HSE

Occupational Health & Safety
and Environmental Protection unit

Development of Radiation Protection Monitors and Technologies for Safety-Critical Applications

Examples of application of Formal Methods Verification at CERN

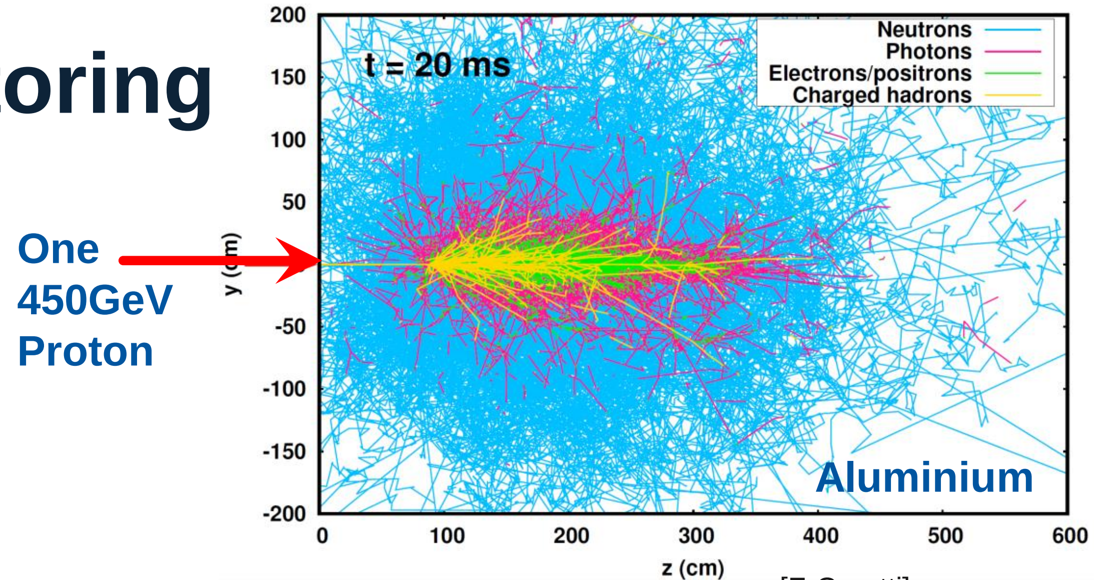
Hamza BOUKABACHE on behalf of HSE-RP

04/07/2024

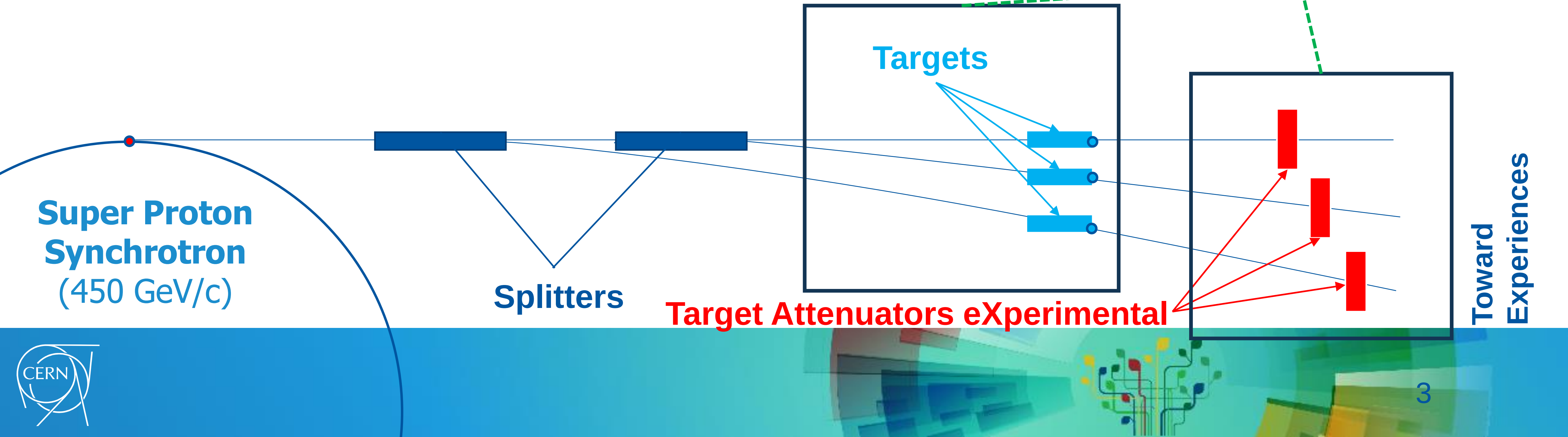
Why do we need a radiation monitoring

When Accelerators are in operation

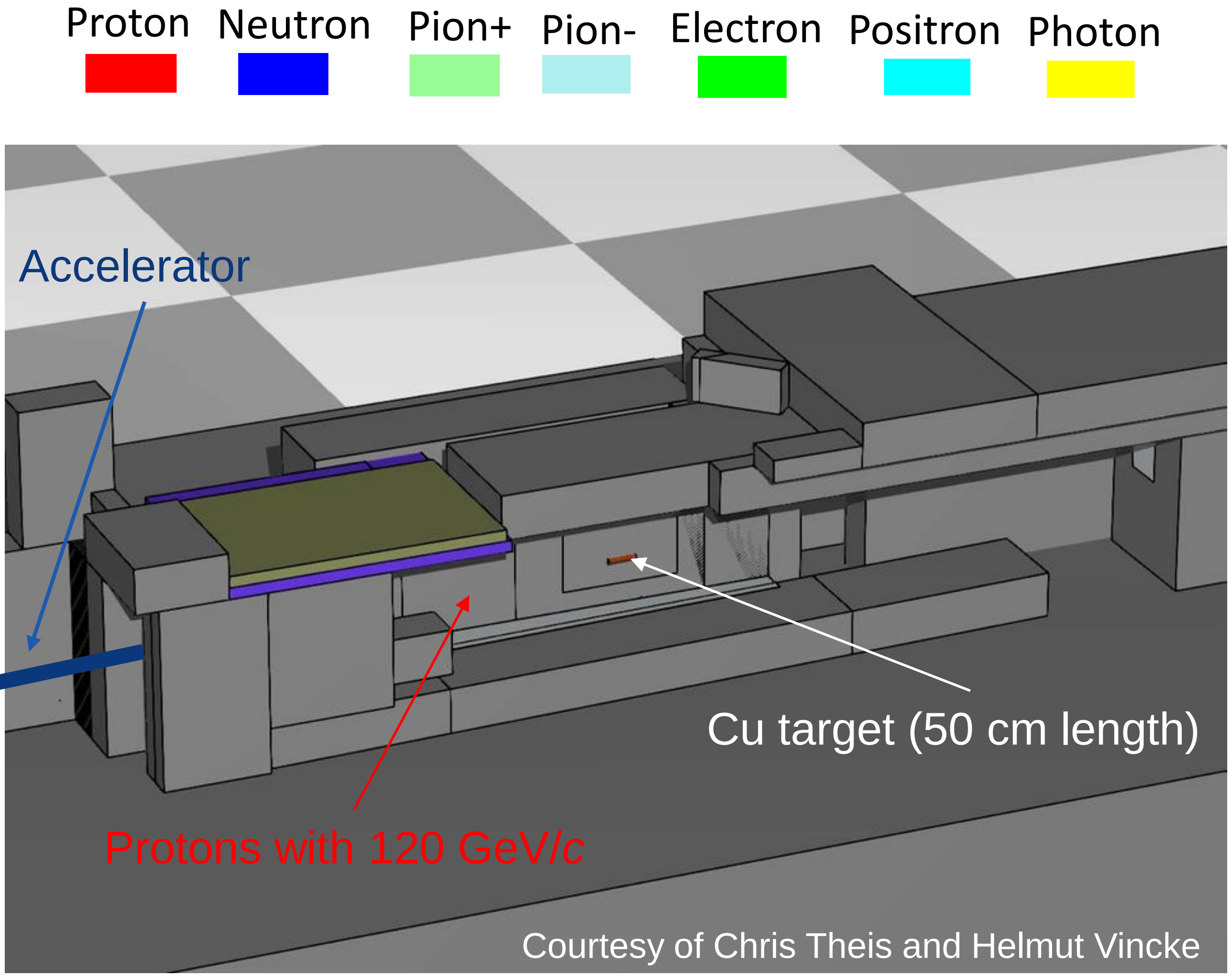
The interaction beam-matter generates stray radiation



[F-Cerutti]



