Commonalities and Differences in Functional Safety Systems between ISS Payloads and Industrial Applications

6th IAASS Conference, Montreal, 21-23 May 2013

M. Malyshev (1) , J. Kreimer (2)

(1) HE Space Operations B.V. / Netherlands , (2) Astrium Space Transportation/Germany

The paper is intended to address the following points

- Assess differences and commonalities in technical safety requirements and certification processes for programmable ("computer-based") functions between ISS context and industrial applications
- Show example of existing (under development) functional safety system in EML payload
- Evaluate advantages and limitations of using COTS functional safety items (compliant to IEC 61508 or similar standards) in ISS payloads

Context

- ISS provides a platform for Experiments in micro-g/reduced gravity

- ISS Program poses less requirements on Payloads than on ISS elements and systems, only safety requirements are imposed, e.g.:
  - an ISS system/vehicle "…**shall perform its function** when exposed to the utilization environment … or in case of a failure…";
  - a payloads "…**shall not produce unsafe conditions**…" in a similar case. Note: damage to ISS and other payloads is a hazard, hence physical interfaces (primarily electrical) have to be compliant and prevent failures propagation

Context (cont.)

- No ISS program requirements w.r.t. performance, project management or quality
  - typically payload sponsor requirements more restrictive than ISS program w.r.t. design and development, quality, reliability
- COTS items use with limited restrictions
  - compliance to few basic technical requirements (primarily – materials utilization)
- Complex experiments
  - require flexible functions, long term operations, need experiment parameters /protocols change

    e.g. robotics, materials processing
    - Computer based control is needed
    - Functional Safety standards - (IEC 61508 as a “baseline”)

Functional Safety COTS items

- High variety of COTS items - but many industries and applications where safety is a priority
  - Medical
  - Process industries
  - Automotive
  - Aerospace
  - Nuclear

  many producers and items on commercial market

- COTS items of interest for experiments (ISS payloads)
  - PLCs/CPUs and
    - relevant I/O modules
    - SW development tools
  - Sensors and actuators

Functional Safety Requirements

- ISS Payloads Safety
  - Technical requirements for hazardous functions (few pages in SSP 51700), failure tolerance is basic requirement, tailoring depending on criticality (one- or two- failure tolerance)
  - Policy and approach for safety risk management outlined

- IEC 61508
  - Technical requirements (Part 2 and Part 3)
  - Safety Management Requirements (Part 1), covers all life cycle (from concept to disposal)
  - Both tailored for required safety risk reduction level, Safety Integrity Level: SIL 1 to SIL 4

Fail Safe approach

ISS Payloads functional safety requirements - comparable to requirements of standards used for ground applications

- "fail safe" approach is basic functional safety requirements for ISS Payloads - requirements for computer based systems outlined in MA2-97-083 (PSRP Interpretation Letter) – about 10 requirement items
- IEC 61508 – requirements address most of MA2-97-083 items in detailed way (provide references and definition of design and implementation techniques, development tools, documentation requirements, etc.)

  "Fail safe" is not explicitly mentioned, but intended
- Items designed / built according to IEC 61508 (or similar standards) - expected to be "fail safe" in compliance to letter MA2-97-83

Certification Processes

ISS Payloads Safety (SSP 30599, Appendix J)

- Certification of compliance process, assisted by ISS Program, via reviews by a Payload Safety Review Panel
- Tailored depending on experiment complexity and hazard potential

IEC 61508:

- Safety Assessment Required, level and independence tailored for required Safety Integrity Level
- SIL capability of items may be certified by different organizations (certification bodies)
- Items manufacturers are interested to obtain SIL capability certification to get better market position

EML as Safety Instrumented System

Electromagnetic Levitation

Uses

- Levitate an electrically conductive object using electromagnetic fields
- Heat and melt samples
- Process liquid samples without contact to a container wall
- Undercool samples
- Study thermophysical data

Experiments

- Sample Size: 5-8 mm diameter
- Materials: Metals, Alloys, Semiconductors
- Temperatures: up to 2100 °C
- Melt Cycles: seconds to minutes

EML Modules inside EDR rack (Training Model)

