Safety Assessment for Medical Test Lab

Dr. David Endler
Systems Engineering Consultant
Freelancer & Member of oose eG

Agenda

- DLR :envihab test laboratory
- System safety process
- Design iterations
- Safety integrity levels
- Safety requirements and V&V
- Summary

Source:DLR

Introduction Dr. David Endler

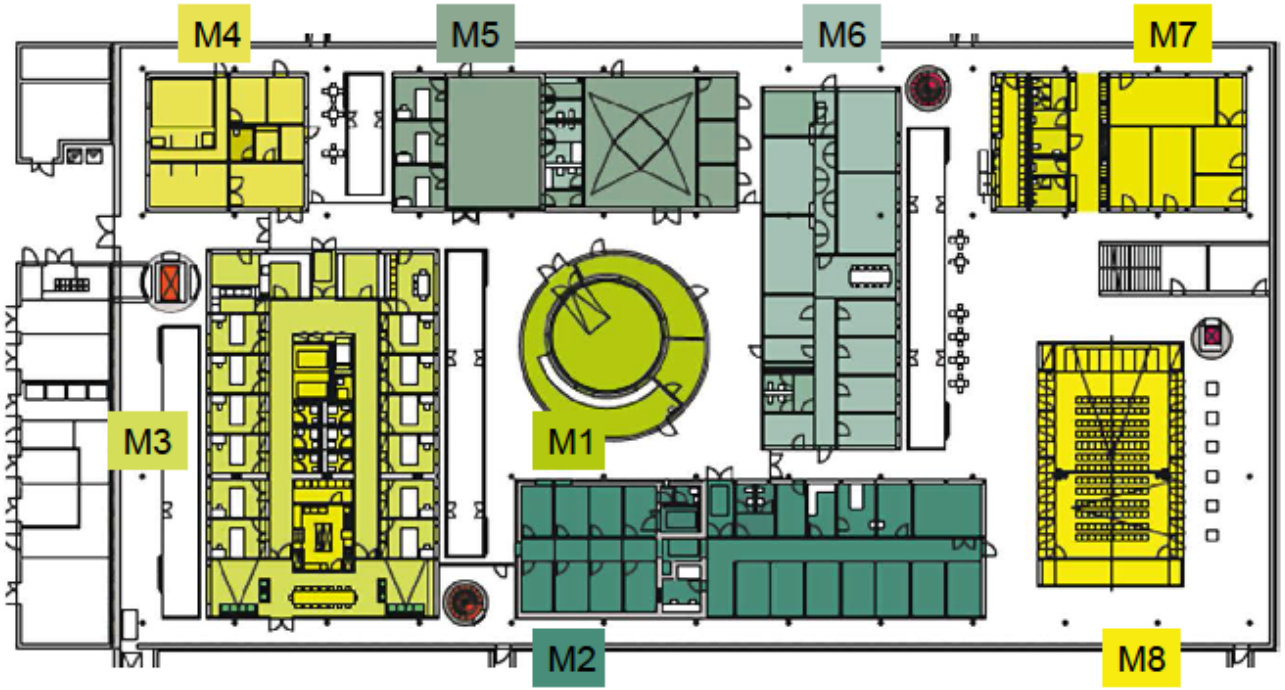
- Systems Engineering Consultant – Freelancer
- Independent member of oose eG
- Deputy Technical Director of INCOSE
- DIN representative in ISO JTC 1 / SC 07 / WG 07 (Software and systems engineering – Life cycle management)
- Accredited trainer for SE-Zert trainings

Environment (1/2)

DLR German Aerospace Center :envihab consists of 8 separate modules

Source:DLR

Environment (2/2)



:envihab Module/:envihab moduls

M1 Kurzarmzentrifuge I/Short Arm Centrifuge I
M2 Physiologielabor I/Physiology Lab I | Barolabor I/Baro Lab I
M3 Wohn- und Simulationsbereich I/Living and Simulation Area I
M4 PET-MRT/MRI-PET
M5 Psychologielabor/Psychology Lab
M6 Biologielabor/Biology Lab
M7 Infrastruktur/Infrastructure
M8 Forum/Forum

DLR Deutsches Zentrum für Luft- und Raumfahrt
Institut für Luft- und Raumfahrtmedizin

Source: DLR

Research of DLR Institute of Aerospace Medicine

The scientific work of the DLR-Institute of Aerospace Medicine in :envihab is concerned, among others, with the following questions:

- What happens to the human body on a flight to Mars?
- How does being confined to bed after a serious illness impact the body?
- How does the lack of daylight affect mood?
- Are there any measures to counteract these adverse effects?

