EUROPEAN SPALLATION SOURCE

Machine Protection Implementation

Systems Engineering Approach – Organization – Schedule

Christian Hilbes, ZHAW

Lund
Date: 2015-12-08

Overview

- SE Approach
  - Background and Motivation for System-of-Systems Approach
  - Application of SoS-SE concept for MP
- Organization
  - Project Structure Concept
  - Review Concept
- Schedule
  - Two phase approach

Purpose of Systems Engineering

- From DoD Systems Engineering Fundamentals:

  "Its [the SE process] purpose is to provide a structured but flexible process that transforms requirements into specifications, architectures, and configuration baselines."

- That's what it is… but why should we do that?

  "The discipline of this process provides the control and traceability to develop solutions that meet customer needs"

- The more challenging our goals are, the bigger the risk for failing meeting "needs" is getting.
- Systems Engineering is Risk Mitigation!

Systems Engineering and Safety Critical Systems Development

- SE is required by all standards dealing with Safety Critical Systems Development → focus is on mitigating the risk for systematic failures like:
  - Incomplete or inadequate requirements specifications.
    - You cannot protect yourself from things you didn't anticipate.
    - Requiring to do the wrong thing will cause problems.
  - Design flaws.
    - Like inadequate choice of sensor or actuation systems.
  - Implementation errors.
    - Like software bugs or badly soldered electronic components.
- The safer it should be, the more stringent the SE requirements.

Choosing the right SE approach

- Lots of SE standards, literature, best practices, … but which way to go?
- Is there “the right” SE approach?
- Should we blindly follow a specific standard, just because it’s a standard?

- Goal of SE: mitigate risks for project failure.
- First, identify the risk situation, then choose an SE approach!

Risks that might impact Machine Protection SE at ESS

- Large number of networked systems need to work together to reach the ESS goals.
  - Including availability goals!
- Each single system requires a very high degree of expertise from very differing fields.
  - Proton Source, Beam Monitoring, HF Systems, Magnet Systems, Fast Beam Choppers, …
- Wide spread expert and research groups, “managed” by different divisions, working in different countries on the primary goal, which is to produce neutrons.

Risks that might impact Machine Protection SE at ESS

- Identified hazard: classical SE “single-system view” and Top-Down requirements elaboration might not be manageable as expected.
- Consequences:
  - Partial or latent “loss of control” of the process.
  - If hazard impacts systems having no role within MP: specified facility operation parameters might not be reacheable without a time-schedule delay.
  - If hazard impacts systems playing a role within MP: uncontrolled risk for machine damage!

    → Not acceptable! We need to take measures…

Notes on Beam Interlock System and Machine Protection

- Machine Protection cannot be achieved when there is only a Beam Interlock System
  - BIS does not include sensor subsystems needed to detect potential problems, nor does it include actuation systems capable of bringing the facility into a safe state.
- Without systems that detect hazardous situations, and without systems that enforce a safe state, the BIS is powerless.
- The BIS is conceptually the easiest part of the whole.
  - Although it has tough timing requirements, non-trivial logic and plays a central role in every beam-related protection function…

Notes on Beam Interlock System and Machine Protection

- Machine Protection does not only mean “to protect from beam induced damage”.
- Machine protection has to prevent and mitigate damage from any source.
  - This means that there might well be a need for protection functions implemented in local systems that have no link to the Beam Interlock System at all.

System-of-Systems Engineering Approach

- The Machine Protection “System” exhibits all major characteristics of a System-of-Systems.
  - There is no single dedicated “Machine Protection System”
- Adapt extended architectural decomposition pattern
  - “System” composed of “subsystem” is not enough.
  - “System-of-Systems” composed of “constituent systems” solves the issue.
  - Example:
    - The proton source will feature a function to switch-off the beam upon request from the Beam Interlock System.
    - Saying that the proton source is a “subsystem” of a “machine protection system” is not adequate.