Liquid sample in ground coil

EML as Safety Instrumented System

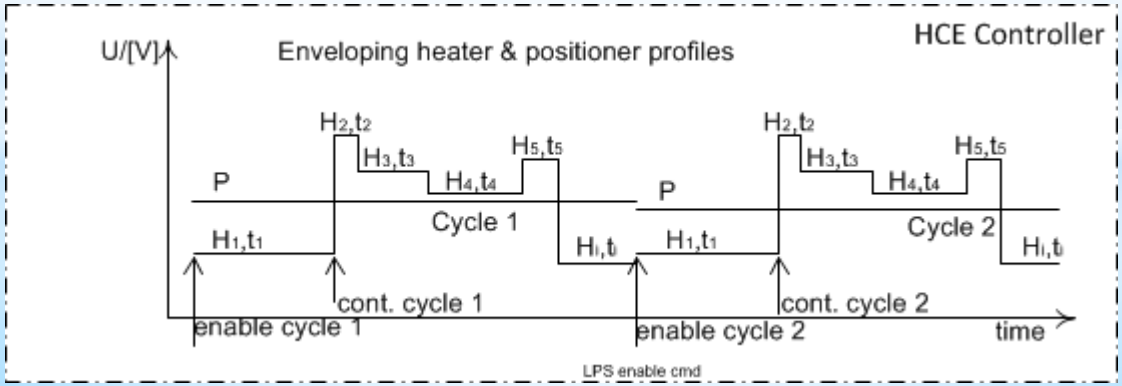
EML Toxic Sample Dust Hazard

- vapours from molten metals/metals at high temperatures
- amount depends significantly on
  - Sample temperature
  - Free metal surface
  - Processing atmosphere
  - Duration of sample at molten phase
- at pressure >1 mbar absolute - metal vapours can form fumes and dust particles
- potential ultra-fine and nano-size particles accumulation in cabin => toxicity hazard for crew

EML as Safety Instrumented System

Hazard controls

- Adequate Levels of Containment for sample processing
- Limitation of processing temperature and time to pre-evaluated limits
- Pre-evaluated limits low enough to prevent any toxicological impact, even in case of containment failure
- Failure tolerance for process parameter limitations by Functional Safety System (Hazard Control Electronics (HCE) in parallel to the EML process controller (ECE))



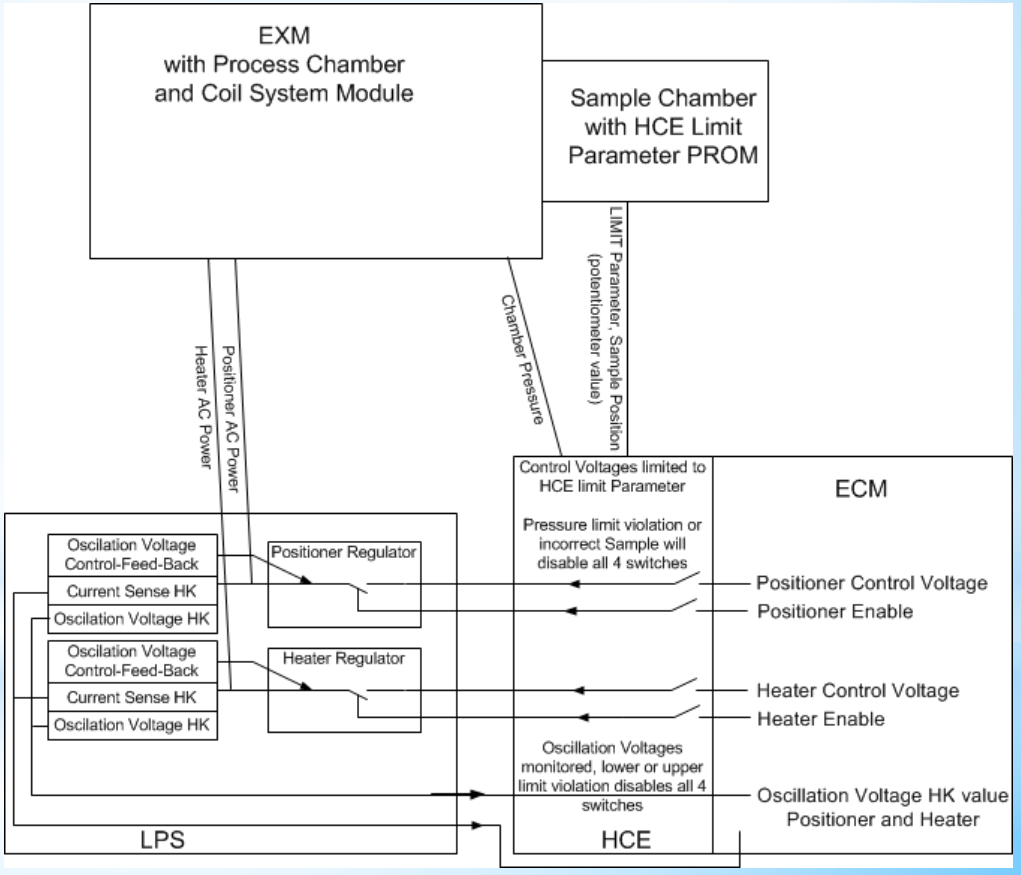
EML as Safety Instrumented System

EML HCE within EML System Architecture

HCE concept - default configuration fail safe - OFF

disabling of heater and positioner power supply towards the levitating coil => disabling any sample heating

- LPS heater power via independent inhibits
- nominal ECE signals hardwired through HCE logic
- concept ensures signals to LPS only forwarded when HCE is active and correctly working