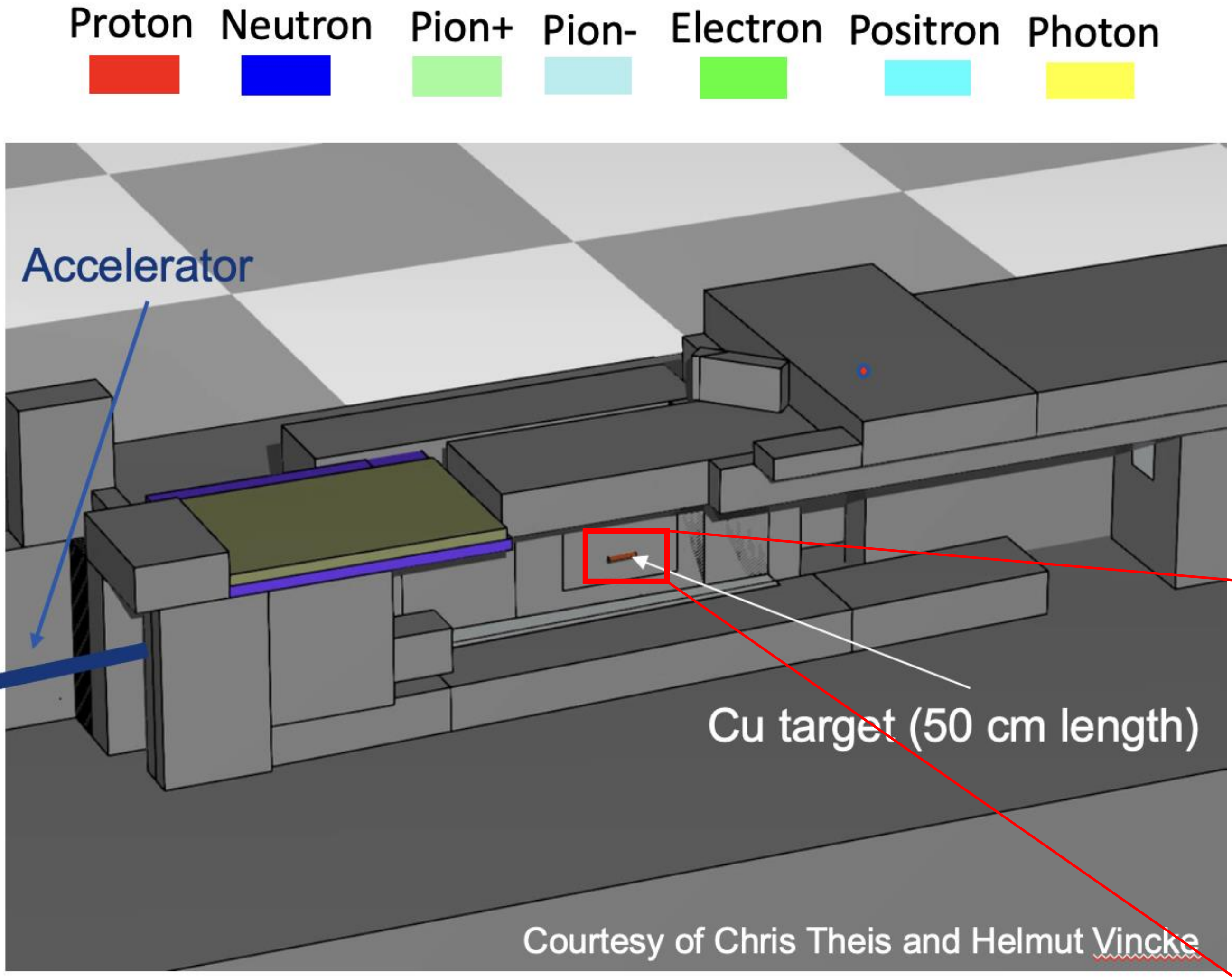
Why do we need a radiation monitoring



When Accelerators are in operation

→ The access to the beam tunnel and experimental areas is closed

Why do we need a radiation monitoring

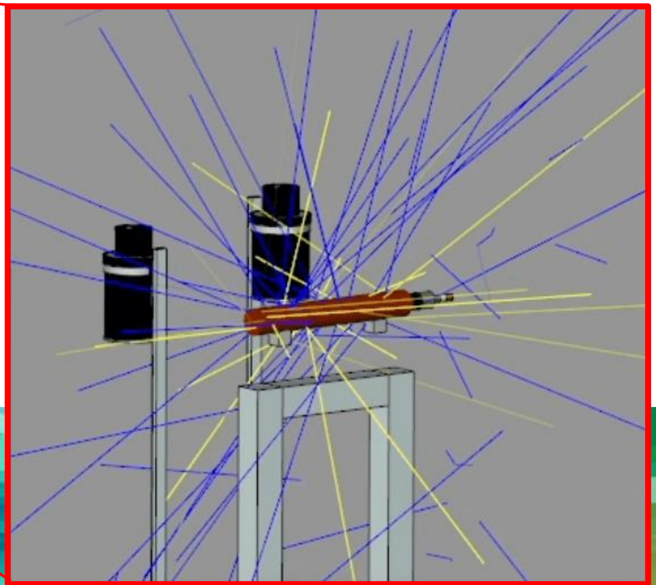


When Accelerators are in operation :

→ The access to the beam tunnel and experimental areas is closed

When Accelerators are stopped :

The target became radioactive (activation)

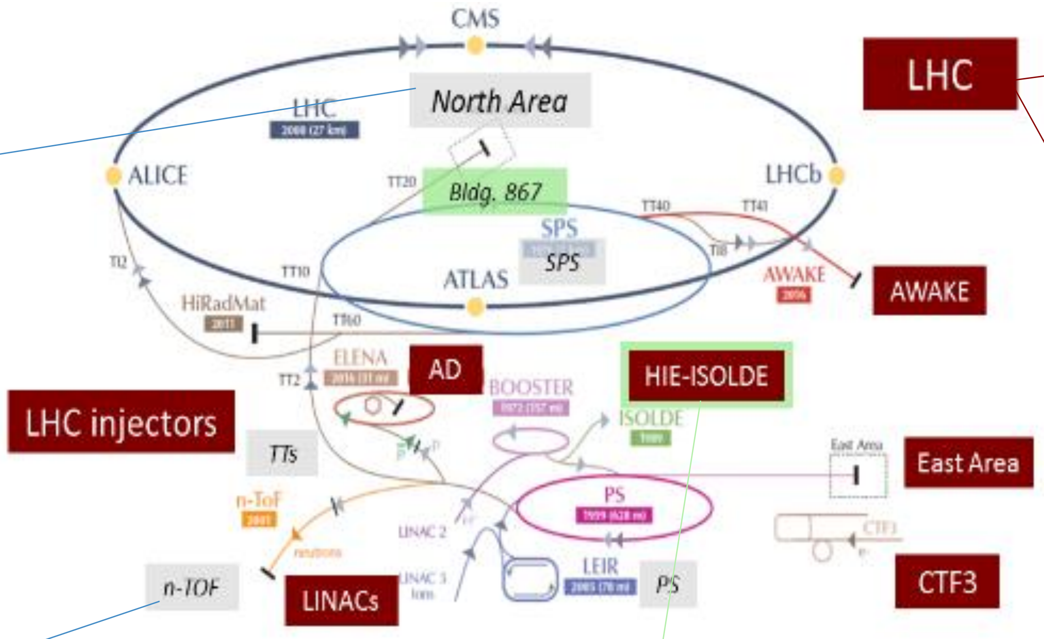


Radiation & Environmental Protection Before LS2

864 Radiation Protection channels & **523** Environmental channels

ARCON VME Chassis

Area Monitoring (ARCON)



GRAMS

RAMSES

Area Radiation Monitoring

Induced Activity Monitors

Water Monitors

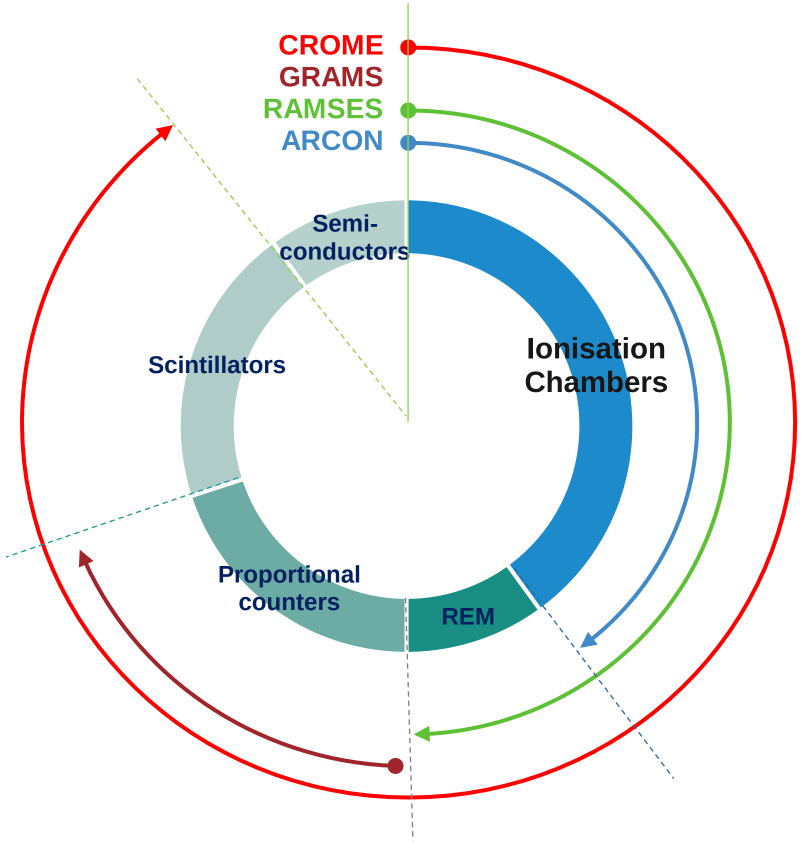
Stray Rad Monitors

Ventilation Monitors

CROME Requirement - 2015

- **Development of a new generation of monitoring system**

  This system provides:
  - Continuous real-time monitoring of ambient dose equivalent rates over **9 decades**
  - Alarm and interlock functionality with a probability of failure down to **10e-7**
  - Long term permanent and reliable **data logging** by linking to a SCADA supervision
  - **Edge computing** : Powerful processing capabilities for embedded calculation
  - **Versatile** interface

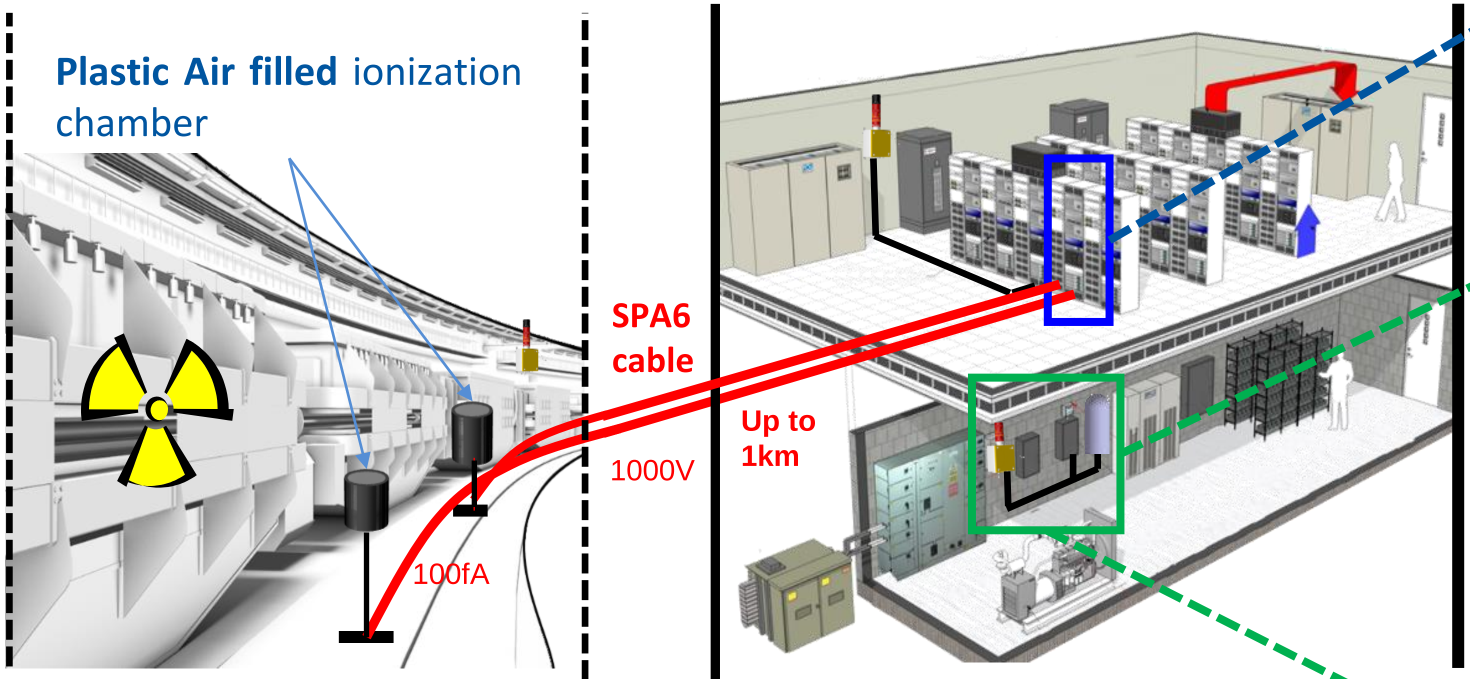


- **Replacing ARCON system**
- **Preparing for future, RAMSES** : 14 years of operation

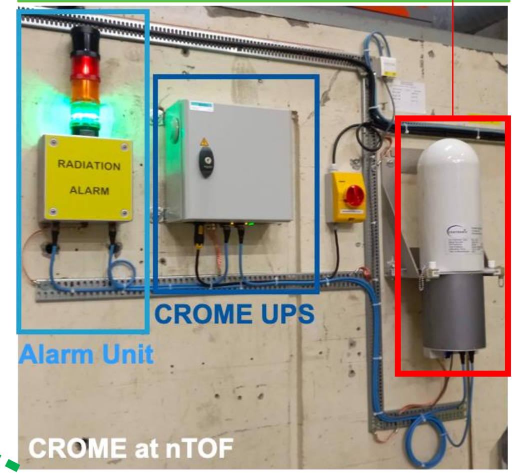
CERN Radiation Monitoring Electronics (CROME)

Two configurations:

