
CIRiS
CENTRE FOR
INTERDISCIPLINARY
RESEARCH IN SPACE

“Space Safety”

TTT 4234-Space Technology I
- Autumn 2016 –

Knut Fossum
06.10.2015

Knut.Fossum@ciris.no
www.ciris.no

Motivation / Objective

- Introduction to space safety as a integral part of all space projects
- Foster the understanding of systemic challenges in complex sociotechnical systems
- Advocate (new) safety methods and process as a tool for increased efficiency and resilience

Outlook

- Some Definitions and Considerations
  - What is safety
  - Why do we do dangerous stuff….
- Basic Principles of Space Safety
  - The cause of accidents
  - The space system design process
  - The safety review process
- The Basic Principles and methods
  - Hazard elimination and limitation
  - Barriers (inhibits) and interlocks
  - Fail-safe design
  - Fault tolerant design
- Space Safety Standards in Europe
  - ECSS standards
  - ECSS Space product assurance branch
  - The effort of harmonization
  - Emerging Principles

Some definitions

- **Safety**
  - "The condition of being free from undergoing or causing hurt, injury, or loss"
- **Risk**
  - "The possibility of loss, injury, disadvantage, or destruction"
  - "The consequence of uncertainty (for something that humans value)
- **Hazard**
  - "Condition that poses a level of threat to life, health, property, or environment
- **Resilience**
  - "A system or organization capacity to anticipate disruptions, adapt to events and create lasting value through safe and efficient operation
- **Efficient**
  - "Doing something well and thoroughly with no waste of time, money or energy