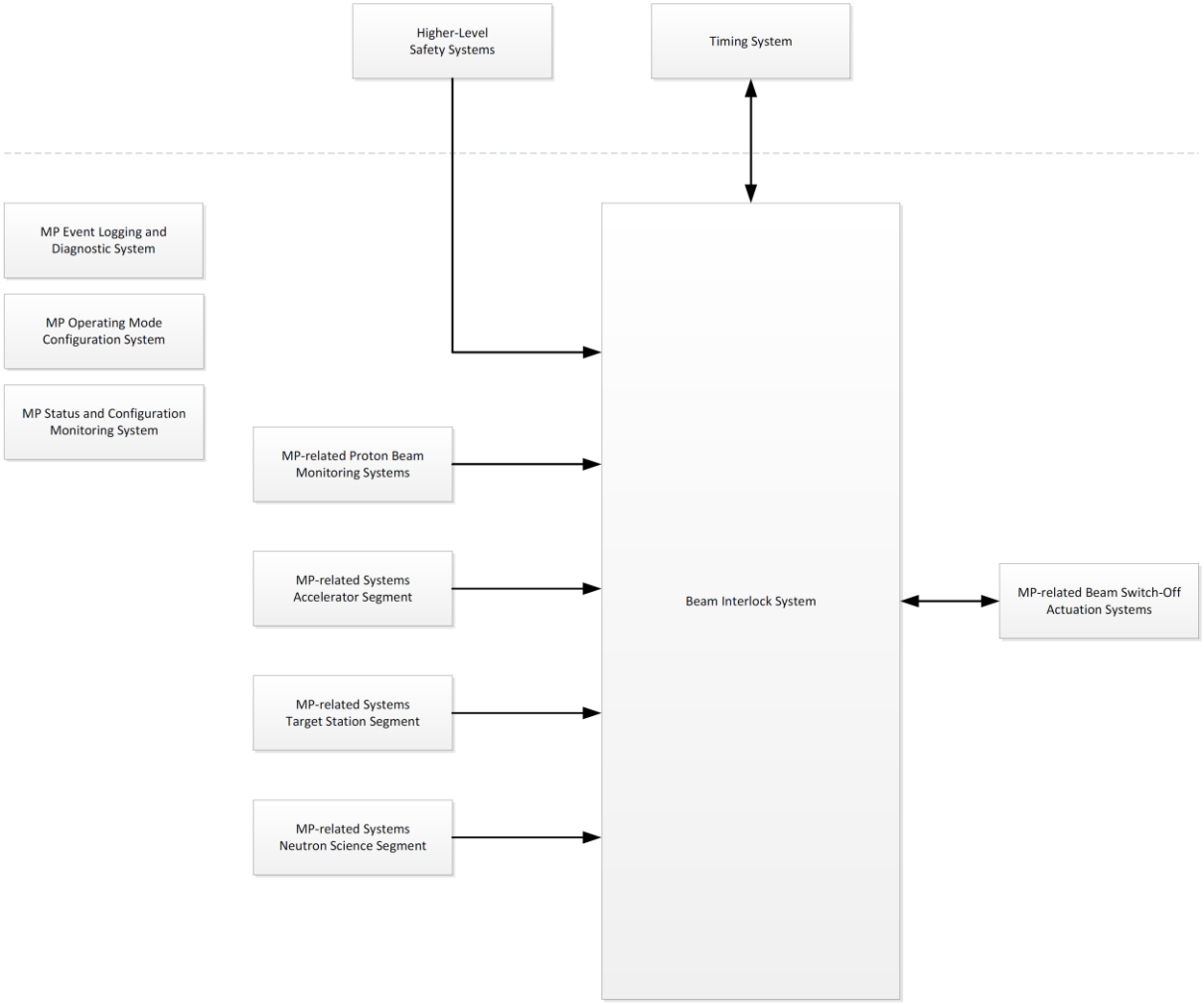
Differences SoS-SE versus not SoS-SE Capability Objectives and High-Level Requirements

- What an SoS is supposed to do is specified in terms of “capability objectives”
  - The capability objectives specify the emergent properties the SoS should have.
- Capability objectives are translated into “high-level requirements” for the constituent systems
  - Example Proton Source System MP-related functions
    - Traditional SE: perform a “centralized” hazard analysis (by a team of experts) and directly formulate protection function requirements that the Proton Source Team should implement.
    - SoS-SE: performing a hazard analysis and specifying adequate protection functions is a high-level requirement for the Proton Source Team.

Differences SoS-SE versus not SoS-SE Architectural Framework

- Instead of developing a “System Architecture”, SoS-SE defines an “Architectural Framework” the constituent systems will have to fit in.
  - Definition of classes of constituent systems.
  - Expected behaviour in terms of high-level requirements and capabilities per class.
  - Minimal interface requirements per class.

