

---

# QQD Vision and Industry Spin-In

## Structured Approach for Human Dependability in Space Projects

Fabio Restagno  
ESA TEC-QQD  
fabio.restagno@esa.int

David Avino  
Argotec S.r.l. – Turin, Italy  
david.avino@argotec.it

---

## Outline

 1 *ESA TEC-QQD Vision*

2 *Industry Lessons Learnt (an Example)*

3 *Summary and Conclusions*

- 
- TEC-QQD's support ESA projects in the domains of Safety and Dependability.
  - Space Systems comprise Ground and Space Segments and involve Hardware, Software and Human.
  - The TEC-QQD workshop initiative HUDEP is intended to hold a forum for information exchange on Human Dependability.
  - TEC-QQD is aiming at supporting the development of a Structured Approach for Human Dependability in Space Projects.

- 
- TEC-QQD provided support in the past to Human Space Projects (e.g. with R&D studies and Analyses) in the field of human dependability.
  - The ECSS Standards Q-ST-30 and Q-ST-40 define Dependability and Safety Assurance activities, requirements and analyses and address Human Dependability and Human Errors.

---

## **ECSS-Q-ST-40C and ECSS-Q-ST-40-02C**

### **1. Hazard Analyses for Flight and Ground**

*Are the key tools to identify and eliminate or control all those conditions that could lead to potential human exposure to hazards and hazardous effects, they have also responsibility to identify and analyse human errors and procedural deficiencies that could become causes of potential hazardous consequences.*

### **2. Operating Hazard Analysis**

*Has the purpose to identify hazards and recommend risk reduction alternatives in procedurally controlled activities during all phases of intended system usage. In particular the OHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons and equipment.*

---

## **ECSS-Q-ST-40C and ECSS-Q-ST-40-02C**

Human Error Analysis Q-ST-40C 7.5.4.6:

*Whenever safety analyses identify operator errors as a cause of catastrophic or critical hazards, a dedicated analysis shall be carried out.*

*The human error analysis shall be used to support the safety analysis for the identification of human operator error modes and their effects and for the definition of adequate countermeasures to prevent or control human operator errors.*

*The human error analysis shall be developed from the early phases of the project onwards in order to define recommendations for the hardware and software design, procedure development and training preparation programme.*

---

## **ECSS-Q-ST-30C and ECSS-Q-ST-30-02C**

ECSS-Q-ST-30C, Dependability & Q-ST-30-02C FMEA

activities and analyses specific to Human activities, errors & Operations:

- 1. Identification of human factors in the technical specifications and how they influence dependability.***
- 2. Dependability engineers support to the review of the operations manual and procedures for consistency with dependability analyses.***
- 3. Verification that dispositions to minimize failures due to human errors are included in the procedures.***
- 4. Analysis of Hardware, Software and Human Functions.***
- 5. FMEA to support also the verification of safety analyses, maintainability analysis, tests, maintenance planning and Human Interfaces.***
- 6. During phase CD review of operational procedures to evaluate human reliability problems related to MMI.***
- 7. Human Errors are analysed, as needed, with process FMECA or with a functional FMEA.***

- 
- TEC-QQD recognizes the importance of industry spin-in regarding Human Dependability (space, railway, nuclear, ...).
  - TEC-QQD is committed to ensure that experience and knowledge are not lost and become a consolidated know-how.
  - An example of technical know-how to be retained for future space projects is the experience and lessons learnt from crew and controllers training on Columbus operations.