Scope of Research – DLR Institute of Aerospace Medicine

- Cardiovascular, bone and muscle research
- Laboratories for studying the effects of oxygen reduction and pressure decrease on test subjects

Applicable Safety Standards

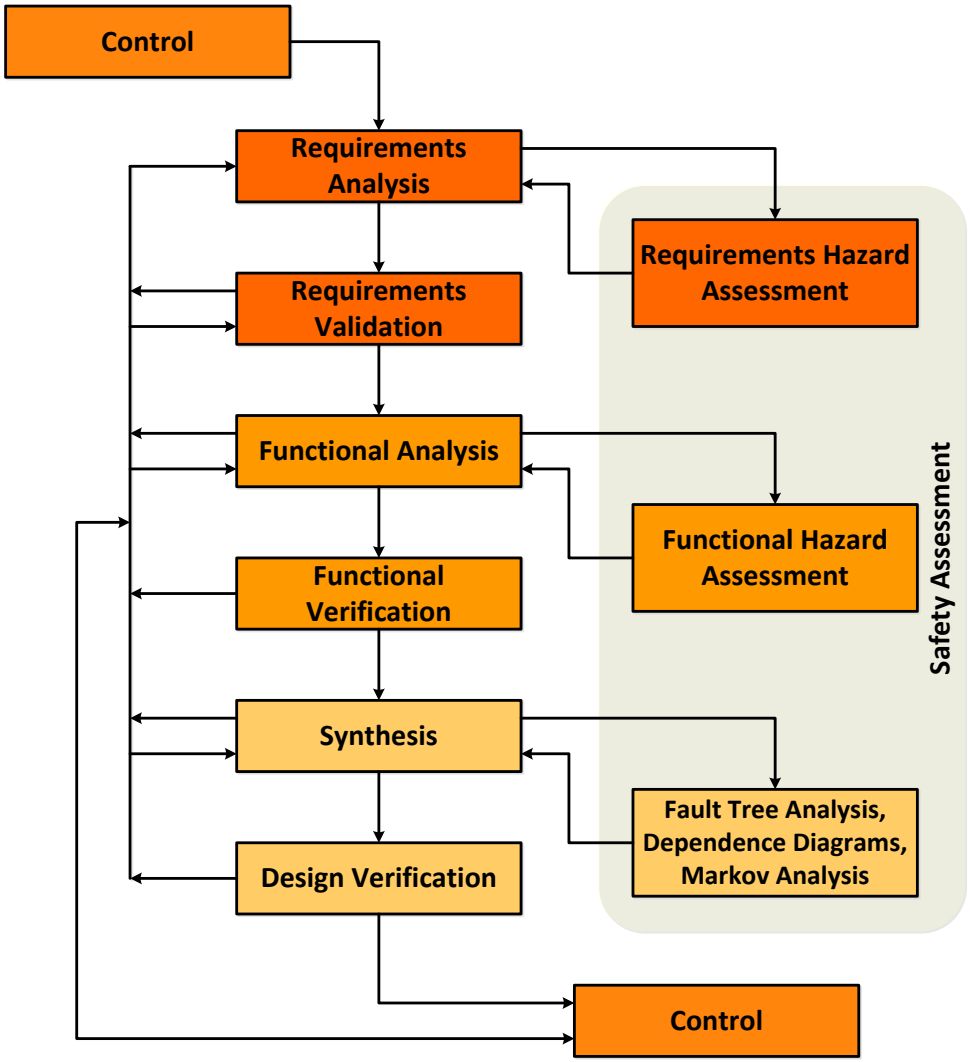
- No safety standard in place for this application