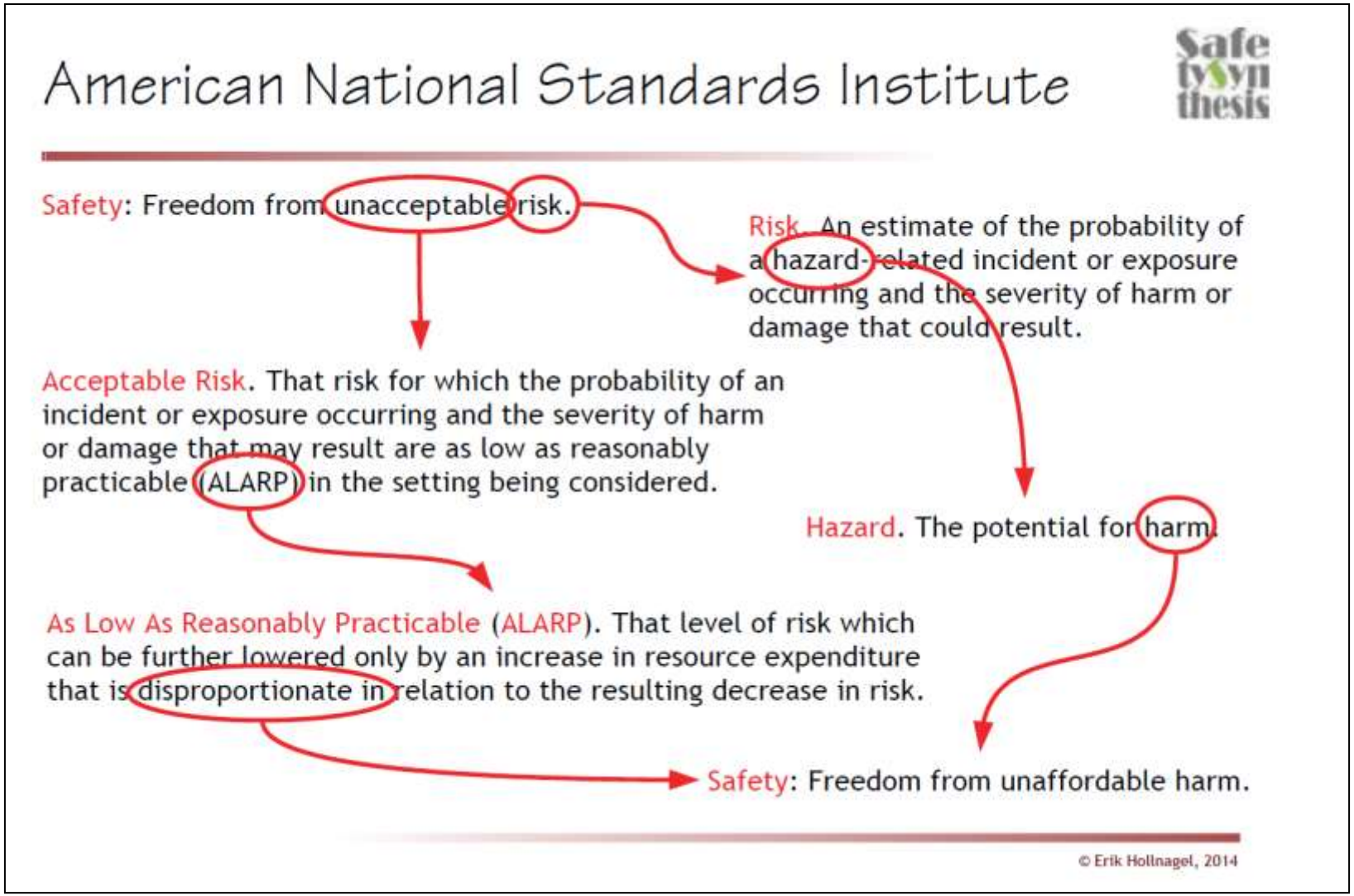
Some contemplations

- **Safety – vs. mission objectives**
  - Implementing sufficient safety often results in compromised mission functionality and objectives
- **Safety and efficiency**
  - Increased safety often result in decreased efficiency
- **Safety and cost**
  - Implementing increased safety measures often result in increased cost
- **Safety, product and quality assurance (PA & QA)**
  - Better safety often result in better PA and QA, and vice versa

Why we do dangerous stuff…

Courtesy of NASA

The balance of safety and efficiency



Basic Principles of Space Safety

- The cause of accidents
- The space system design process
- The safety review process

The Causes

Understanding a complicated world

Safe by design thesis

Accidents, incidents, breakdowns, disruptions,

"Act of god" → Technical failure → Human factor → Organisational culture → Complex systems

The types of causes may change over time, but we still believe in causality

The causes of accidents (1/2)

- **Space missions are risky**
  - Extreme nature of the environment
  - Technological limitations
  - High complexity operations

- **Still, most accidents caused because of..**
  - Design decisions
  - Manufacture decisions
  - Operational decisions

…made within the technological knowledge and capabilities existing at the time….

Credit: AP Photo/Scott Lieberman

The cause of accidents (2/2)

- **3 general types of design and manufacturing errors**
  - Underestimation of environmental conditions
  - Deficient control of known hazardous characteristics
  - Poor and flawed detailed design

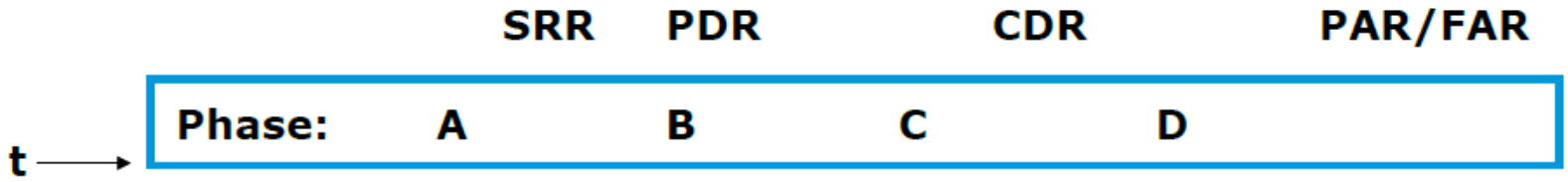
- **Human error, an evolution in approach**
  - In the past, instruction and training
  - Existing, prevention by design
  - Emerging, develop resilient MTO-concepts

MTO = Man – Technology - Organization

Photo: Christine S. Diamond, Lufkin Daily News/AFP/Getty Images

The design process

❖ **Main phases of the ESA design process**



✓ System Requirements Review (SRR)
- ➢ The complete set of requirements is agreed with Industry (optional)

✓ Preliminary Design Review (PDR)
- ➢ Industry presents the draft design and reviewers check with the agreed requirements

✓ Critical Design Review (CDR)
- ➢ Industry presents the final design and reviewers check with the agreed requirements.