---

## Outline

1 *ESA TEC-QQD Vision*

 2 *Industry Lessons learnt (an Example)*

3 *Summary and Conclusions*

---

## Operations and Training – *Industry Argotec*

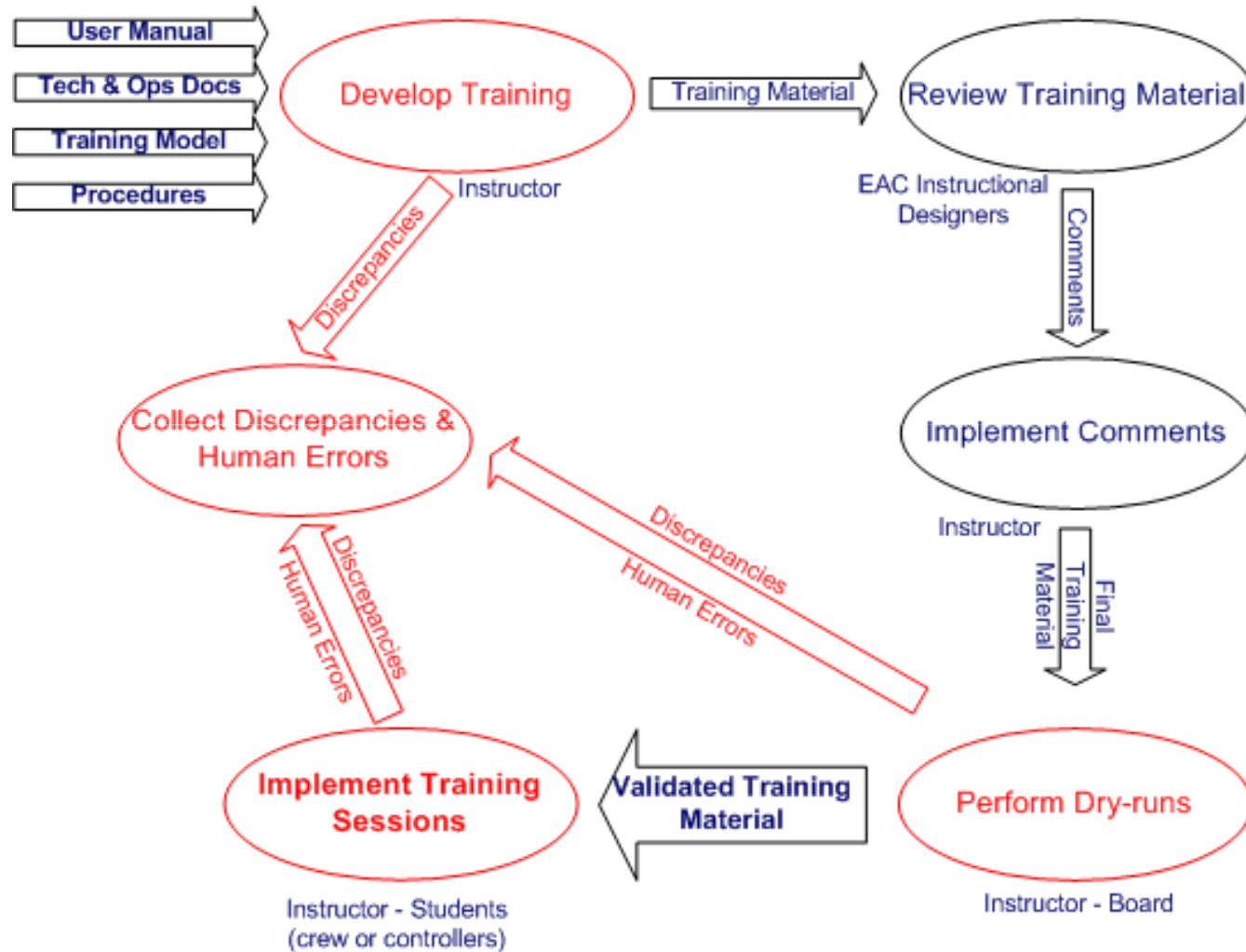
- The following slides are based on the experience gained during several realtime Human Spaceflight operations (e.g. MPLM missions operations, ESA Taxi Flights, ESA “Astrolab” Long Duration Missions, Columbus Simulations and Operations) and as instructor at the European Astronauts Centre (EAC).

---

## Training and its relation with Human Errors

- Training is a key asset to reduce the Human Errors and to accomplish the mission's targets.
- Training has to be considered as an important source of information to identify possible Human Errors and from which analyse the Causes and the Avoidance Criteria.
- Training several final operators (crew & ground) on the same subject (e.g. operational procedures, MMI, displays) is usually a major test-bed to identify the causes of errors before realtime operations.
- The training effectiveness is dependent on the quality of User Manuals, Tech Documentation, Training Models and Procedures.