➢ **State-of-the-art**

Standard Safety Process

- Plan System Safety
- Establish system description
- Identify safety requirements
- Identify, analyze and categorize hazards
- Treat risks
- Verify and validate safety requirements

Systems Engineering & System Safety



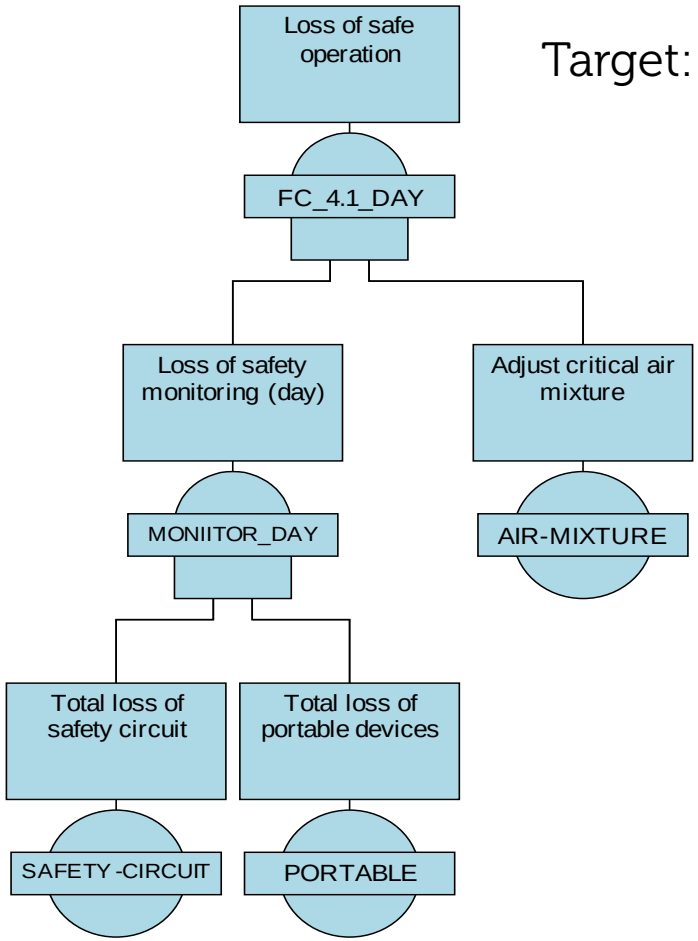
Derived from ISO/IEC 26702:2007, figure 4

Critical Functions

Functions identified:

1. Allow access to laboratory
2. Supply laboratory with fresh air
3. Condition laboratory atmosphere
4. **Ensure safe operation**
5. Determine system state (to control laboratory atmosphere
6. Indicate system state
7. Control laboratory atmosphere
8. Provide comfort
9. Take away used air
10. Allow exit of laboratory