Conceptual view of CROME at CERN



Bulk



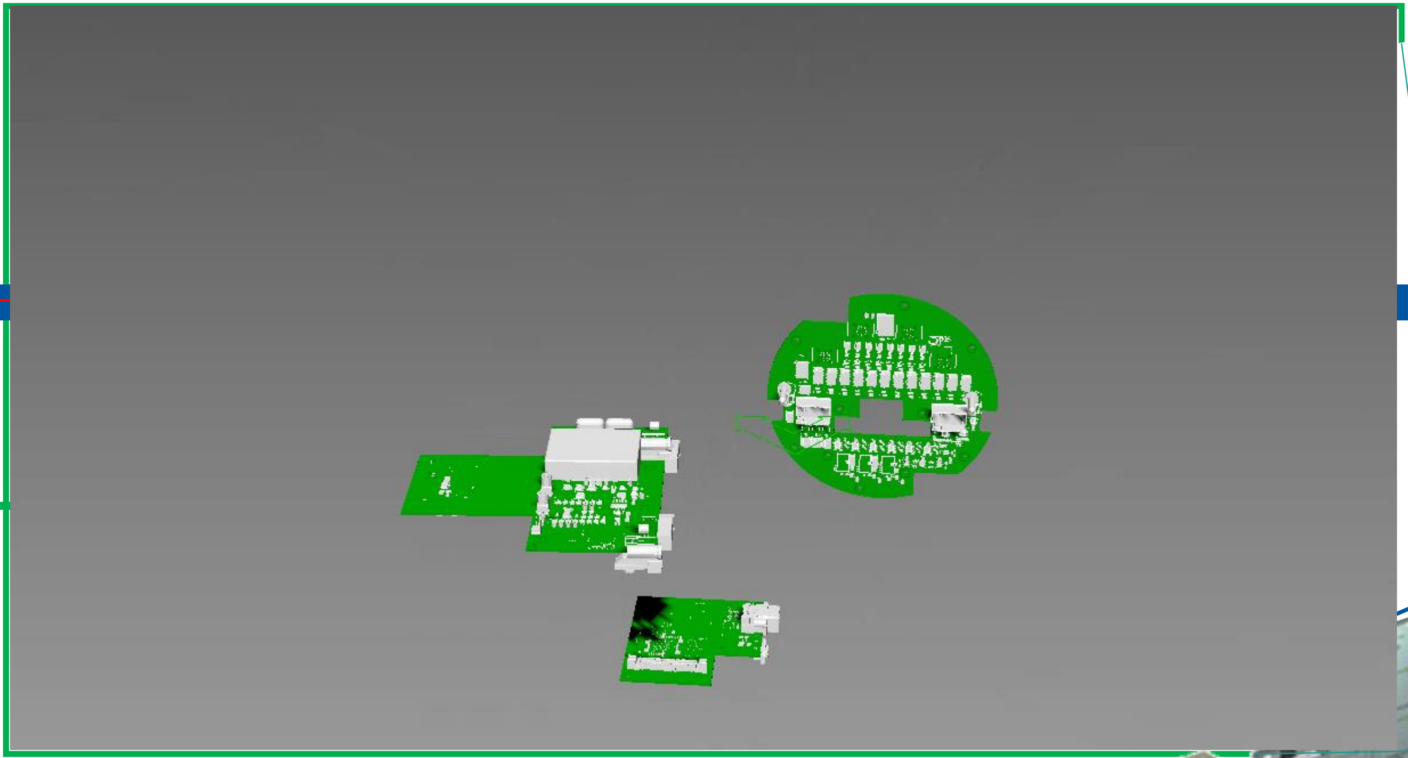
Rackable

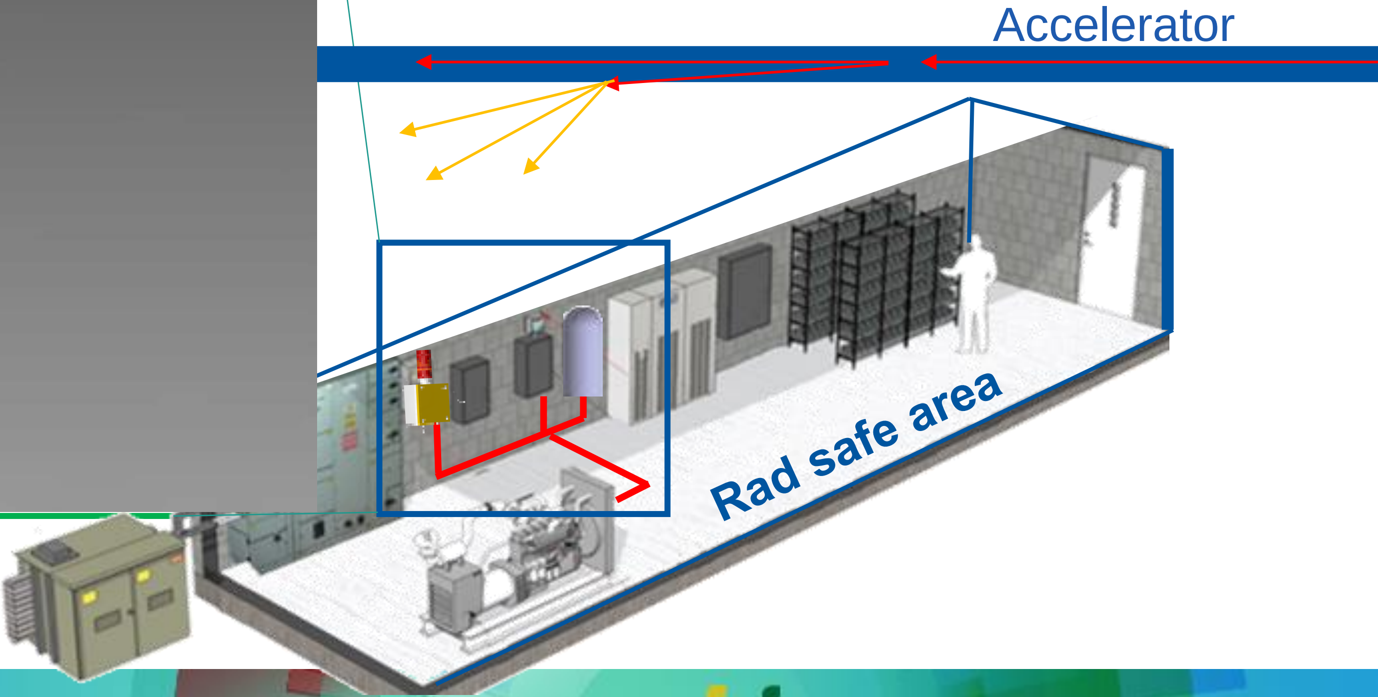
Radiation Monitoring and processing units