✓ Acceptance Reviews (PAR/FAR)
- ✓ Industry presents the built and verified model.
- ✓ Reviewers check that this model matches the agreed requirements

The safety review process (1/4)

- **The safety requirements**
  - The requirements is the foundation for the safety review process
  - A comprehensive set of well accepted safety requirements exist
  - Differences between the dominating space agencies exist
  - “Safety is safety” often results in the same basic principles
  - Cooperation in the ISS program has contributed to harmonization

The safety review process (2/4)

- **The safety panels**
  - The two main entities is the “safety team” and “safety review panel”
  - Safety team (Industry / developer)
    - ✓ Identify hazards and implement safe design
    - ✓ Hold the “burden of evidence”
  - Safety review panel (Agency / customer)
    - ✓ System, payload and ground safety review panels
    - ✓ Conduct reviews, not audits
  - Participating disciplines / entities
    - ✓ Engineering directorate
    - ✓ Mission operation directorate
    - ✓ EVA office
    - ✓ Astronaut office
    - ✓ ISS program office (Shuttle)
    - ✓ Electrical systems
    - ✓ Pressurized systems
    - ✓ Structures & materials
    - ✓ Toxicology
    - ✓ Radiation & biohazard

Review: A formal assessment or examination of something with the possibility or intention of instituting change if necessary
Audit: An official inspection of an individual or organization, typically by an independent body

The safety review process (3/4)

- **The safety reviews and safety data package**
  - The safety team compile a safety data package to the review panel
    - ✓ Identification and description of all hazards
    - ✓ Assessment of all hazards against the proposed design and operational concept
    - ✓ Each hazard is described in a dedicated hazard report
  - Usually each development has minimum of 3 reviews
    - ✓ Safety I – Around same time as the preliminary design review (PDR)
    - ✓ Safety II - Around same time as the critical design review (CDR)
    - ✓ Safety III – Just prior to the shipment to launch site
    - ✓ Ground safety review – Same timeframe as safety III
  - Safety I – Identification and description of all possible hazards
  - Safety II – Implemented controls and verification methods
  - Safety III – Results of the final verification status

The safety review process (4/4)

- **The nonconformance's**
  - If adequate control of a hazard cannot be realized a Non-conformance report (NCR) is initiated
    - ✓ Initiate a dedicated review and decision process of the safety review
  - Developments with unapproved nonconformance report is cannot be deemed as sufficiently safe for flight
  - Solutions are often to be found trough acceptance of higher cost, loss of mission functionality/objectives or increased risk

The Basic Principles and methods

- Hazard elimination and limitation
- Barriers (inhibits) and interlocks
- Fail-safe design
- Fault tolerant design

Principles and methods (1/5)

- **Hazard elimination and limitation**
  - Hazards can often be eliminated by selection of a design solution
    - ✓ Selection of nominal air instead of pure oxygen
    - ✓ Leak-before-burst design for pressure vessels
    - ✓ Power conversion between distribution system and outlets/utilization

1967: Apollo 1 Fire

Courtesy of NASA

1970: Apollo 13 explosion

Illustration

Principles and methods (2/5)

- **Barriers (inhibits) and interlocks**
  - Applied to physically isolate the hazard (barriers)
    - ✓ Separate incompatible materials
    - ✓ Relays between battery and pyrotechnical initiator
    - ✓ Isolation valves between propellant tank and thrusters
  - Commands, personnel, computers & SW and procedures <u>are not</u> barriers and should not be considered so in any design
  - Applied for specific states or situations (interlocks)
    - ✓ Protection from rotating items, heated surfaces and energized lasers
      - Can be removed when hazard source is not activated
    - ✓ Interlocks can also automatically remove the hazard source
      - Such as a power to rotating equipment when barrier is removed.

Principles and methods (3/5)

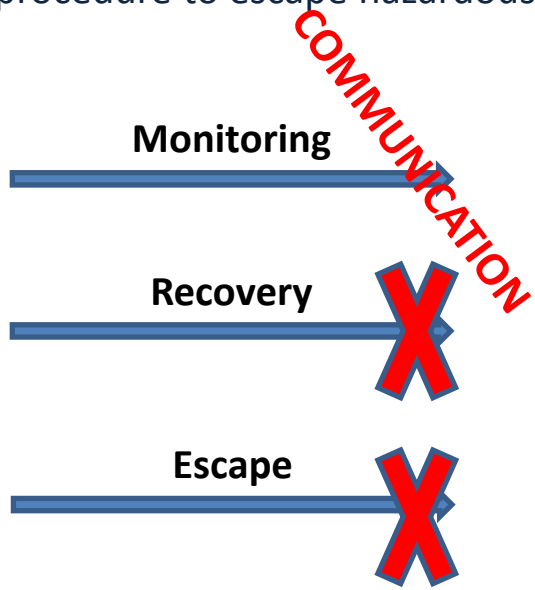
- **Fail-safe design**
  - ✓ Fail passive
    - De-energizes systems awaiting corrective actions
    - Fuses and circuit breakers are typically fail passive devices
  - ✓ Fail active
    - System / equipment remains energized in safe mode awaiting corrective actions
    - Redundant fasteners in structures are example of fail active design
  - ✓ Fail operational
    - System still allow operation but is reverted to safe mode
    - Functionalities that present a unsafe situation is lost
- Fail-safe and redundancy is often used as synonyms, although they are different concepts
  - Redundancy imply increased system reliability
  - Fail-safe does not maintain or ensure safety by enhancing reliability