Critical Failure Condition



Target: $1x10^{-8}/h$

Function Independence

Separation of control circuit and safety circuit

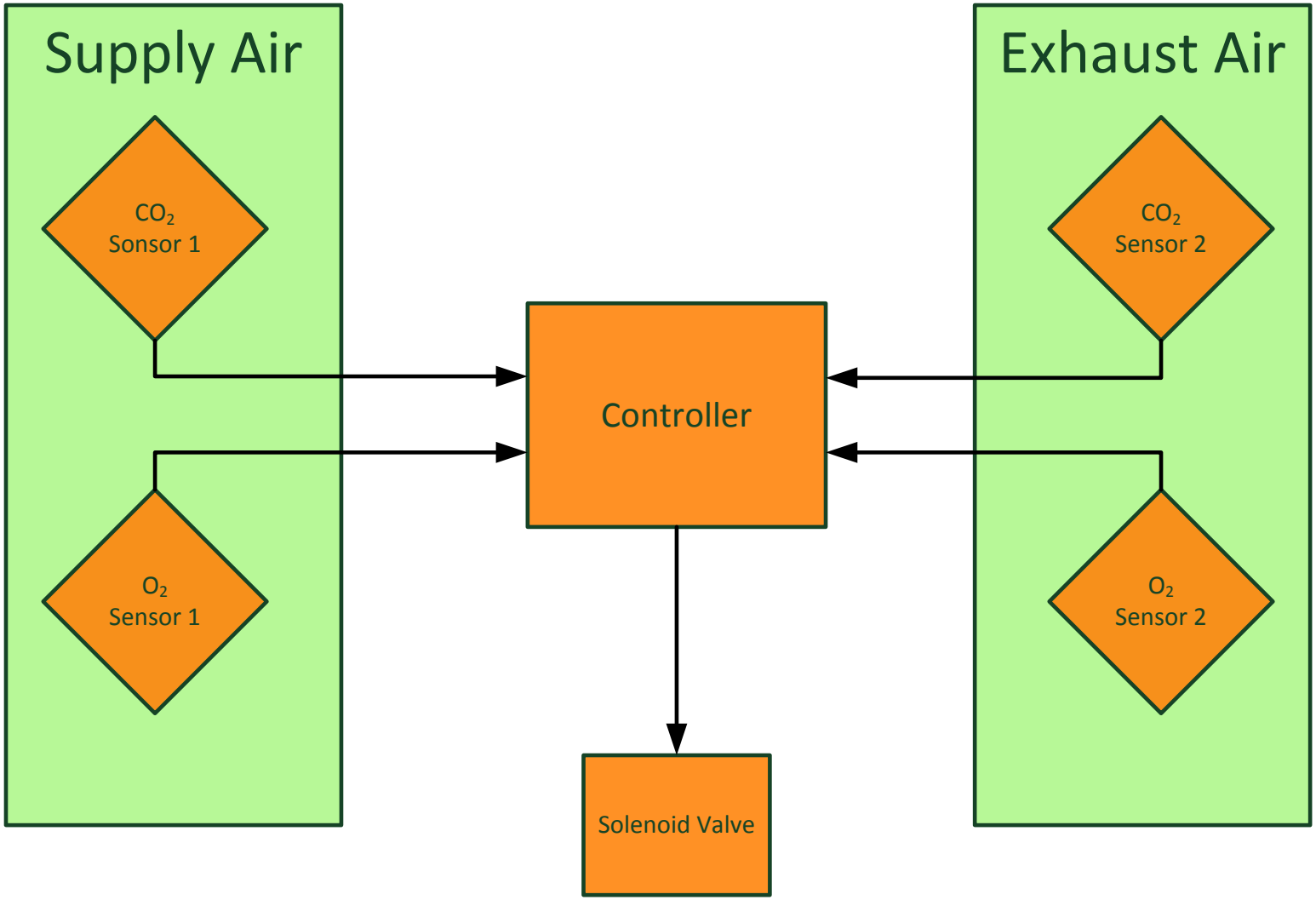
Control Circuit

- Control N_2/CO_2 enriched atmosphere
- Control room temperature
- Control air humidity