Uninterruptible Power Supply
Includes a battery for continuous operation

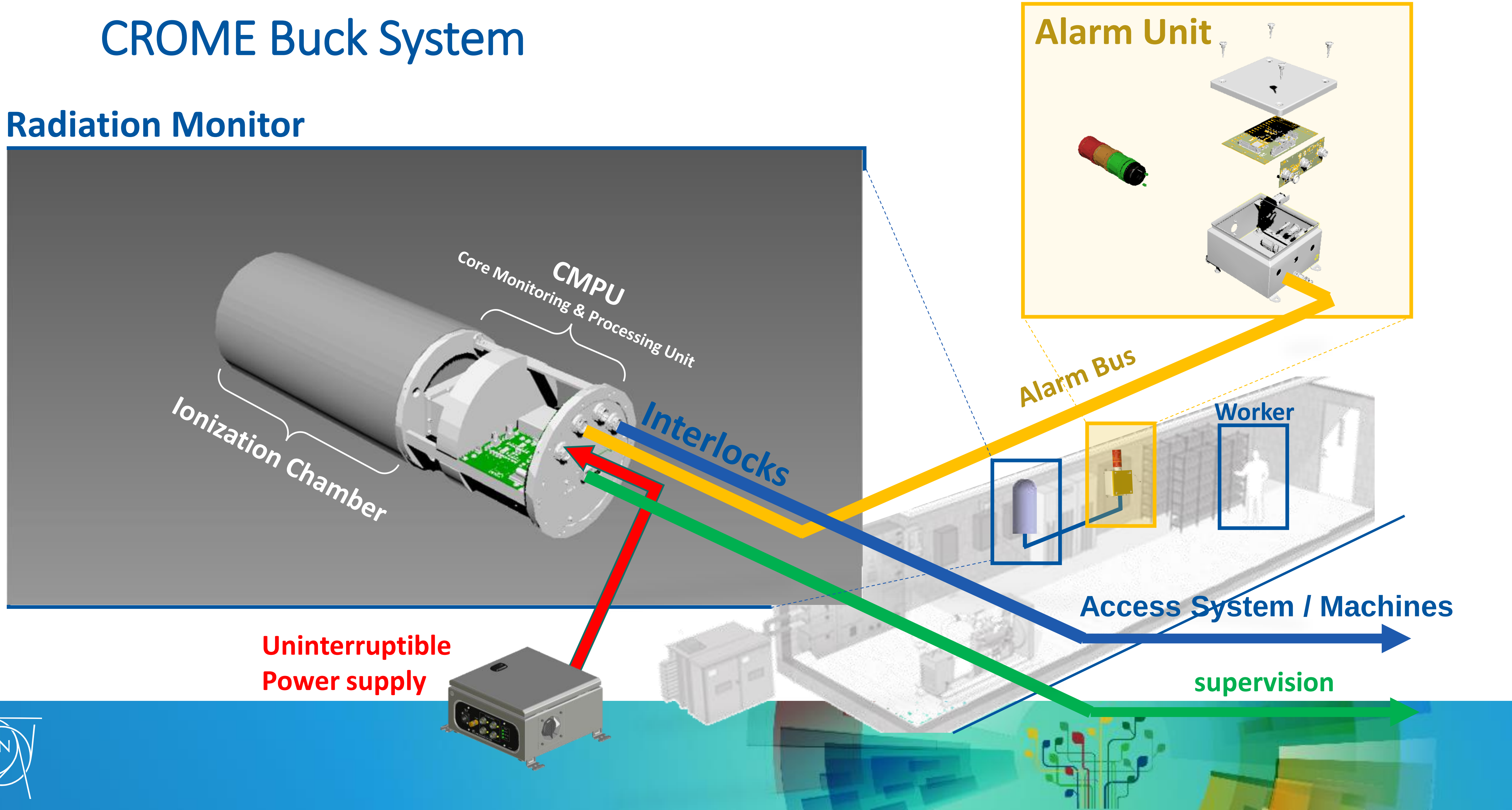
CROME Buck System

Radiation Monitor



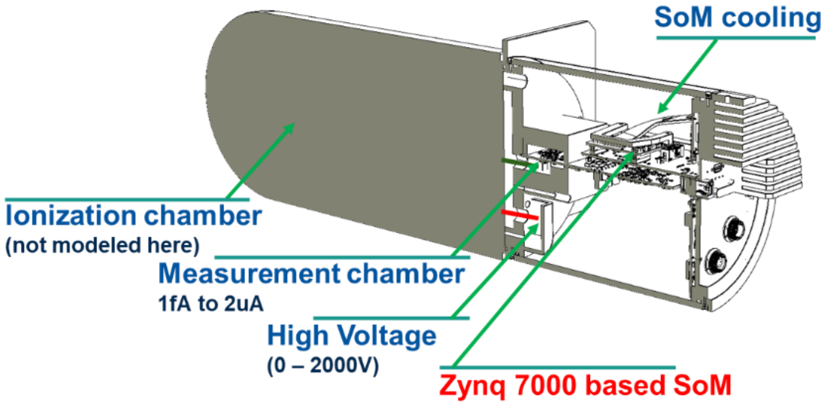


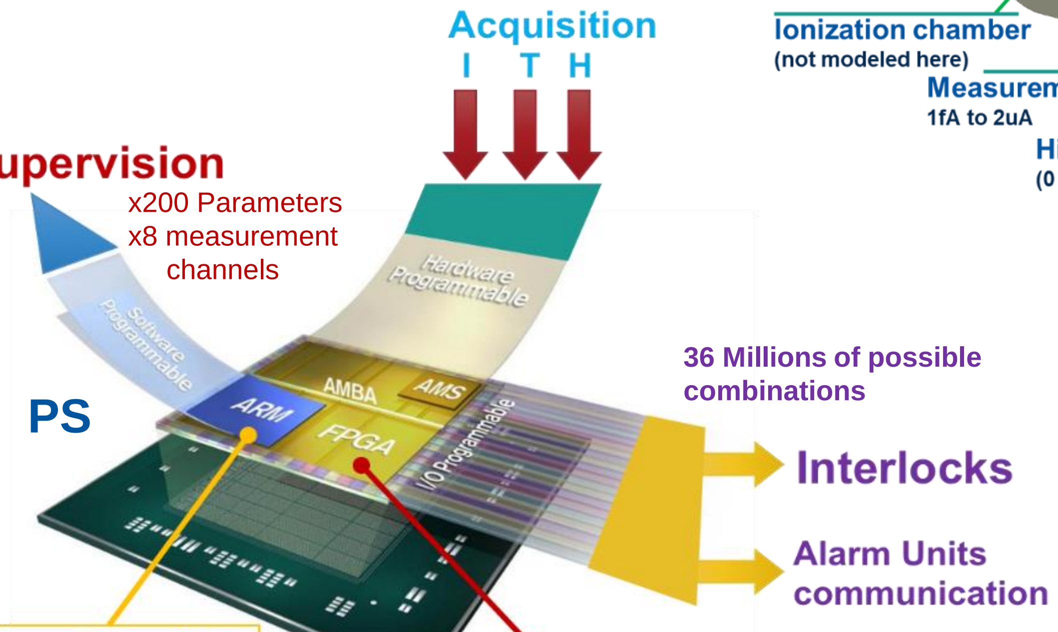
CROME Buck System

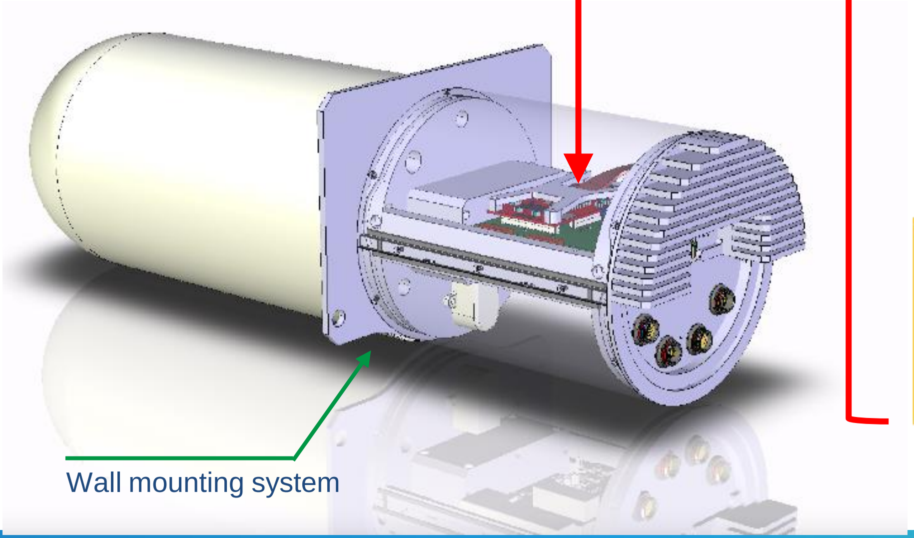


CERN Radiation Monitoring Electronics (CROME)

Highly Integrated Solution :







Linux Operating System :

- Data storage and management
- Supervision
- …

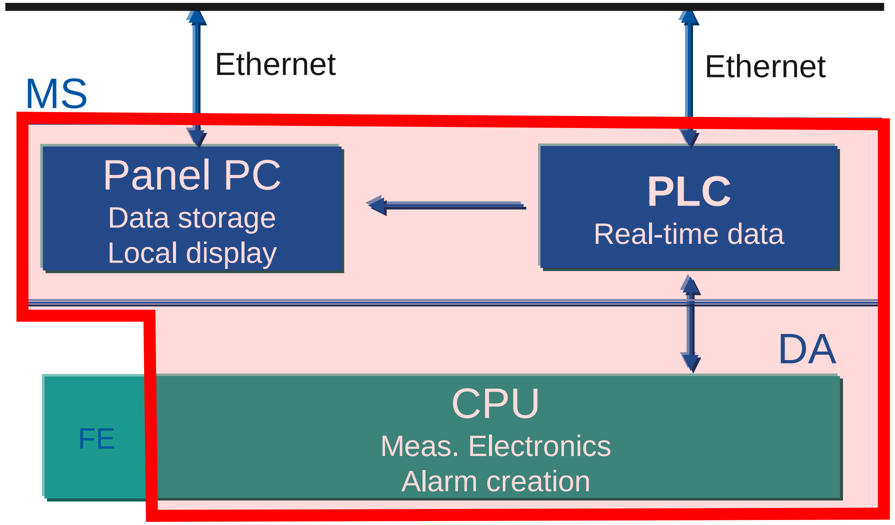
Safety Critical part :

- Measurement algorithms
- Real Time temperature compensation
- Dose rate calculations
- Cumulated dose calculation
- Interlock generation
- …

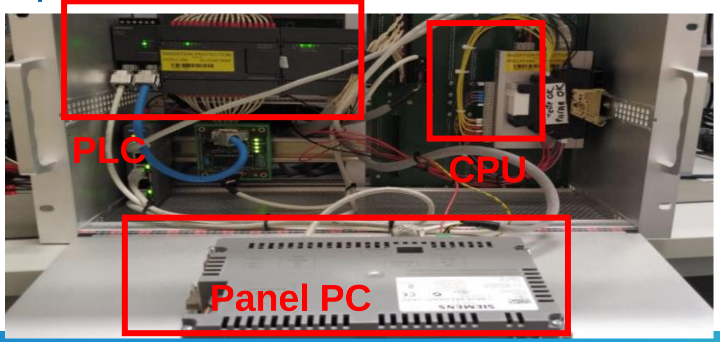
PL

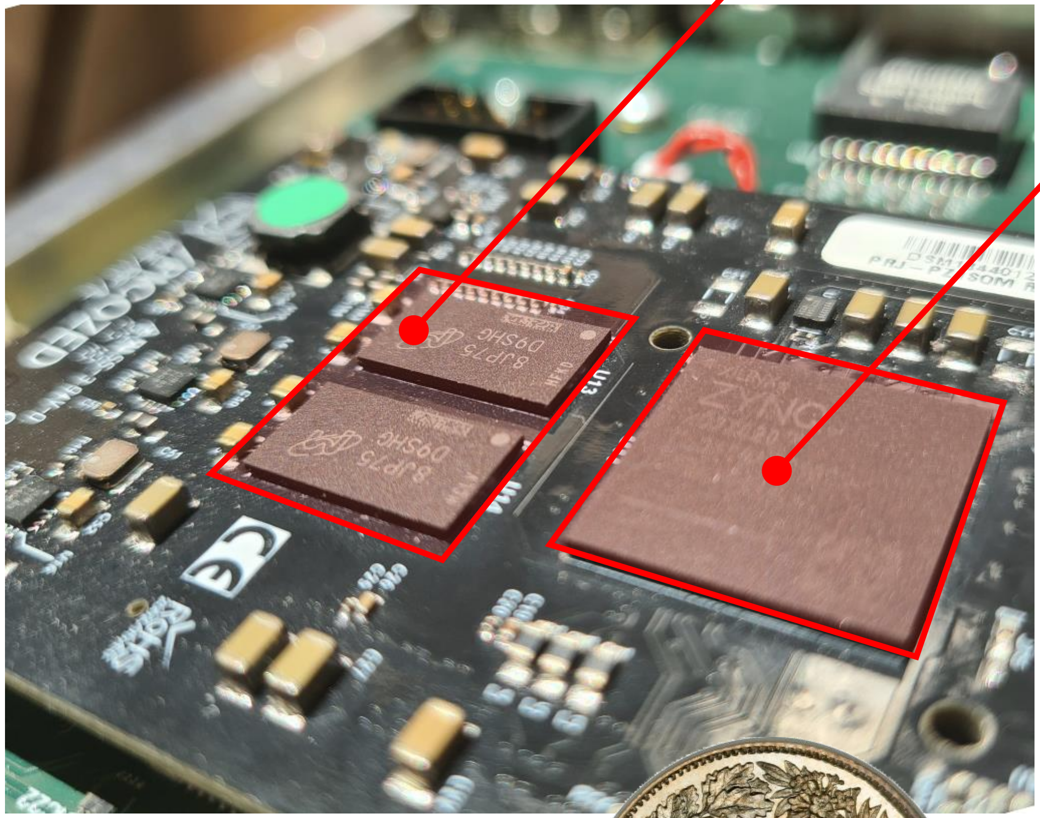
CERN Radiation Monitoring Electronics (CROME)

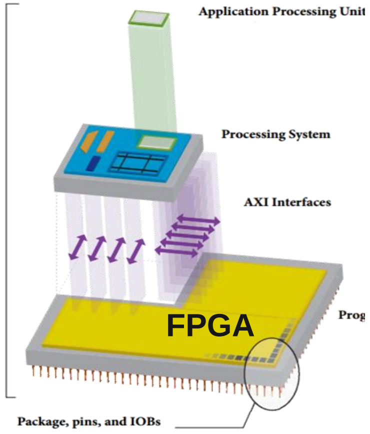
RAMSES System (Outsourced 2004)