# Training Development and Implementation Flow



---

## Collecting the Ops Products Discrepancies

- Comments, anomalies and Human repetitive errors identified during the training sessions are usually collected and reported to the defined recipients (e.g. procedures developers, MMI developers, system engineers, etc.).
- Trouble Ticket (TT) and Anomaly Report (AR) database tools are used to submit the discrepancies.
- However, due to the large number of teams involved in the project, it is not always easy to track the discrepancies and their implementation.
- In addition, in case of procedures or operational products change, what to do with the operators already trained?
  - The easiest solution is to implement Notes or Cautions in the procedures or in the operational documentation, just to catch the attention of the operators during the execution.

---

## Operational Procedures

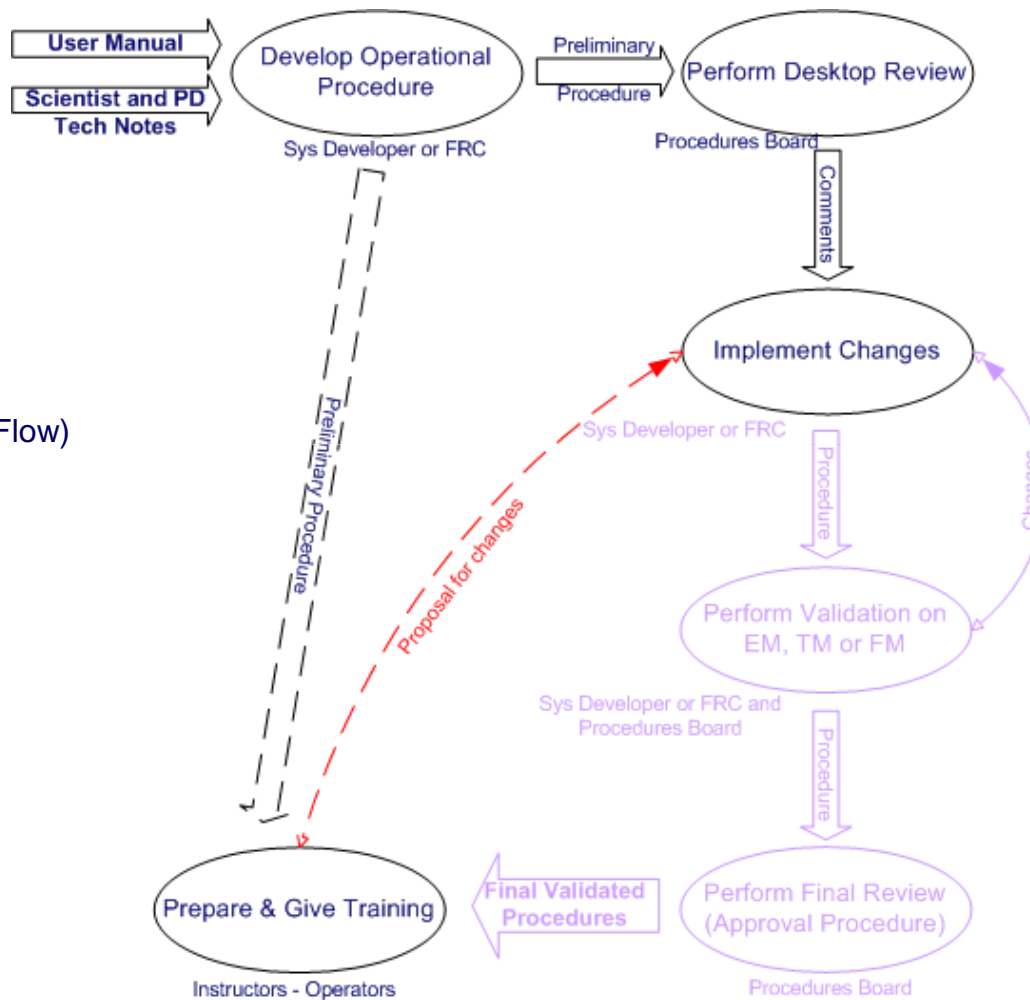
- Procedures are the baseline for the conduct of space operations.
- Training is also based on procedures.
- Finally, the mission success is also dependent on the quality of procedures.