Safety Circuit

- Examine gas mixture
- Shut-off N_2/CO_2 supply

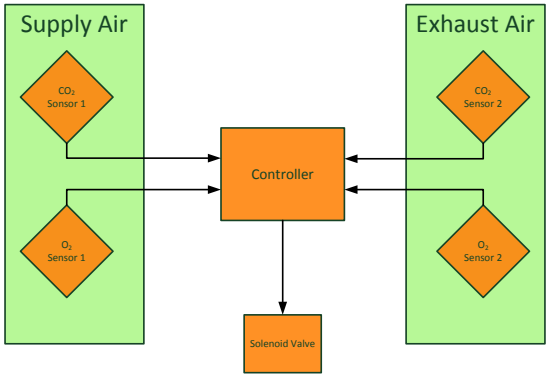
Safety Circuit – Item Independence



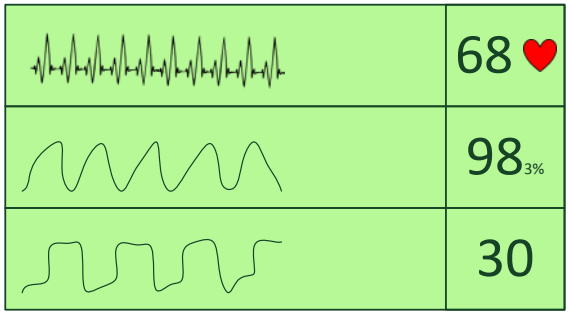
Day and Night Mode

During night additional surveillance required

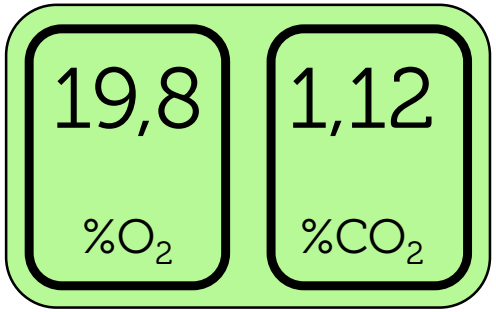
Safety Circuit



Patient Monitor



Portable Device



Function Independence

Separation of control circuit and safety circuit

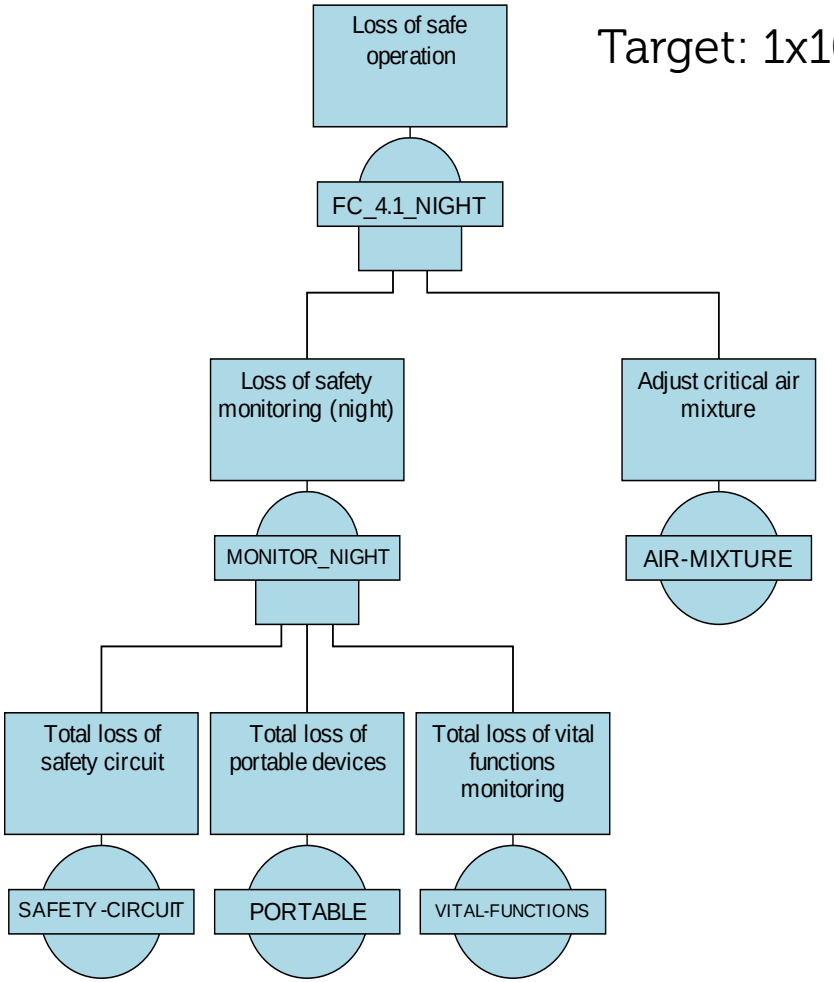
Control Circuit

- Control N_2/CO_2 enriched atmosphere
- Control room temperature
- Control air humidity

Safety Circuit

- Examine gas mixture
- Shut-off N_2/CO_2 supply
- Monitor vital functions of test persons
- Examine gas mixture
- Alarm in case threshold is exceeded

Critical Failure Condition (Night)



Allocation of Safety Integrity Levels

- Safety Circuit meets SIL 2 requirements
- Patient Monitor meets IEC 60601-1 Class 2 requirements
- Portable Device: unclear