Principles and methods (4/5)

- **Fault tolerant design**
  - Fault tolerance maintain defined functions despite faults
    - ✓ Implemented by redundancy, fault detection and response capability
  - Hot (active) redundancy
    - ✓ The redundant element is energized
    - ✓ Don’t need to be switched on (or failed system off)
  - Cold (passive) redundancy
    - The redundant system is non-operative
    - Are intentionally switched on upon failure of primary element

Principles and methods (5/5)

- **Monitoring, recovery and escape**
  - All system design must make provisions for:
    - ✓ Identify and monitor critical parameters and functions
    - ✓ Implement system and procedures for recovering safe state
    - ✓ Implement systems and procedure to escape hazardous condition




AP

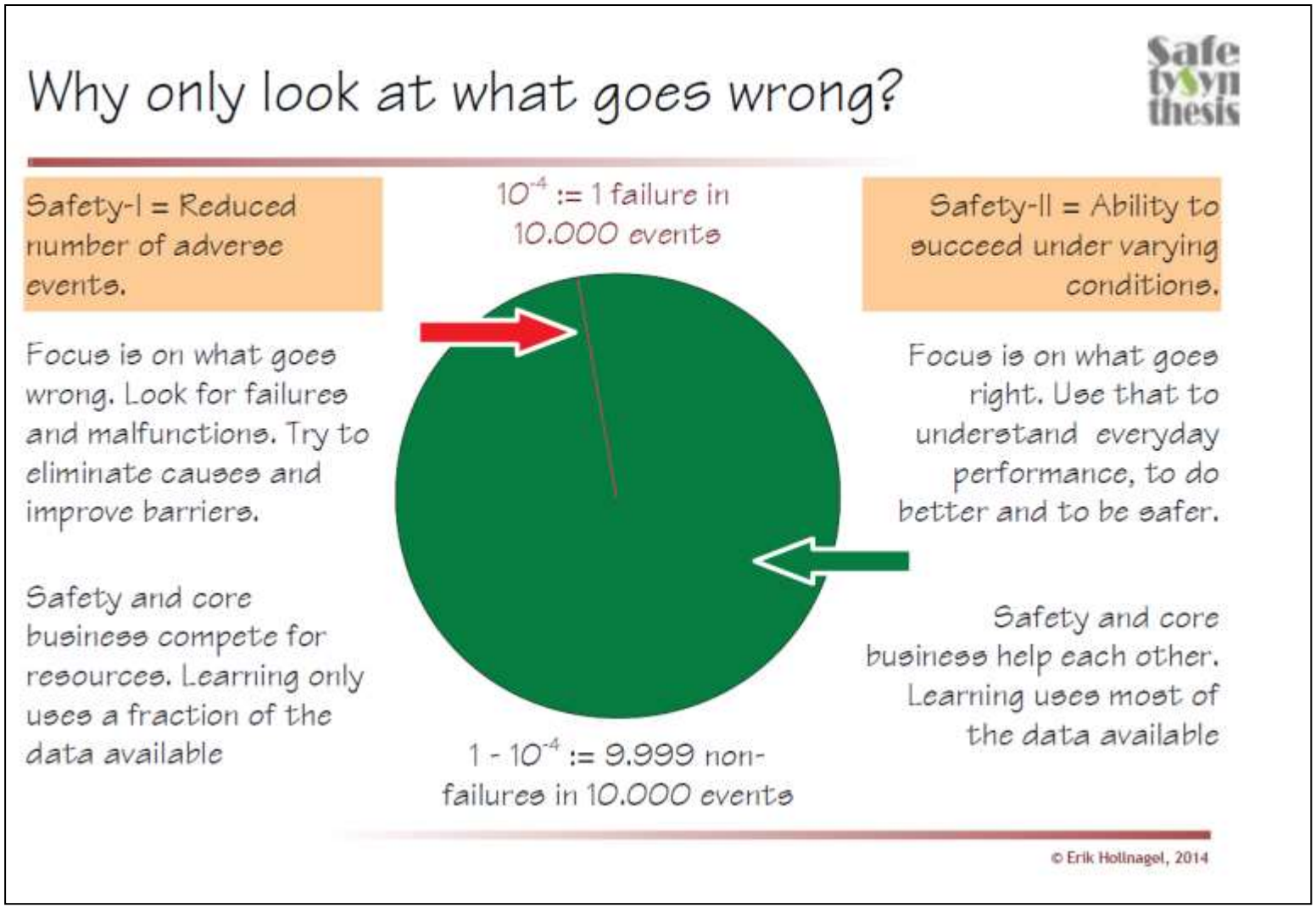
http://www.spacesafetymagazine.com/space-disasters/virgin-galactic/suborbital-spaceflight-need-accidents/

