Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

IAMP Institut für Angewandte
Mathematik und Physik

ESS FBIS PDR – Project Risks

Christian Hilbes - Safety Critical Systems Research Lab - ZHAW

Sent (near Scuol) Switzerland, 29.07.2017 18:15

Main concern: Are we building the right system?

Are we building the right system?

- (1) FBIS has to support ESS Operation, it should not prevent it.
  - Otherwise "workarounds" will be quickly found, resulting in uncontrolled "unsafe" situations.

- At this time, there is insufficient information on the Concept of Operations for ESS.
  - We work with "Benchmark Use-Cases" that are largely based on assumptions.

Are we building the right system?

- (2) FBIS has to control MP-related Actuation Systems such as to put the facility into a “protected state”.

- At this time, there is insufficient dependable information on the functional behavior of those Actuation Systems in the context of Machine Protection.
  - Applies to LEBT- and MEBT-Choppers and Ion-Source Interlock.

Are we building the right system?

- (3) FBIS main role: Implement Logic for Fast Protection Functions.

- At this time, Requirements Specifications for Fast Protection Functions are still being developed.
  - Physical deployment of FBIS depends on sensor locations and redundancy patterns.
  - Challenging ESS availability goals might well force us to go to 2oo3 architecture patterns.

Are we building the right system?

- Time Schedule is pressing, no more time to wait…
  - Development of FBIS SRS and Architecture based largely on hopefully reasonable assumptions
  - ESS SEMP not fully respected
    - SRS not complete yet → no Functional Review… but we need a PDR now to proceed with the development!

- Risks
  - Requirements Specifications for FBIS might be incomplete
  - FBIS Architecture might not fit ESS needs

Risk of Uncomplete Specs…

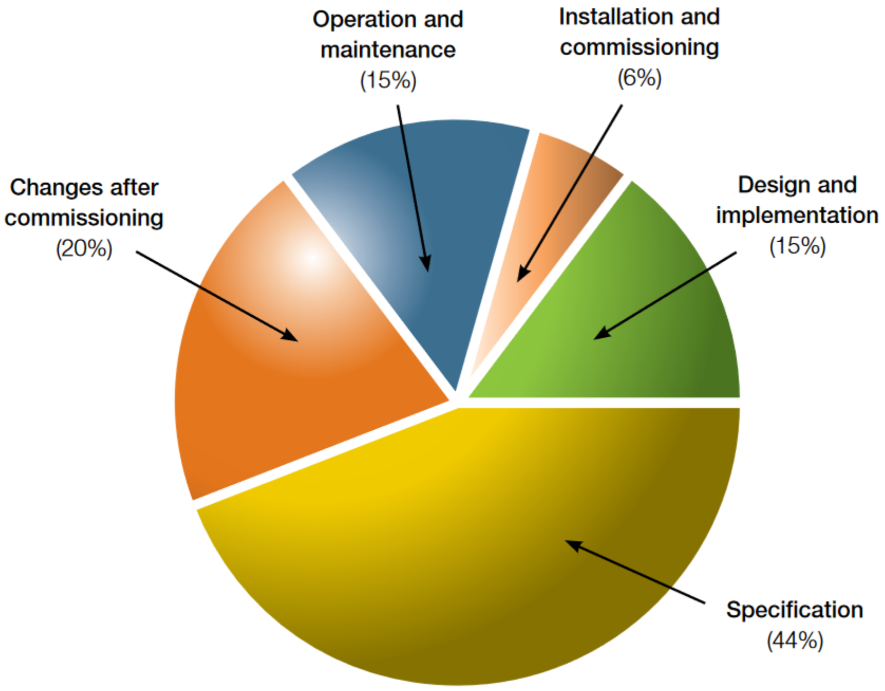
From an old source…

HSE – Out of Control

Why control systems go wrong and how to prevent failure

2nd Edition, 2003 (Original 1995)

http://www.hse.gov.uk/pubns/priced/hsg238.pdf



Root cause of accidents by phase

Mitigation from side of ZHAW

- Devise very flexible architectural elements for FBIS
  - Pro: *Everything can be done…* might be useful anyway, since ESS is a research facility… and things tend to evolve in such an environment…
  - Con: flexibility can be increased through “cleverness” only up to a certain point… after that, complexity will increase…
  - We have to keep the balance and avoid unnecessary complexity!

Requests from ZHAW towards ESS

- (1) FBIS has to support ESS Operation, it should not prevent it.

- ESS should make sure that Operations Responsible check and confirm/update those “Benchmark Use-Case” Assumptions.
  - ESS Operations team in place?

Requests from ZHAW towards ESS

- (2) FBIS has to control MP-related Actuation Systems such as to put the facility into a “protected state”.

- ESS should make sure that the LEBT- and MEBT-Chopper and Ion Source get thoroughly tested (!) with respect to their MP-related functions!
  - Actuation and Recovery performance; Interface behavior…
  - Planned on several occasions but never (?) done.

Requests from ZHAW towards ESS

- (3) FBIS main role: Implement Logic for Fast Protection Functions.

- The MP group has set up a perfect process for Protection Function Specification.
  - Identification of Damage Events → Risk Estimation → Tolerable Occurrence Magnitude → Overall Protection Function Specification → Allocation to Protection Functions and other measures…
- ESS should dedicate adequate resources to the Hazard and Risk Analysis effort to ensure a swift execution of this process!
  - This might not only affect MP group…

View from Mot da Set Mezdis (near Sent), Switzerland, 01.08.2017 06:10