MP-SoS Top-Level Architectural Framework



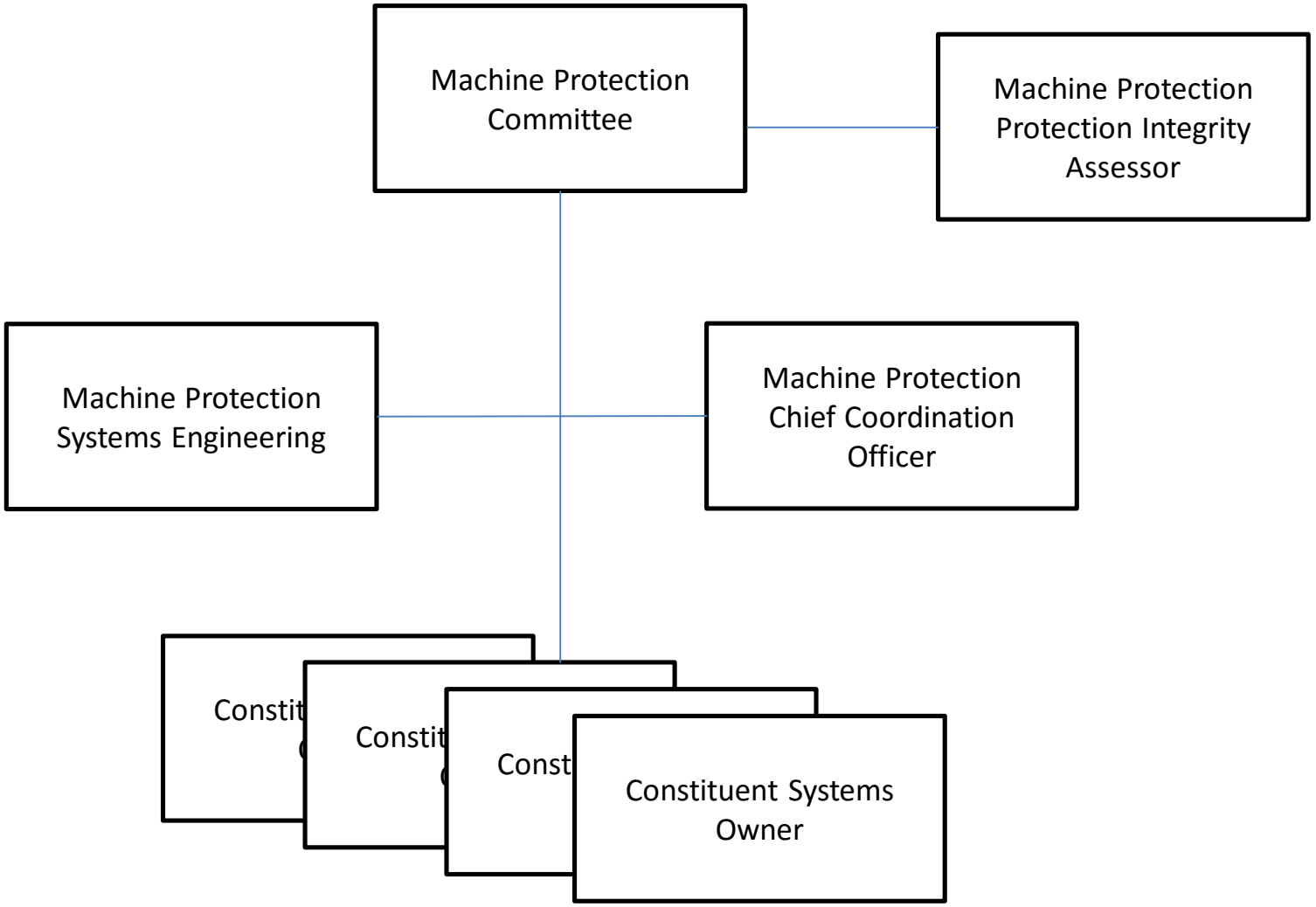
Impact on Constituent Systems Development

- Constituent Systems are independently managed by their owners.
  - No “Machine Protection System Project Manager”…
- Constituent systems are developed according to the general ESS SE rules, with the following additions:
  - In the Requirements Elaboration Phase, the constituent systems have to take into account:
    - the high-level requirements applicable to their class.
    - the MP-SoS Architectural Framework: interfaces and expected behaviour with respect to MP-related functions.
  - Reviews of MP-SoS constituent systems are not independent.