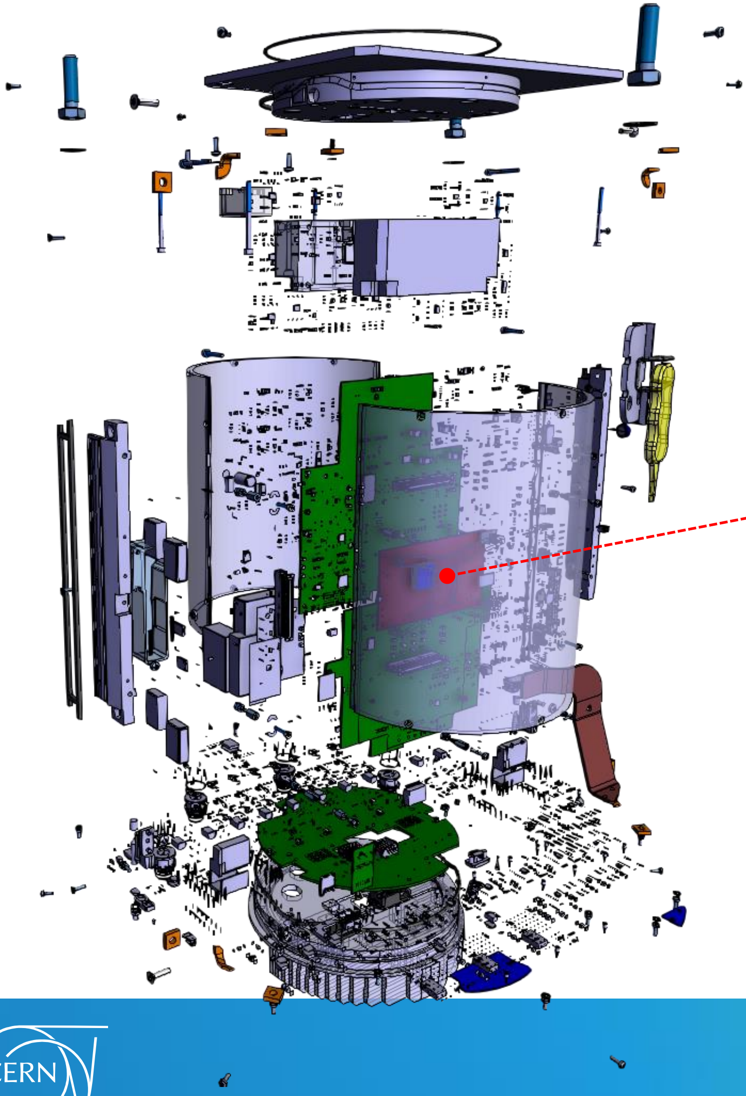
Example of the MS Rack

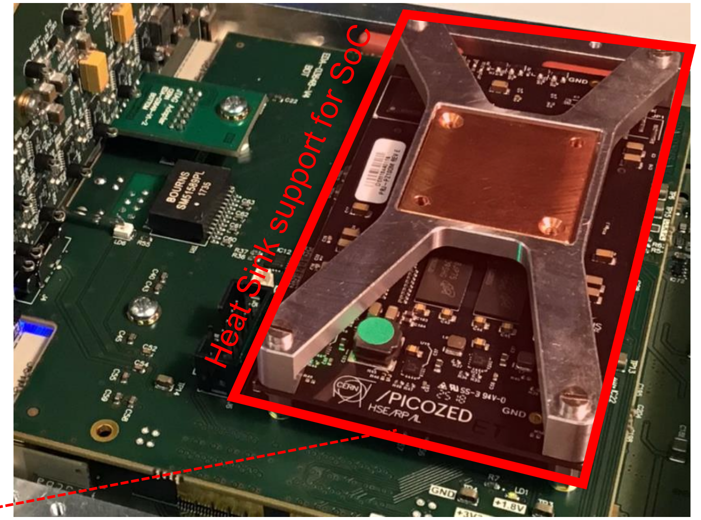






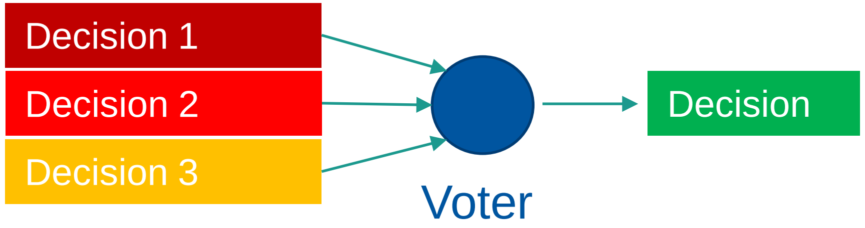
CERN Radiation Monitoring Electronics (CROME)



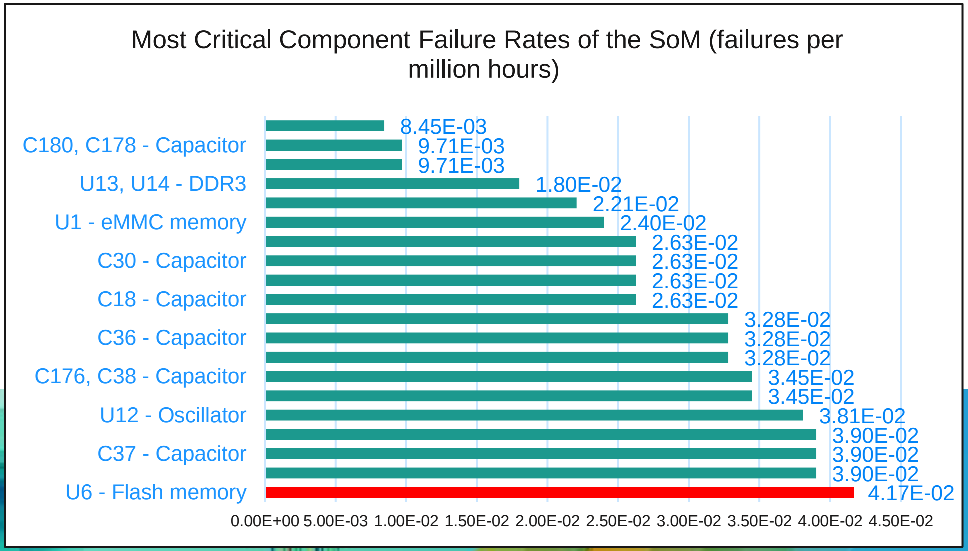


Critical decisions are taken into the FPGA section of the SoC (38 billion of possible combinations)

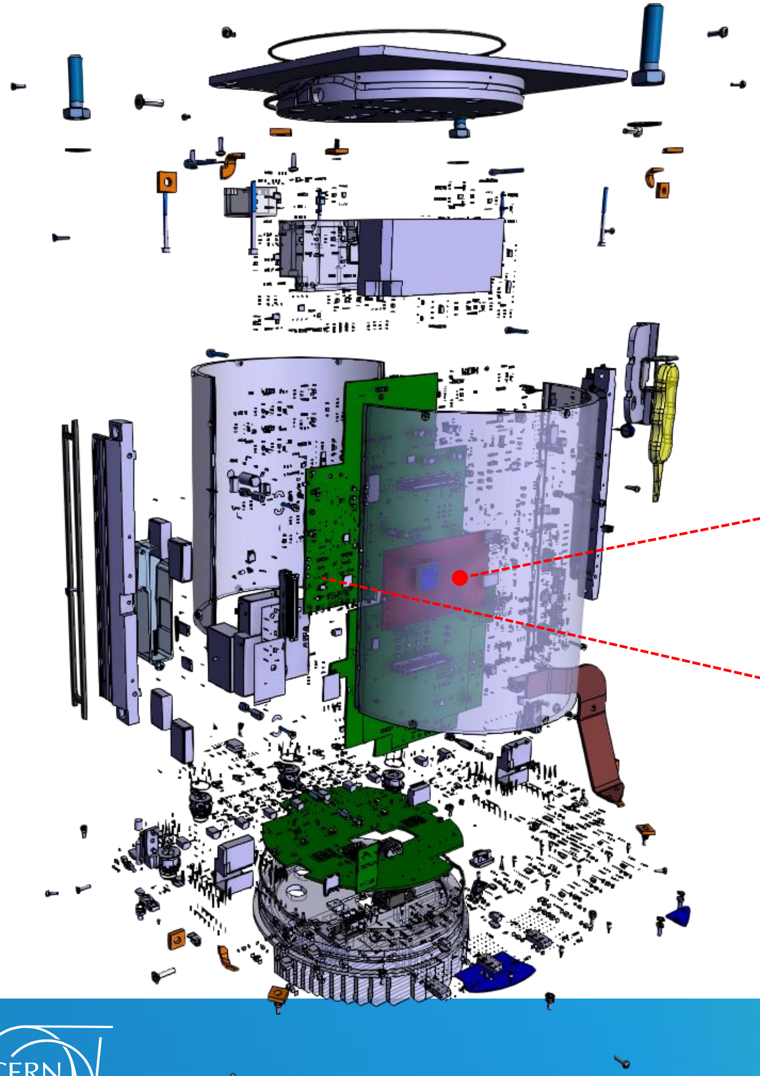
- ✓ SIL2 compatible floating point calculation engine
- ✓ Developed a safe architecture (memories are protected, data is exchanged and checked with checksums)
- ✓ Direct democracy with a global triplication :

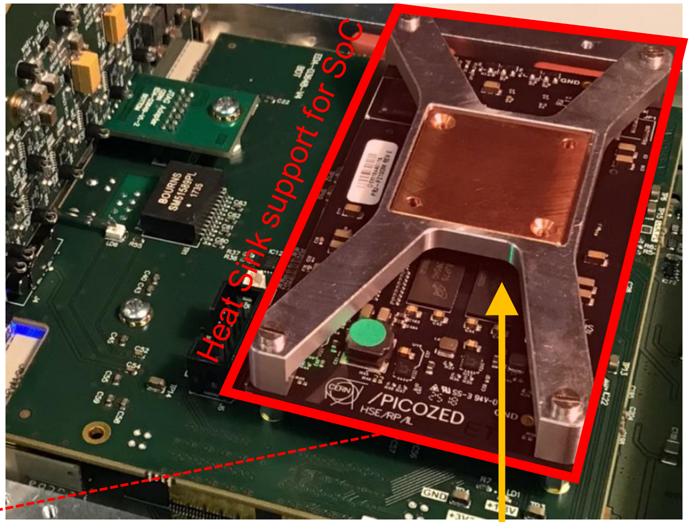


- **All the components have been individually analyzed** (> 3000 references)
- **Critical components have been replaced**
- **Redundancies**
- **Testability**

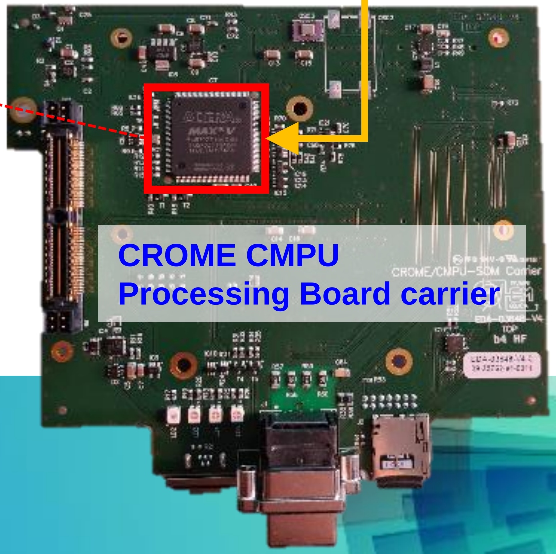


CERN Radiation Monitoring Electronics (CROME)



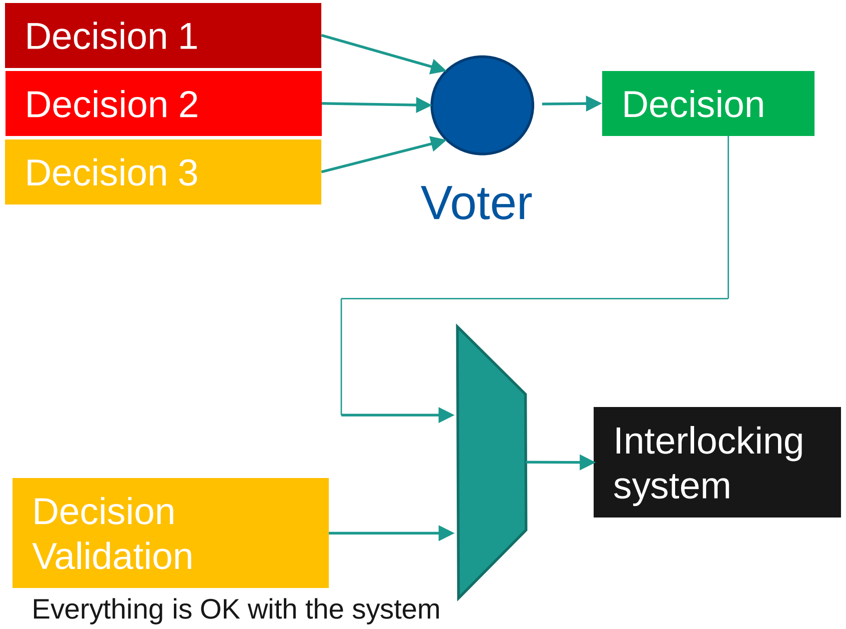


Extended testability
97% of dangerous failures



Critical decisions are taken into the FPGA section of the SoC (38 billion of possible combinations)