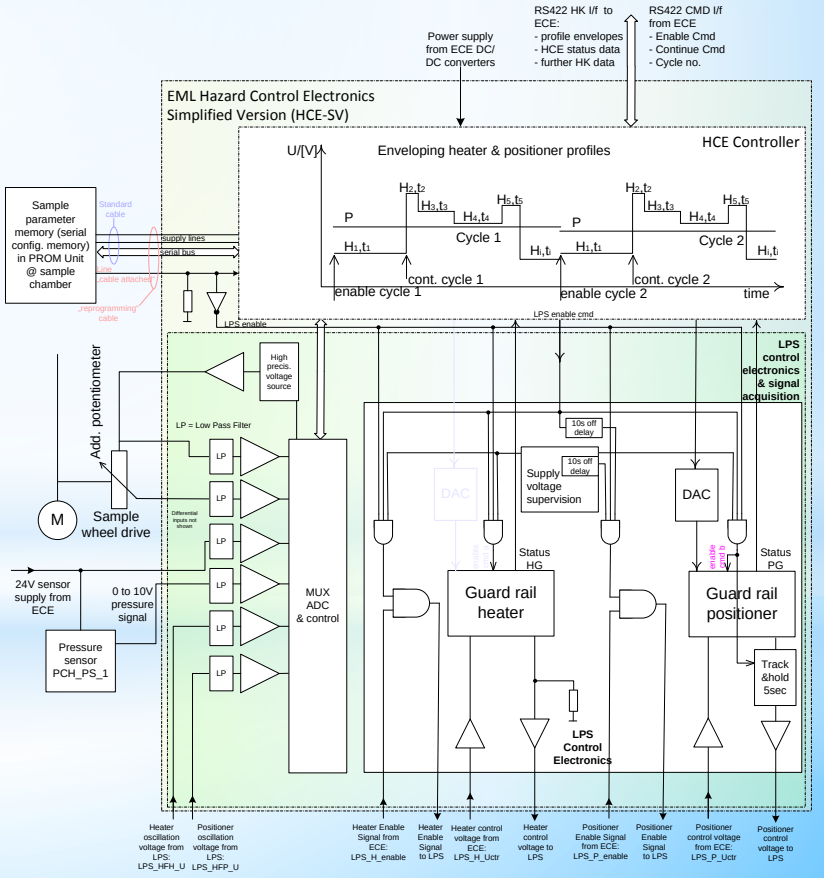
EML as Safety Instrumented System

EML HCE System Integrity as Safety-Related System

associated with similar requirements and techniques from IEC 61508

Measures against random hardware failures:

- components selection (MIL Std and SCC standard components)
- parts de-rating per ECSS-Q-30-11A
- HCE power supply monitoring
- signal monitoring, comparison to limit values and enabling of heating based on discrete electronics
- radiation tolerant hardcoded integrated circuits to store and process limit values



EML as Safety Instrumented System

EML HCE System Integrity as Safety-Related System
associated with similar requirements and techniques from IEC 61508

Measures to prevent systematic faults:

- structured design / development processes including FMECA, FPGA development per ECSS Standards
- product assurance involved in complete process cycle (design, MAIT) based on established and qualified processes (ECSS-Q-ST-70 series)
- defined process for experiment program and limit profiles development
  - large effort on ground testing of sample materials
  - parabolic flight campaigns to ensure correct prediction of limit profiles for heater voltage over time
- ground operations procedures for on-line monitoring/evaluation of sample processing per nominal process control conducted by ECE (ensure independent second level of processing control)
- limit profile parameters stored in dedicated memory, not write accessible while sample processing

EML as Safety Instrumented System

EML HCE seen from IEC 61508 or IEC 61511

HCE considered as Safety Instrumented System (SIS)

Safety Instrumented Function (SIF) is

- to protect from faults and failures in the Equipment Under Control (EUC) - EML main computer based system (ECE), that may lead to process deviation from the as-planned program.

Hazard associated with process deviation is production of excessive amount of metal fumes and dust

- Hazard only in case of sample heating beyond predefined limits

⇒ "fail safe" design of HCE, disabling heater activation signal from ECE to LPS, comparable to Low Demand Mode from IEC 61508 prospective

Use of SIL capable COTS in ISS payloads

SIL capable items:

- hardware or SW items (components or sub-systems, e.g. PLCs or CPU boards, communication buses, I/O modules) certified to be able to perform safety function at certain SIL (according to IEC 61508 or other industry specific functional safety standard)

Potential benefits using COTS items certified to SIL requirements:

- Investment in functional safety design, development and assessment done by an item provider (assessment and certification may be even by third parties).
- reduction of Payload Organisation effort for computer based system compliant to ISS payload safety requirements
- Items produced applying certain quality control (as required for SIL certification) => reduced product assurance effort for PO

Use of SIL capable COTS in ISS payloads (cont.)

Expected limitations when using COTS items

- early selection of software and network standards, based on SIL qualified products
  - for ISS MIL-1553B network selected for safety relevant data interfaces, but not implemented in all payloads or e.g. on-board laptops and laptop interfacing components
- fast development cycles of commercial operating systems and hardware platforms => re-use difficult because of long development and utilization cycles
- adaptation of payload system design to certified COTS

  =>high overhead for individual payload
  - only standardisation and overhead distribution over several payloads could lead to a positive turn-over compared to the COTS development cycles for series or mass-production