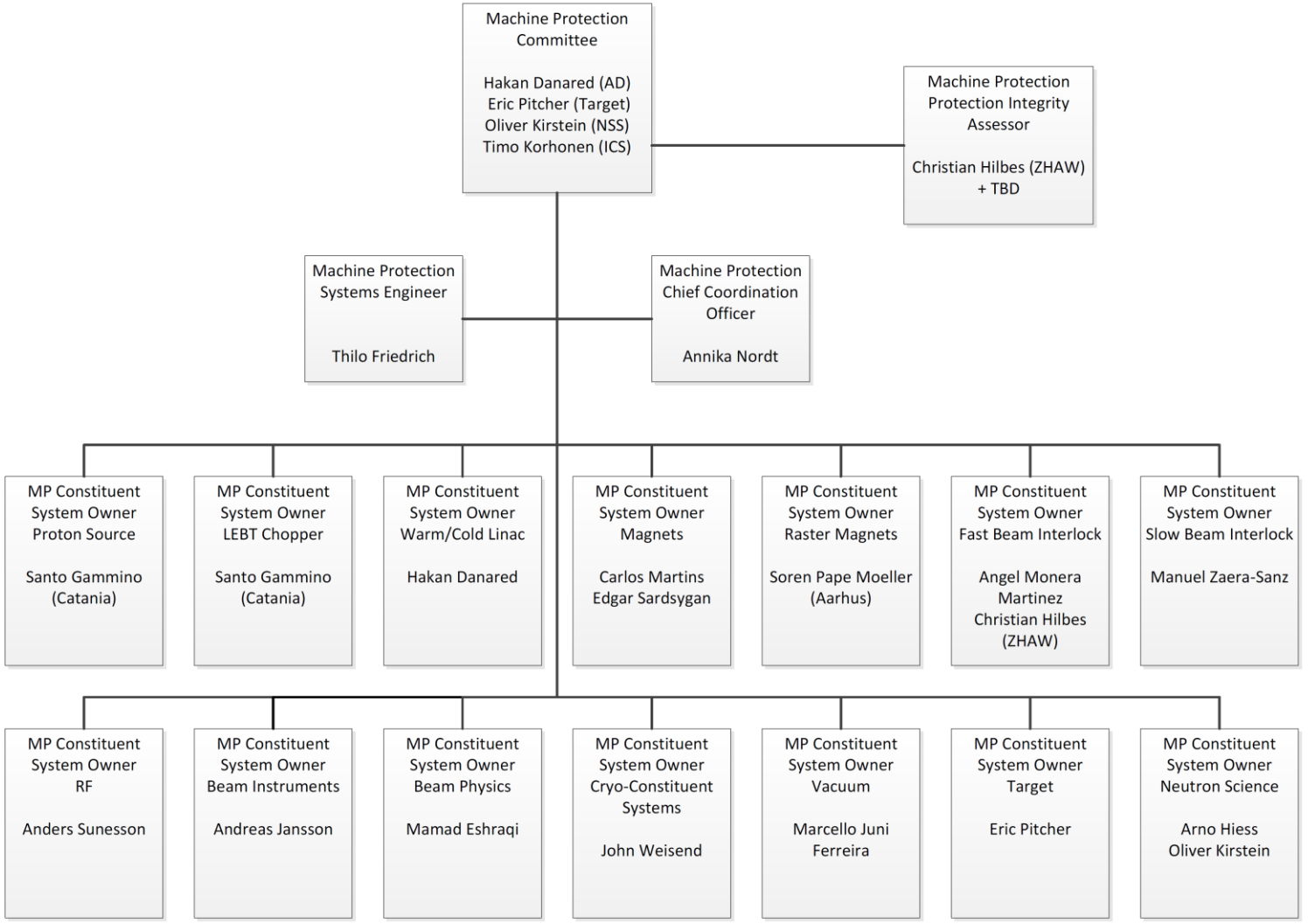
MP-SoS Project Structure Concept

- Reaching the MP-SoS Goals while keeping the constituent systems independence as needed:
  - Requires cross-divisional MP-SoS project management structure.
  - Requires exhaustive coordination effort between involved constituent system owners.
  - Requires additional System-of-Systems level of SE management.
  - Requires independent protection integrity assessment.

MP-SoS Project Structure Concept



MP-SoS Project Structure



MP System-of-Systems Reviews

- Introduce MP System-of-Systems Review activities in addition to the constituent systems reviews.
  - Each constituent system is reviewed according to the provisions of the ESS-SEMP.
    - This includes of course a review of MP-related functionality of the constituent system.
    - Goal: Make sure the single constituent systems are ok.