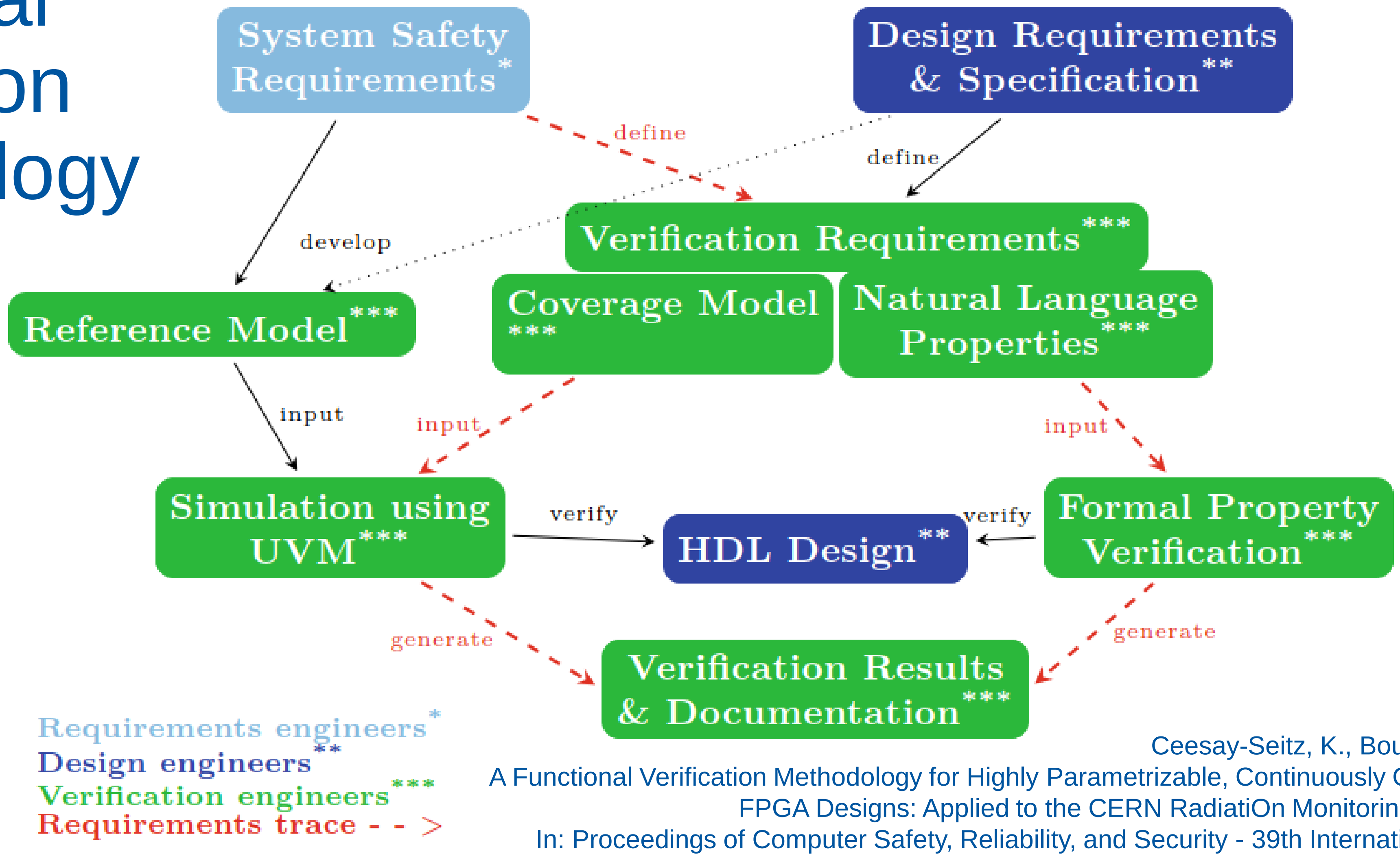
- ✓ SIL2 compatible floating point calculation engine
- ✓ Developed a safe architecture (memories are protected, data is exchanged and checked with checksums)
- ✓ Direct democracy with a global triplication :



Probability of dangerous failure per hour:

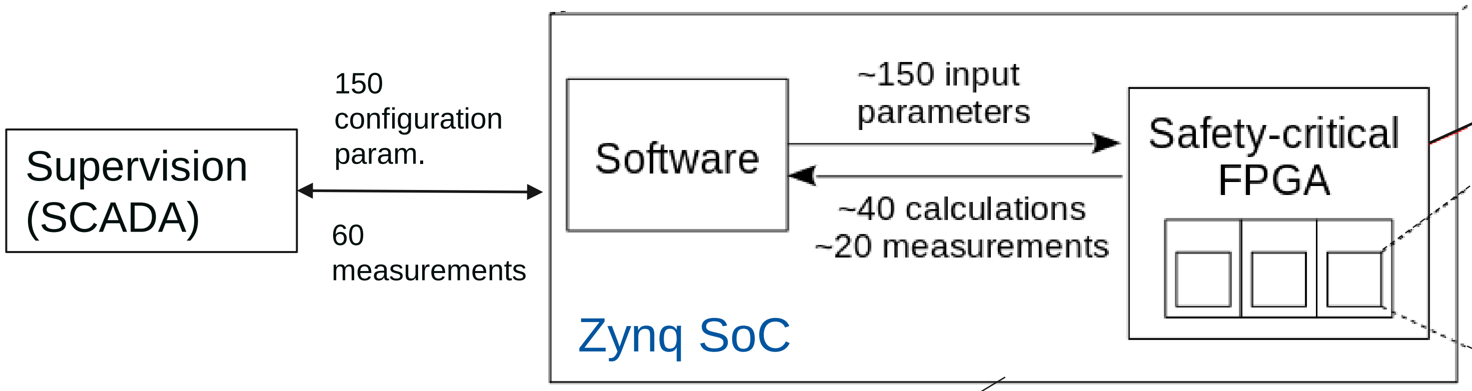
$$PFH = 9.28 \cdot 10^{-08}\ [fpmh]$$

Functional Verification Methodology



Ceesay-Seitz, K., Boukabache, H., Perrin, D.:
A Functional Verification Methodology for Highly Parametrizable, Continuously Operating Safety-Critical FPGA Designs: Applied to the CERN RadiatiOn Monitoring Electronics (CROME).
In: Proceedings of Computer Safety, Reliability, and Security - 39th International Conference (2020)

Verification Example



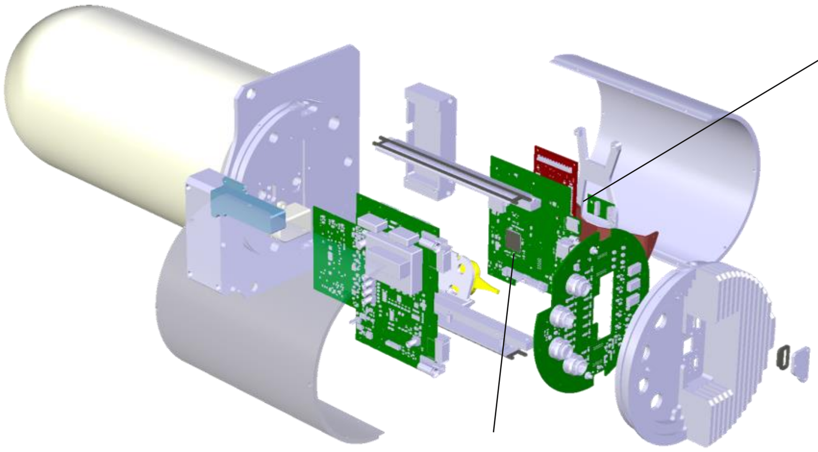
Alarm Units / Interlocking system

Alarm/Interlock Matrix:

Huge configurable logical formula
451 input bits (= 2^{451} configuration options)

Drives safety-critical outputs

sequential depth: 4 clock cycles



With a Reference model in SystemVerilog

(Only constraint: parameters do not change during 4 cycles of formula evaluation)

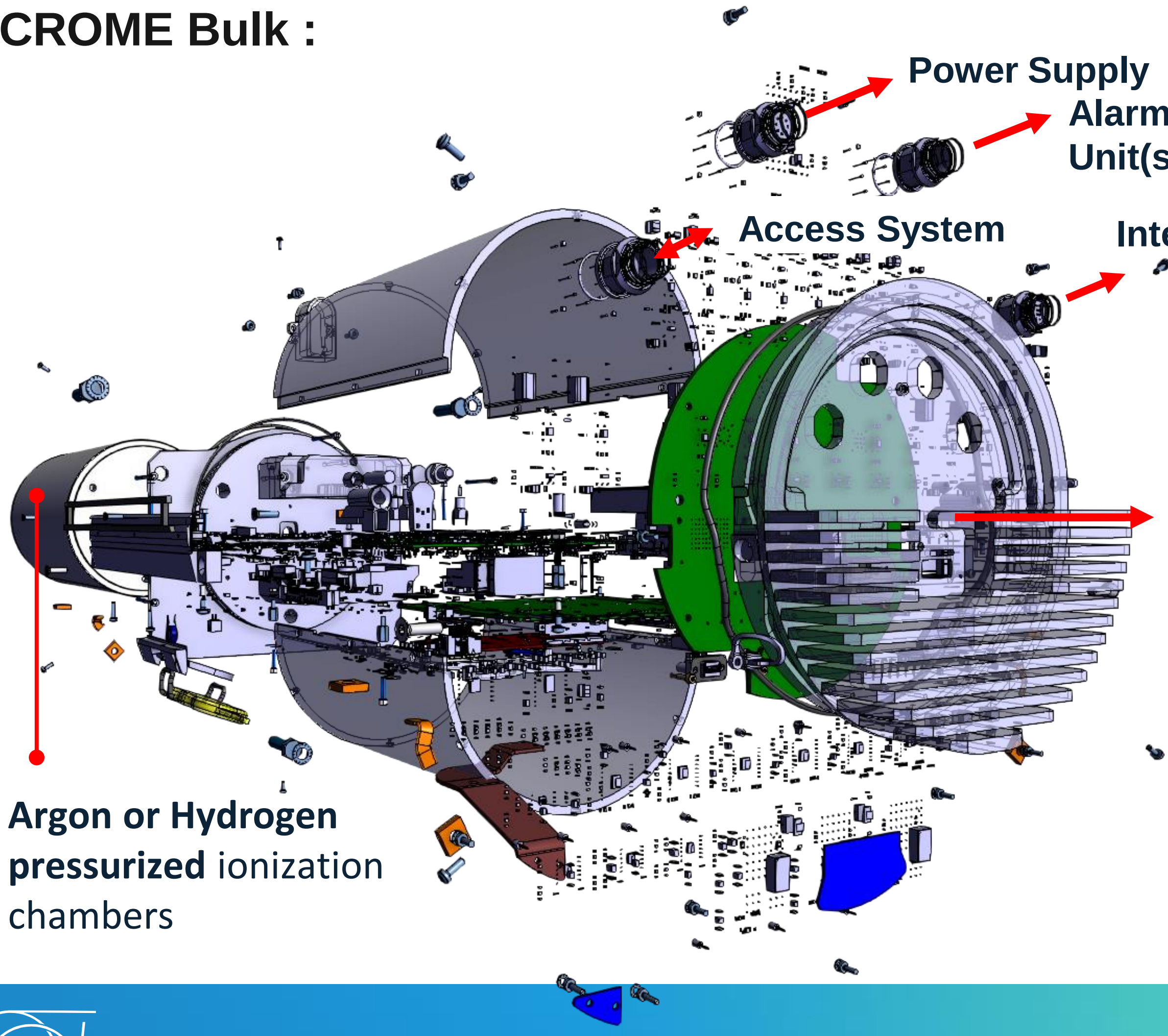
→ **46 properties proven in 33 seconds** (estimated simulation time: **$8*10^{137}$ years**)

Fault: In one particular configuration **radiation dose alert** was not triggered due to a wrong VHDL vector range