# Operational Procedures Development Flow

(Example of Payload Procedures Dev. Flow)

*Acronyms:*

- PD Payload Developer
- EM Engineering Model
- FM Flight Model
- FRC Facility Responsible Centre
- TM Training Model



---

## Simulations (1/2)

- Most of the time, training and simulations are a good test-bed for the identification of possible inconsistencies and human errors.
- 6-8 months before the mission (or launch campaign) the simulations start.
- Scope of the simulations:
  - Check the environment;
  - Final Operational Procedures Validation (if required);
  - Final interfaces validation (i.e. ground and crew displays);
  - Operators (crew and flight controllers) training and certification.

---

## Simulations (2/2)

- In case common and repetitive human errors have been identified during the simulations, they are induced by wrong boundary conditions.
- At this stage, HW and SW products are hardly changeable. Therefore, this inconvenient is often overcome with changes on the operational products (e.g. procedure's notes, checklists, console handbook, cheat-sheets).
- From the past experience, it is not always easy to track the resolution of Anomalies or discrepancies identified during simulations, due to:
  - Different teams involved in the simulation, but not responsible for the changes (e.g. sim team, ops team, systems developers, etc.);
  - Contractual issues (these discrepancies may lead to an ECR, then to a CCN).

---

## Lessons Learnt on Possible Causes of Human Errors based on Experience (1/2)

- **Time constraints:**
  - Too many activities in the same schedule (packed operations timelines);
  - Time devoted to activities w/o taking into account specific environmental burdens (i.e. µg, activity locations and constraints, etc.);
  - External pressure (e.g. willingness to demonstrate a good and quick performance).
- **Errors due to Self-Confidence** (i.e. procedures run by heart, repetition of similar procedures or similar activities).
- **Procedures Quality** (e.g. training on TM or EM, sometimes not fully compliant with the Flight HW).

---

## Lessons Learnt on Possible Causes of Human Errors based on Experience (2/2)

- **Lack of Training** as impacted by external factors:
  - Late delivery of Procedures, that forces the utilization of preliminary procedures;
  - Pressure from tight schedule (i.e. crew to fly in a short time, controllers following too many lessons in a very short time);
  - Fidelity of Training Models (i.e. different labels, different SW or HW versions);
  - Lessons given months/years before the activity implementation.

# Lesson Learnt for Human Errors avoidance solutions: Example of formats for “How to Increase the Attention”

- To increase the operator’s attention during an activity execution, the following information blocks are used in the Procedures or in the “Notes”:

NOTE

Notes provide additional or amplifying information that is ‘nice to know’ for a step of a procedure.

**CAUTION**

**Cautions provide information necessary to prevent hardware damage or malfunction.**

**WARNING**

**Warnings provide information necessary to ensure crew safety.**

The screenshot shows a web application window titled "Activity details Dialog -- Webpage Dialog". The URL is <https://ops2.jsc.nasa.gov/apps/ostpv/ActDetailMiniMode/FullSizeFrame.aspx?actIDArray={49356D83-A752-47D6-A2B5-2D48022}>. The "General" section contains the following fields:

- Activity Name: SW TR-PWS2&CBL-STOW
- CPS ID: 892
- ORIG DO ID: A0000000229F51ESCP2
- Activity Status: Completed
- Activity Location: COLUMBUS
- Proc Location: BLANK
- Procedure Number: (empty)
- Filter Category 1: CDG
- Filter Category 2: BLANK
- Filter Category 3: BLANK
- Origination: ESA-COL-CC
- Class: System
- Time Critical:

The "Notes" section is highlighted with a red border and contains three entries:

- Execution Note**: Stow PWS-2 and its accessories according to today's stowage locations, refer to message 17-0828
- OpsNote**: Stow PWS-2 and its accessories  
Перезагрузка ПО - укладка кабелей после перезагрузки
- CrewNote**: Laptop Desk and Bogen Arm stowed together in NOD154\_C1 rather than NOD154\_C2 (for convenience of access).

