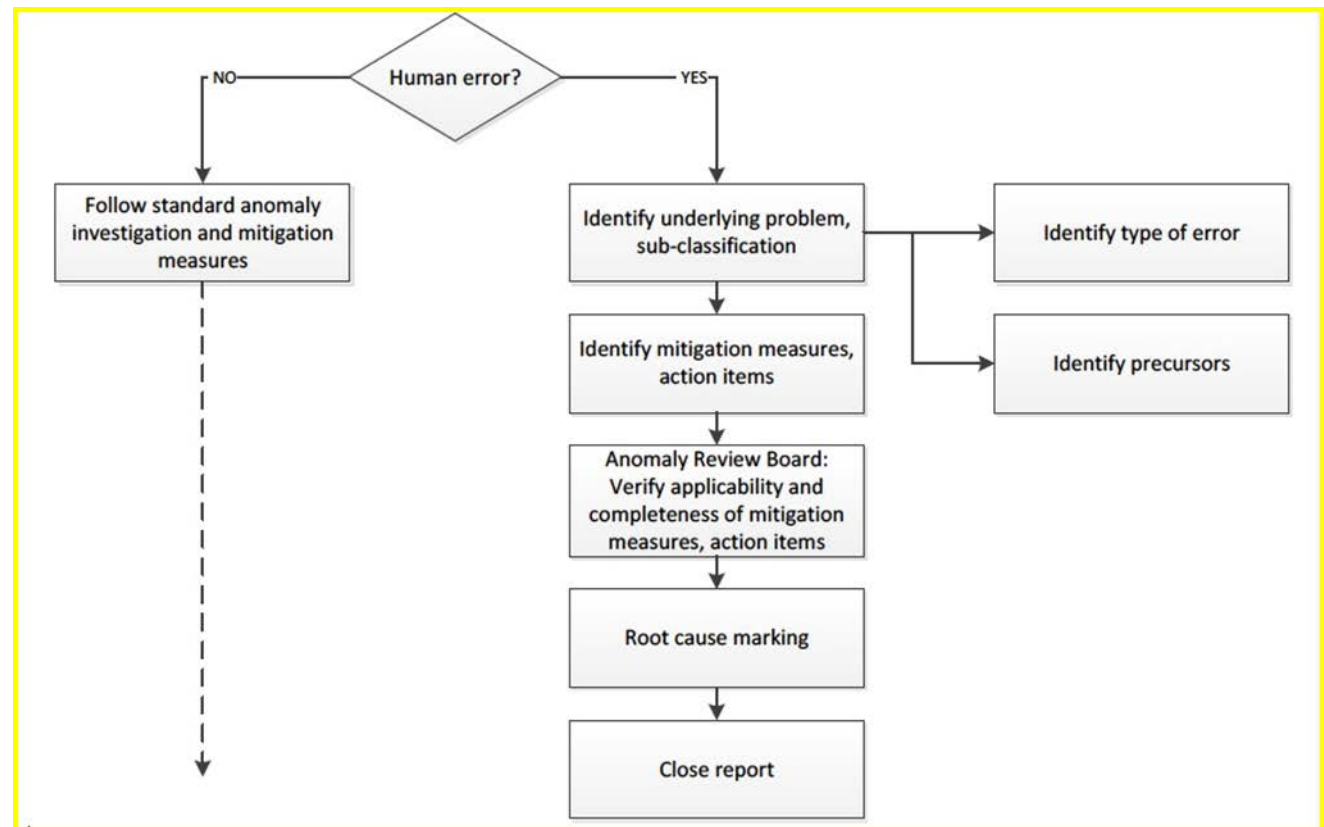
Human Error Reporting:



Human Dependability Handbook

Human Error Reporting & Investigation

Human Error Investigation:



Human Dependability Handbook

Human Dependability in Various Domains

Human dependability is an important discipline for all industrial sectors:

- domains that represent safety critical industrial systems
- infrastructures and “high reliability organizations”
- where a human is situated in the loop of controlling a complex system, network, process or asset
- often also required by the regulatory authorities



Human Dependability Handbook

Human Dependability in Various Domains

DOMAIN	GENERIC ENVIRONMENT	EXAMPLE	DOCUMENT
Space	Ground station network control, Launch sites, Isolation chambers & space simulators etc.	ESTRACK Control Centre	NASA HRA Methods (Chandler et al, 2006)
Defense & security	Nuclear submarines, Flight deck/cockpit, Guided Weapons Systems, High security prisons etc.	HMS Astute	UAV Mishaps HF Analysis (Thompson et al, 2005)
Transport & infrastructure	Air Traffic Management, Flight deck/cockpit, Marine vessel traffic , Railway operation, Tunnels & channels	VTS Houston Texas	Railway Human Factors Guide (RSSB, 2008)
Energy& utilities	Nuclear Power Plants, Chemical Processing Plants & refineries, Grid operation etc.	Tricastin NPP	Safety Culture Assessment (IAEA, 2002)
Science & engineering	Science reactors, Heavy ion particle accelerators, Neutrino observatories, Robotic deep sea exploration etc.	Super-Kamioka Neutrino Detection Experiment	CERN Safety Guide (CERN, 2005)
Life sciences & medical	High security laboratories, Telemedicine, infection control & pandemic response, Surgery, anesthesiology, Intensive care units etc.	Centres for Disease Control and Prevention	Laboratory Biosafety Manual (WHO, 2004)
Other	Emergency response centres, Industrial production and manufacturing facilities etc.	Inmarsat Maritime Rescue CC	Industrial Robotics Safety Guidelines (OSHA, 1987)

Conclusion

Human Dependability is the basis for optimizing the functional role & performance of human in a technical system or project !

Big challenge: Human must keep complex technology under control - not the other way round: complex technology gains control over the human !

The HOPI * Prophecies:

If we dig precious things from the land, we will invite disaster.

Near the day of Purification, there will be cobwebs spun back and forth in the sky.

A container of ashes might one day be thrown from the sky, which could burn the land and boil the oceans.



* native Red-Indian population in North America

**Man was a creature made at the
end of a week's work.... when
God was tired. - Mark Twain**

**We cannot change the human
condition but we can change the
conditions in which humans work.
- James Reason**



Thank you !