Outputs were **not** consistently **in safe state** when invalid inputs were applied (inputs are anyway checked at software level)

CERN Radiation Monitoring Electronics (CROME)

CROME Bulk :



Exhaustively proven <u>radiation dose **alarm generation</u>**

Findings in integration/calculation algorithm :

Undocumented design decision

→ **Fault** in rounding mechanism only if internal result was negative

→ **Scenario not covered by simulation** (400000 stimuli applied)

Fault that would happen **after 7 years of continuous operation**

→ Found after 1 second with formal

→ Would require > 7 years of simulation

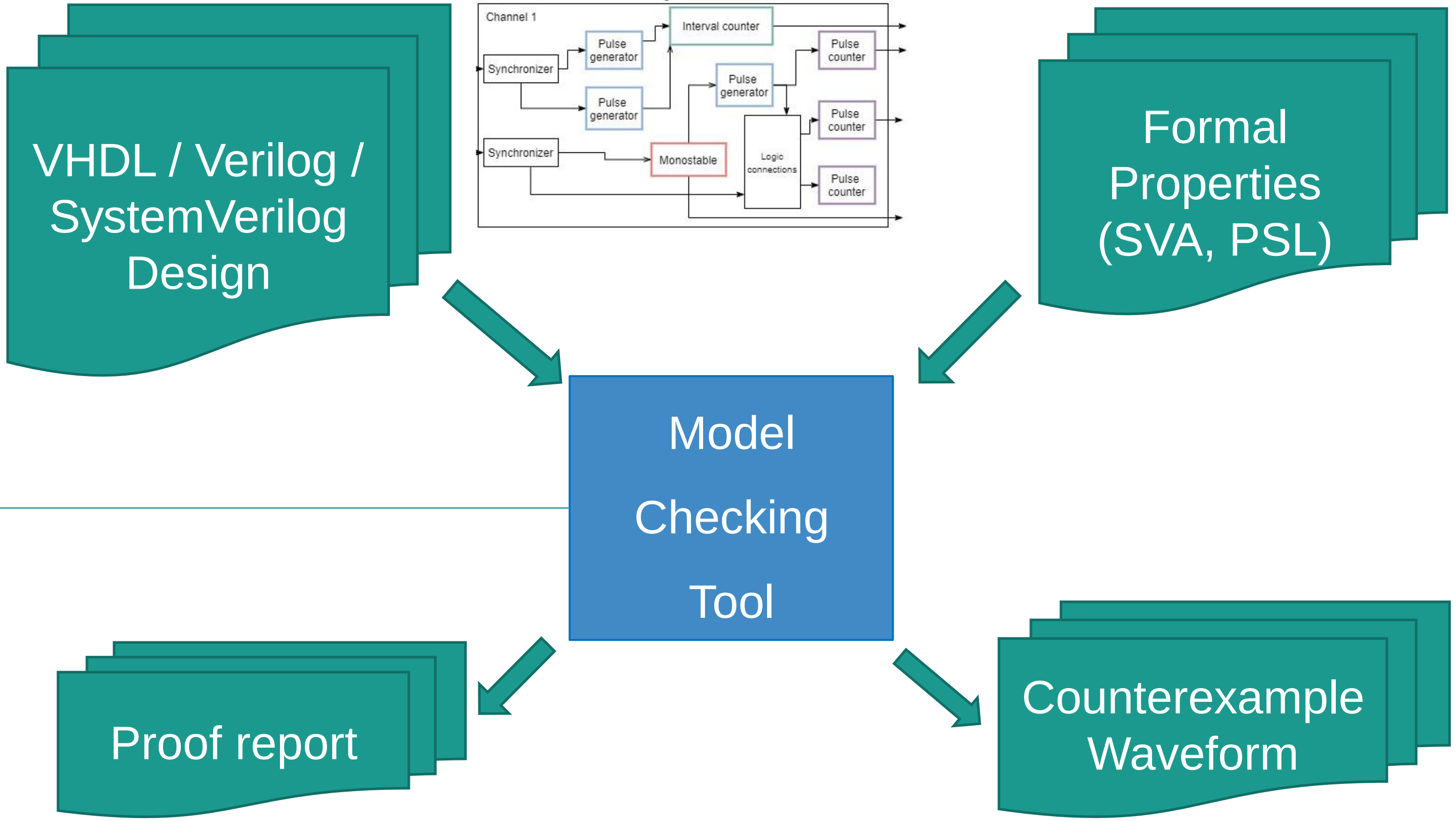
Formal Property Verification – Model Checking

Commercial tools:

- Cadence Jasper Gold
- **Siemens Questa Formal**
- Synopsis VC Formal
- …

Open-source tools:

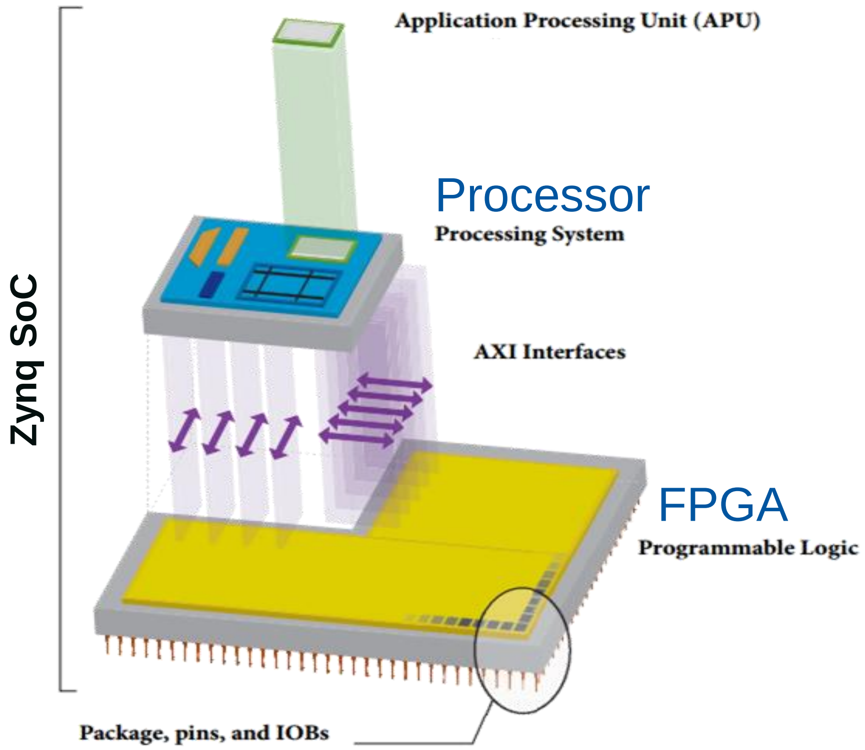
- SymbiYosys,
- EBMC, …

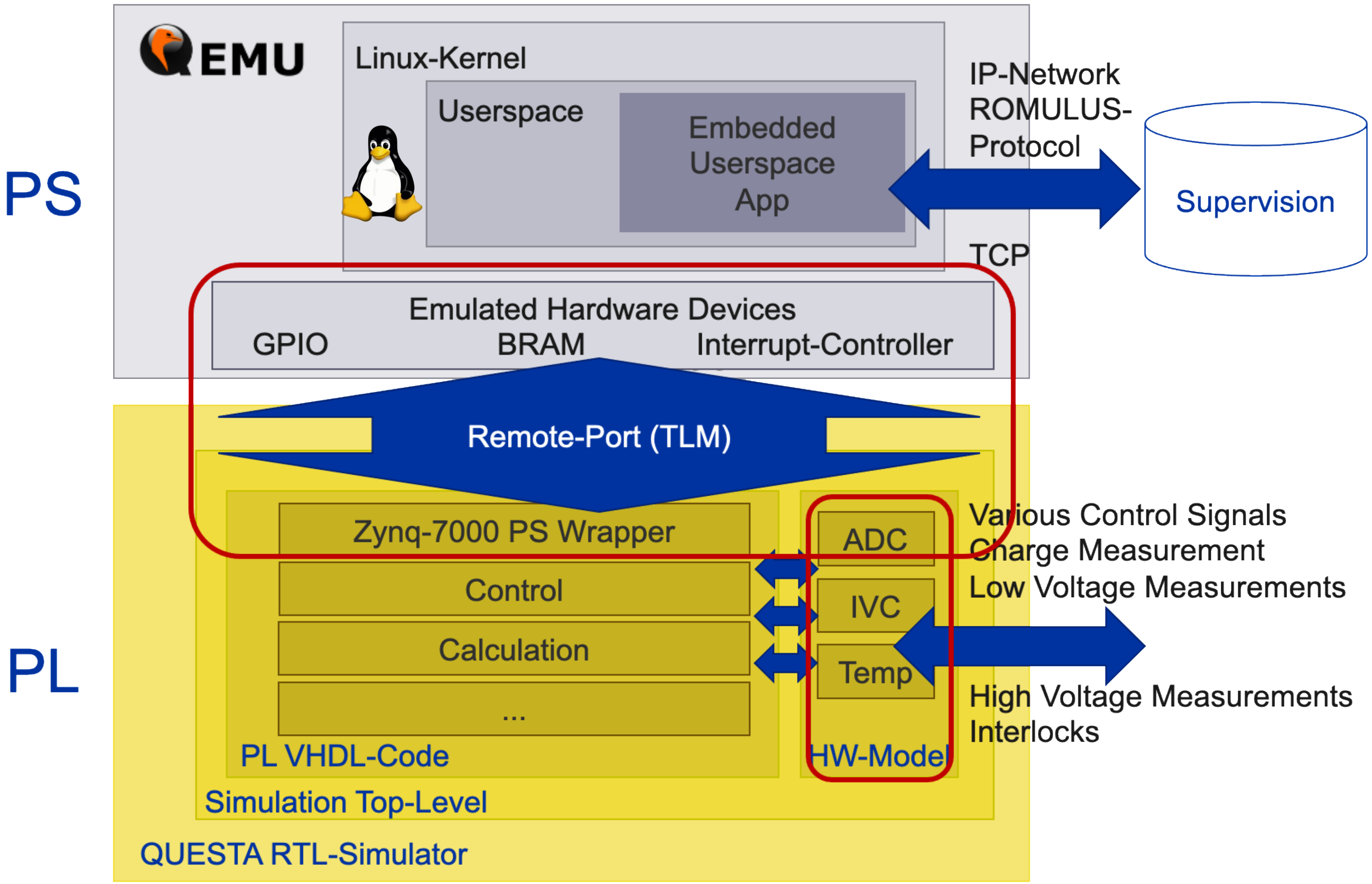



```
property pIntAlarmOn();
  (((mtValidxDI == 1) && $rose(intStartxDI))
   ##`nrCUntilCalcRdy
   ((alarmActivexDI == 1) &&
      (signed'(integralxDO) >= signed'(thresholdxDI))))
    |-> sIntAlarmOn();
endproperty

sequence sIntAlarmOn();
  ##`nrCyclesAlarmRdy (ALARMxDO == 1);
endsequence

assert property (pIntAlarmOn);
```

…routedBindSVA.asAtopCtrGateCntRestAfterGateLenVHDL	10	1s
…te2_top_routedBindSVA.asAtopGateLenSigRouted100ms	7	1s
Accurate2_top_routedBindSVA.asAtopCtrGateCntEq	10	2h 30m 9s
Accurate2_top_routedBindSVA.asAtopCtrGateEndEq	10	2h 31m 37s
Accurate2_top_routedBindSVA.aAtopCtrWeHighLength	10	1s
Accurate2_top_routedBindSVA.aAtopCtrWeHighTime	7	1s
…ChkCtrlNoUnexpectedRst.aNoUnexpectedCntRstSymbolic	7	12s