The Investigations

- **Challenger Accident - January 28, 1986**
  - Rogers Commission Report
  - http://en.wikipedia.org/wiki/Rogers_Commission_Report

- **Columbia Accident - February 1, 2003**
  - Columbia Accident Investigation Board (CAIB)
  - http://en.wikipedia.org/wiki/Columbia_Accident_Investigation_Board

Emerging Principles (1/2)



Emerging Principles (2/2)

- **Resilience engineering**
  - Resilience Engineering looks for ways to enhance the ability at all levels of organizations to create processes that are robust yet flexible
    - ✓ To monitor and revise risk models and to use resources proactively in the face of disruptions or ongoing production and economic pressures.

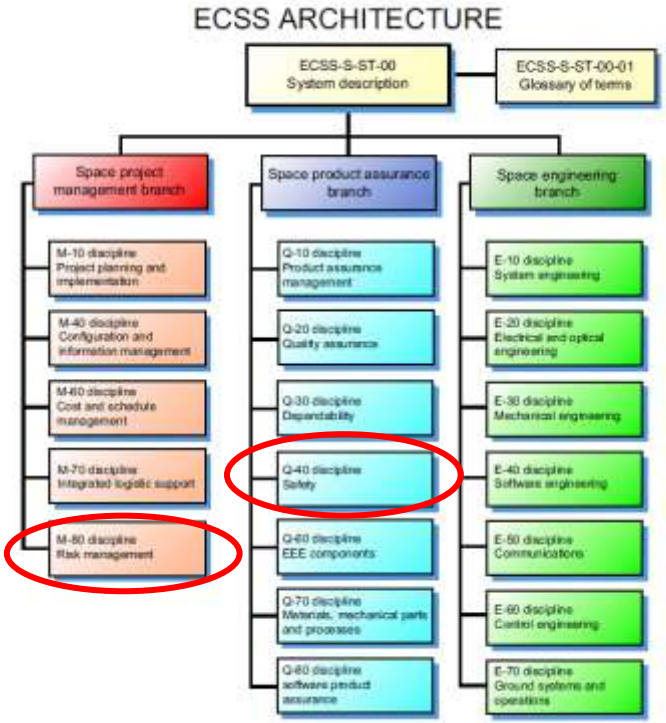
(Conventional risk management approaches are based on hindsight and emphasize error tabulation and calculation of failure probabilities)

Space Safety Standards in Europe

- ECSS standards
- ECSS Space product assurance branch
- The effort of harmonization
- Emerging Principles