The "Attachments" section shows two attachments: Attach. 1 (Delete) 17-0828 and Attach. 2 (Add).

---

## Lesson Learnt Human Errors avoidance solutions Checklists & Procedures

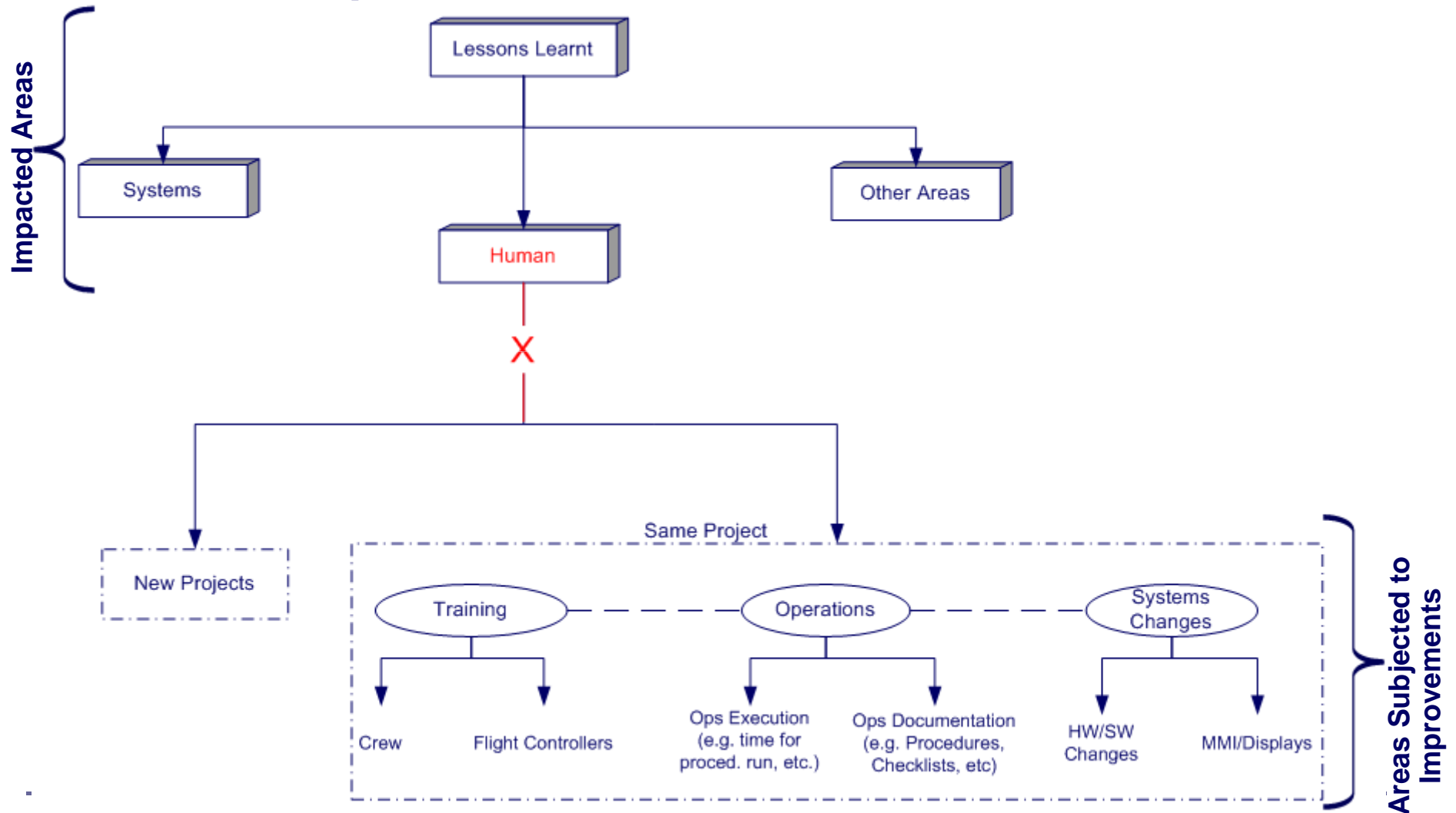
- Checklists with the operator's interaction usually reduce the Human Error, increasing the level of attention required.
- Checklists are used by both, crew and flight control teams.
- Procedures and Checklists are the baseline to reduce the Human errors and to have all the following “actors” *speaking the same language*:
  - Developer;
  - Engineers, Scientists;
  - Procedures Developers;
  - Instructors;
  - Crew/Flight Controllers.
- The correct usage of procedures and checklists is part of the training objectives and is verified during the simulations.