ESS-SEMP Technical Cycle – Reviews Overview

Review	Focus on…	"Go" for…	Target Baseline
Functional Review	Requirements	Architectural Design Phase	Functional Baseline
Preliminary Design Review	Architectural Design	Detailed Design Phase	Allocated Baseline
Critical Design Review	Component Design	Component Procurement	Design Baseline
Test Readiness Review	Component V&V Evidence	Online Testing	
Acceptance Review	System Verification Evidence	Preliminary Operation	Performance Baseline
Operational Readiness Review	System Validation Evidence	Full Operation	Operational Baseline

MP System-of-Systems Reviews

- Introduce MP System-of-Systems Review activities in addition to the constituent systems reviews.
  - Each constituent system is reviewed according to the provisions of the ESS-SEMP.
    - This includes of course a review of MP-related functionality of the constituent system.
    - Goal: Make sure the single constituent systems are ok.
  - An additional MP-SoS review focusses on end-to-end machine protection capability.
    - Consider the big picture is ok.
    - Goal: Make sure protection integrity levels are achieved.

MP-SoS Reviews

MP-SoS Review	Focus on…	"Go" for…	MP-SoS Target Baseline
MP-SoS Functional Review	MP-SoS Capability Objectives and Architectural Framework	"Roll-Out" of MP-SoS Concept and additional requirements to constituent systems SE	Functional Baseline
MP-SoS Preliminary Design Review	Constituent Systems Architectural Design PDR Results	Detailed Design Phase of constituent systems	Allocated Baseline
MP-SoS Critical Design Review	Constituent Systems Component Design CDR Results	Constituent Systems Component Procurement	Design Baseline
MP-SoS Test Readiness Review	Constituent Systems V&V Evidence	MP-SoS End-to-End Online Testing	
MP-SoS Acceptance Review	MP-SoS End-to-End Verification Evidence	MP-SoS Preliminary Operation	Performance Baseline
MP-SoS Operational Readiness Review	MP-SoS End-to-End Validation Evidence	MP-SoS Full Operation	Operational Baseline

Protection Integrity Assessment Architectural Design Level

- No plan to perform systematic Protection Integrity Assessment Activities at the Functional Review Level
  - We do not want to rely on the existence of formal requirements specifications for each constituent system.
- Protection Integrity Assessment Activities start at the Preliminary Design Reviews
  - Based on what is planned to be implemented.
  - Assess if needed MP-related functions have been designed into the constituent systems
  - Assess the rationale for those MP-related functions
  - Assess compliance with respect to protection integrity requirements (architecture).

Protection Integrity Assessment Component Design Level

- …at the Critical Design Review Level
  - Based on detailed design descriptions of constituent systems components.
  - Assess if needed MP-related functions have been integrated into the components design.
  - Assess compliance with respect to protection integrity requirements:
    - Systematic Protection Integrity (component design robustness)
    - Hardware Protection Integrity (quantitative assessment based on FMEDA)

Protection Integrity Assessment Verification and Validation Level

- …at the Test Readiness Review Level
  - Based on verification reports of constituent systems.
  - Assess if all constituent systems behave as specified.
- …at the Acceptance Review Level
  - Based on MP-SoS verification reports.
  - Assess if MP System-of-Systems behaves as expected.
- …at the Acceptance Review Level
  - Based on preliminary operation reports
  - Assess whether MP-SoS is ready for full operation.

Schedule Vision

- Schedule for MP-SoS development and reviews are proposed in two phases, following the ESS schedule:
  - Constituent Systems and Protection Functions needed for Low Beam Power Operation
  - Constituent Systems and Protection Functions needed for High Beam Power Operation

MP-SoS.FR End 2015	Reviews of protection functions and related constituent systems needed for low beam power operation				
	MP-SoS.PDR	MP-SoS.CDR	MP-SoS.TRR	MP-SoS.SAR	MP-SoS.ORR
	Mid 2016	End 2016	Mid 2017	End 2017	Mid 2018
	Reviews of protection functions and related constituent systems needed for high beam power operation				
	MP-SoS.PDR	MP-SoS.CDR	MP-SoS.TRR	MP-SoS.SAR	MP-SoS.ORR
	End 2017	Mid 2018	End 2018	Mid 2019	End 2019