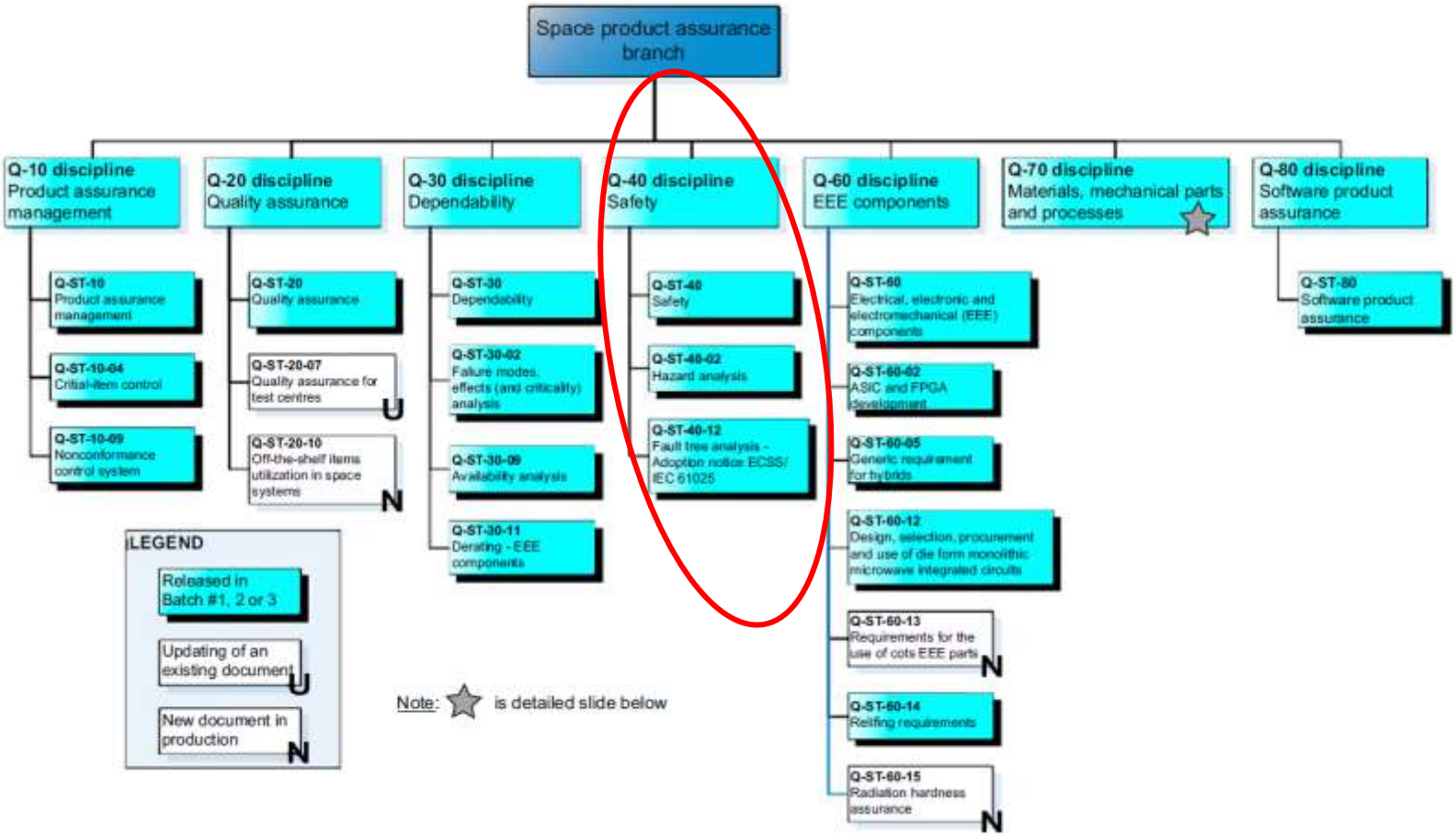
Space Safety Standards in Europe (1/3)

- **ECSS standards**
  - ECSS are themselves not legally binding
  - The application and enforcement is done trough contractual clauses
  - The first truly international set of space safety standards



Space Safety Standards in Europe (2/3)

- **ECSS Space product assurance branch**



Space Safety Standards in Europe (3/3)

- **The effort of harmonization**
  - Organizations involved in harmonization of safety standards
    - ✓ European Committee for Standardization (CEN)
      - https://www.cen.eu/cen/pages/default.aspx
    - ✓ European Committee for Electro-technical Standardization (CENELEC)
      - http://www.cenelec.eu/
    - ✓ European Telecommunications Standards Institute (ETSI)
      - http://www.etsi.org/
    - ✓ European Aviation Safety Agency (EASA)
      - http://easa.europa.eu/home.php
    - ✓ European Cooperation for Space Standardization (ECSS)
      - http://www.ecss.nl/
    - ✓ European Space Agency (ESA)
      - http://www.esa.int/ESA

http://iaass.space-safety.org/ / http://www.spacesafetymagazine.com/

Understanding the role of space safety

Space Safety Regulations and Standards (Chapter 3)
http://www.sciencedirect.com/science/book/9781856177528

Safety Design for Space Operations (Chapter 1)
http://www.sciencedirect.com/science/book/9780080969213

Safety Design for Space Systems (Chapter 4)
http://www.sciencedirect.com/science/book/9780750685801

Thank you for your attention!

Knut.Fossum@ciris.no