---

## How to Improve Collection of Lessons Learnt

- The lessons learnt from training sessions, simulations and operations are an important source of information from which to identify Human Errors avoidance Criteria.
- A good source for lessons learnt could be the **Anomaly Reports (AR)**. The reports are usually rich of information on SW or HW malfunctions, instead they are not detailed enough in case of Human Errors.
- Good improvements can be achieved in splitting the AR from the Resolution Process (RP). A more detailed RP enhances the capability to identify the real cause of the anomaly (when the source is an operator error, the resolution may point to MMI or to a request for procedure changes).

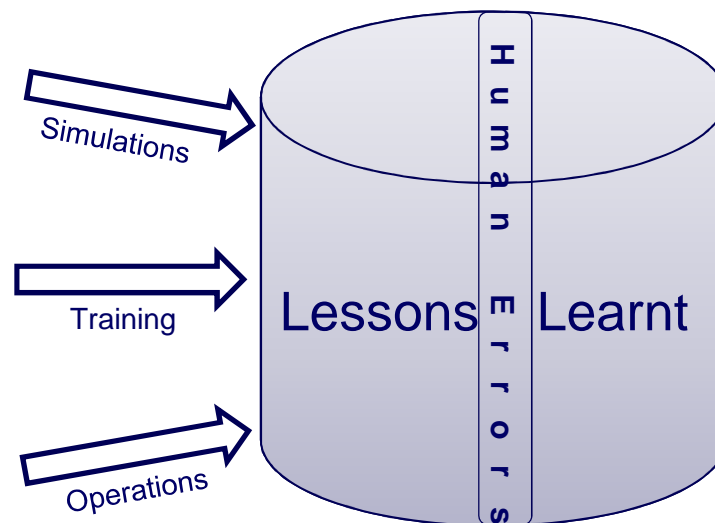
# Flow for Implementation of Lessons Learnt



---

## Lessons Learnt & Human Errors, How to Share

- The process for collecting the lessons learnt is usually well defined.
- However, the critical path is the identification of anomalies as human errors and the analysis of their causes. Furthermore these lessons learnt are not usually spread to the “external community”, but are sometimes kept within the same team.



---

## Proposal for future improvements

How to capitalize experience for improving the human errors avoidance --> (to contribute to Human Dependability increase):

- Use dedicated forms to collect human errors;
- Perform studies to develop an effective approach and to investigate possible methodologies for the analysis of the Human Errors and their relevant Causes;
- Record the solutions adopted to discover, avoid or recover the Human Errors;
- Encourage the collection of human errors and the improvement of Human errors check lists;
- Common Database encompassing human errors, lessons learnt and resolutions.

---

## Outline

- 1 *ESA TEC-QQD Vision*
- 2 *Industry Lessons Learnt (an Example)*
-  3 *Summary and Conclusions*

- 
- We have just seen an example of experience and knowledge to be retained for future space projects.
  - TEC-QQD is committed to foster a structured approach to human dependability by incorporating users needs and requirements from all the stakeholders.
  - TEC-QQD's vision is to support the development of Policy, Analyses, Guidelines, Data, Verification and Procedures for Human Dependability.

---

# QQD Vision and Industry Spin-In

## Structured Approach for Human Dependability in Space Projects

Fabio Restagno  
ESA TEC-QQD  
fabio.restagno@esa.int

David Avino  
Argotec S.r.l. – Turin, Italy  
david.avino@argotec.it