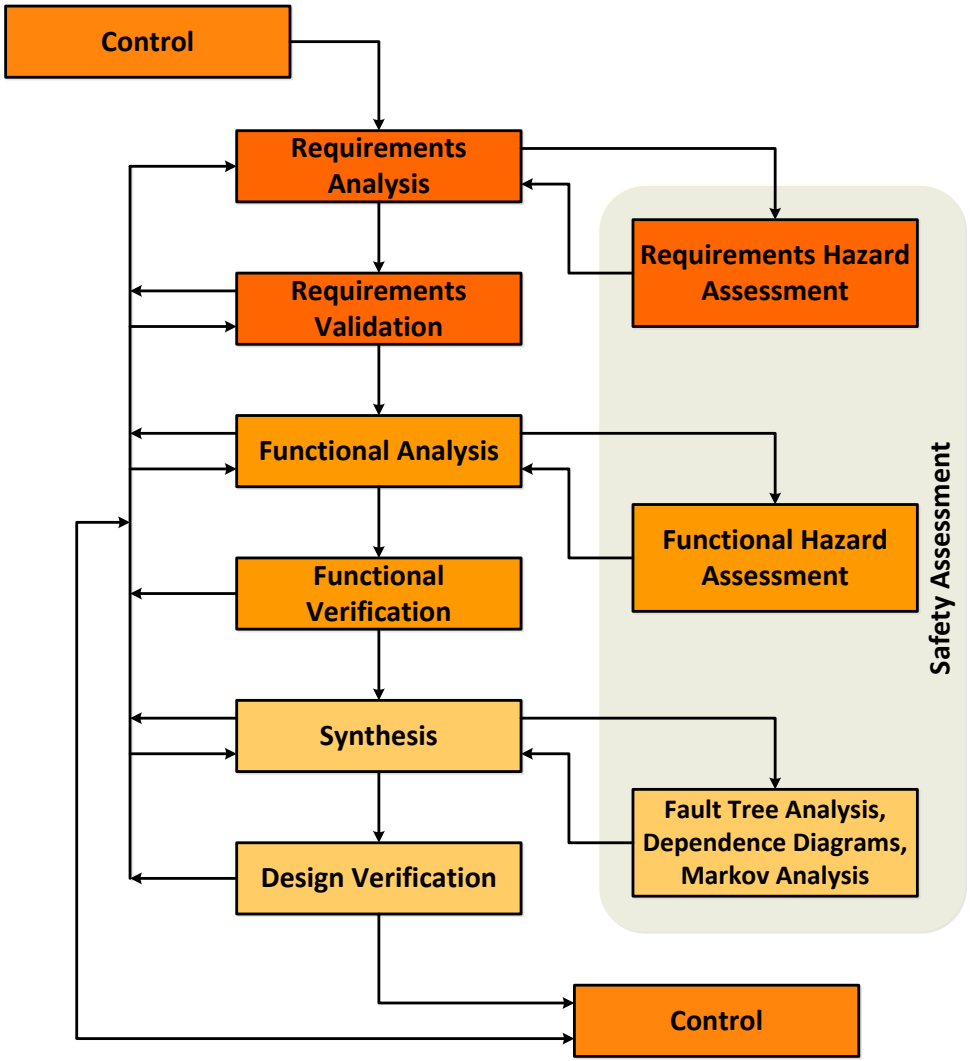
➢ **Equivalent Level of Safety**

Safety Requirements

Safety requirements derived from the safety assessment include

- Failure rates for failure conditions
- Threshold values for sensors in supply and exhaust air
- Emergency procedures level of rigor
- Maintenance of equipment
- Item independence of sensors

Integration of System Safety



Derived from ISO/IEC 26702:2007, figure 4

V&V of Safety Requirements

Verification of safety requirements by

- Test
- Analysis
- Demonstration
- Inspection

➢ **Continuous monitoring of assumptions**

Summary

- DLR :envihab operated by DLR Institute of Aerospace Medicine
- Safety standard for this application: state-of-the-art
- Establish safety requirements early in the lifecycle
- Establish system description to facilitate safety assessment
- Design iterations are inevitable
- Establish substantiation data to pass certification

➢ **Make system safety integral part of system development**