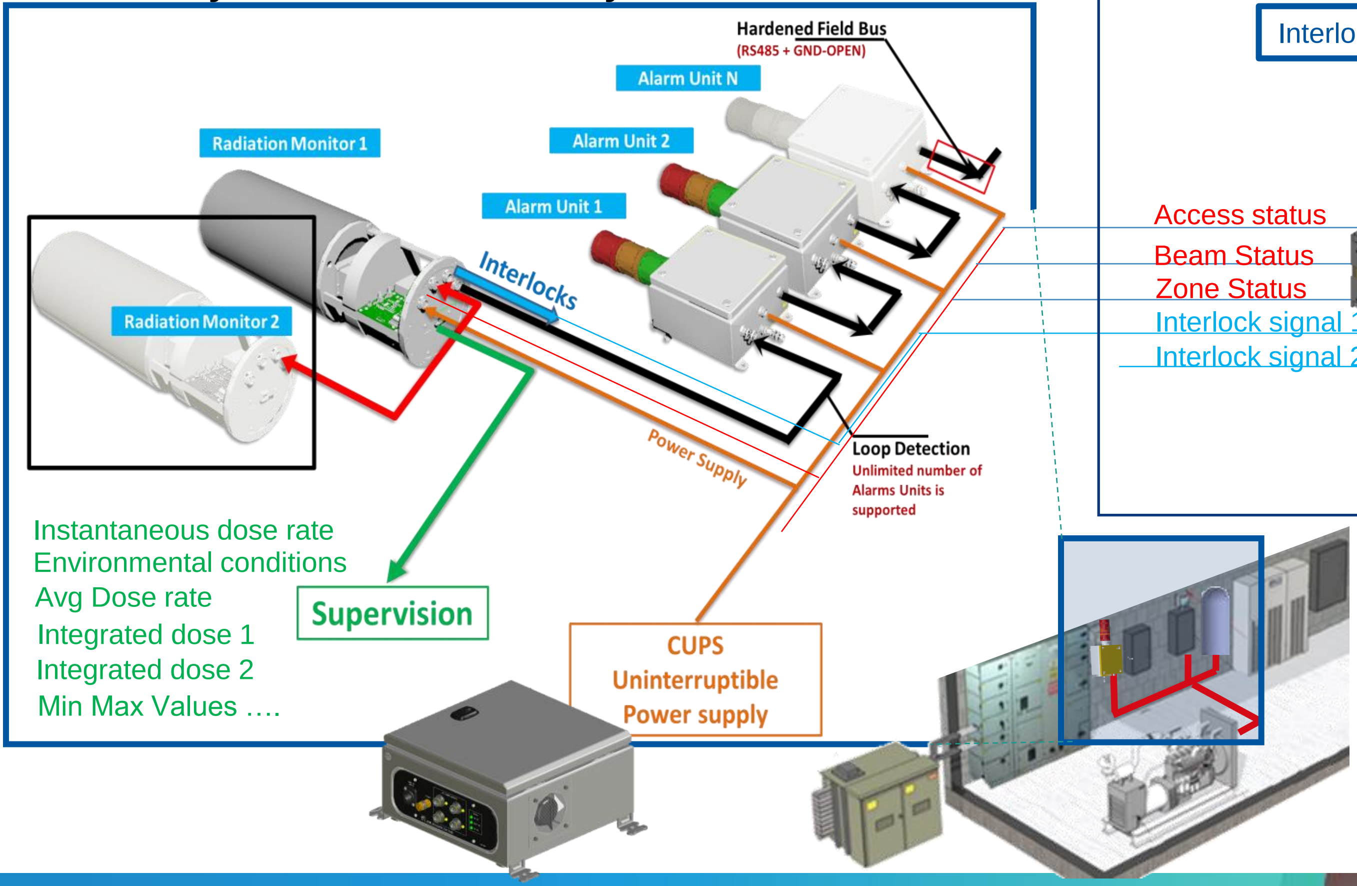
Our Co-Simulation Environment



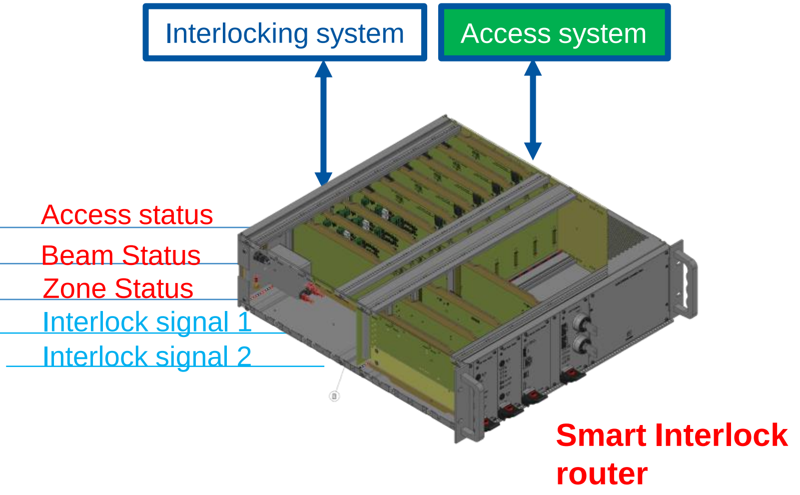


CERN Radiation Monitoring Electronics (CROME)

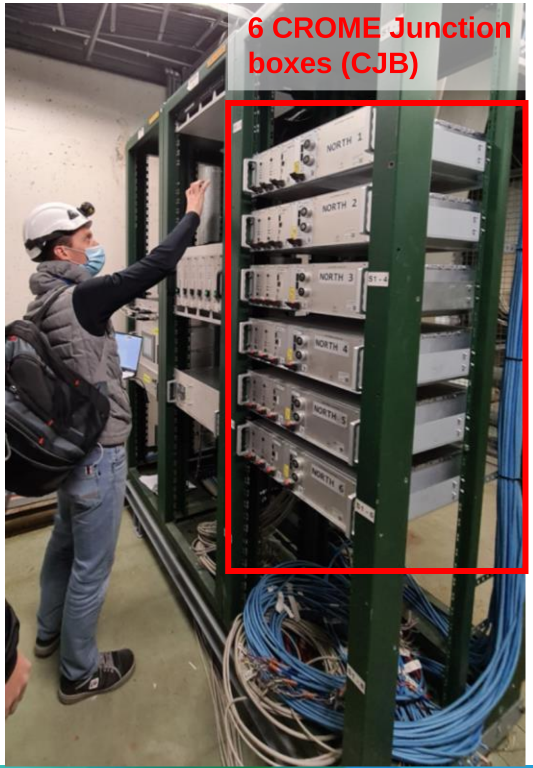
Redundancy can be extended at system level



CROME Junction Box



North Area (EHN1)

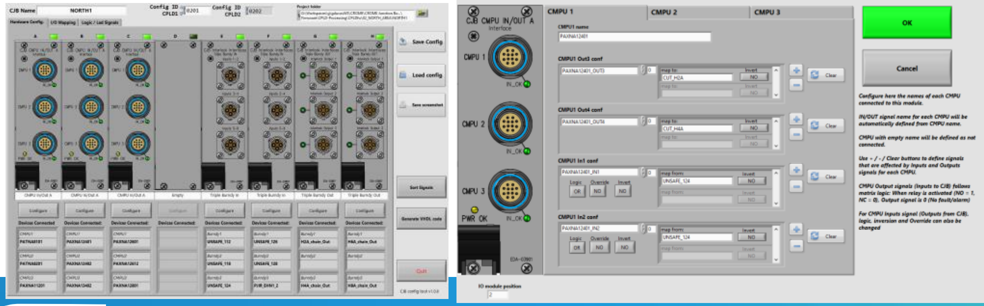


CERN Radiation Monitoring Electronics (CROME)

CROME Junction Box : Configurable Interlock "router"

- Receives interlock outputs from CROME Monitors
- Receives interlock outputs from other RP systems on the zone
- Receives access system signals (doors status,…)
- Combines this signals through a programmable global logic (different for each zone)
- Generates global interlock signals, radiation alarm repeater signals, …

Configuration can be generated automatically using a GUI



Input Outputs Modules :
- PSS SM18
- Burndy IN/OUT
- CMPUs IN/OUT

Power Supply Modules :
- DC IN / AC IN
- 24V, 5V Out

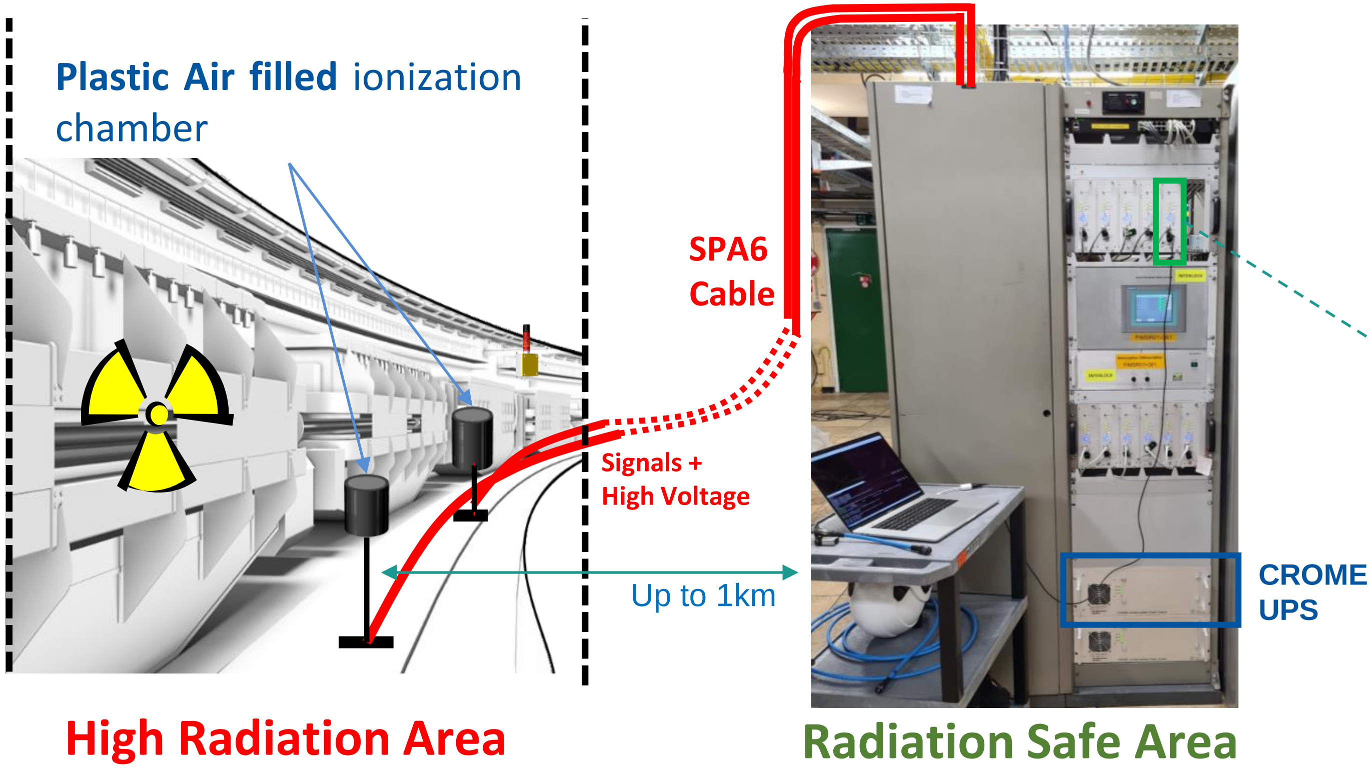
Remote Status module :
- Running Zynq SoC (OS+HDL)
- Collecting data CJB
- Communication (only upstream) with WinCC OA based
- Supervision

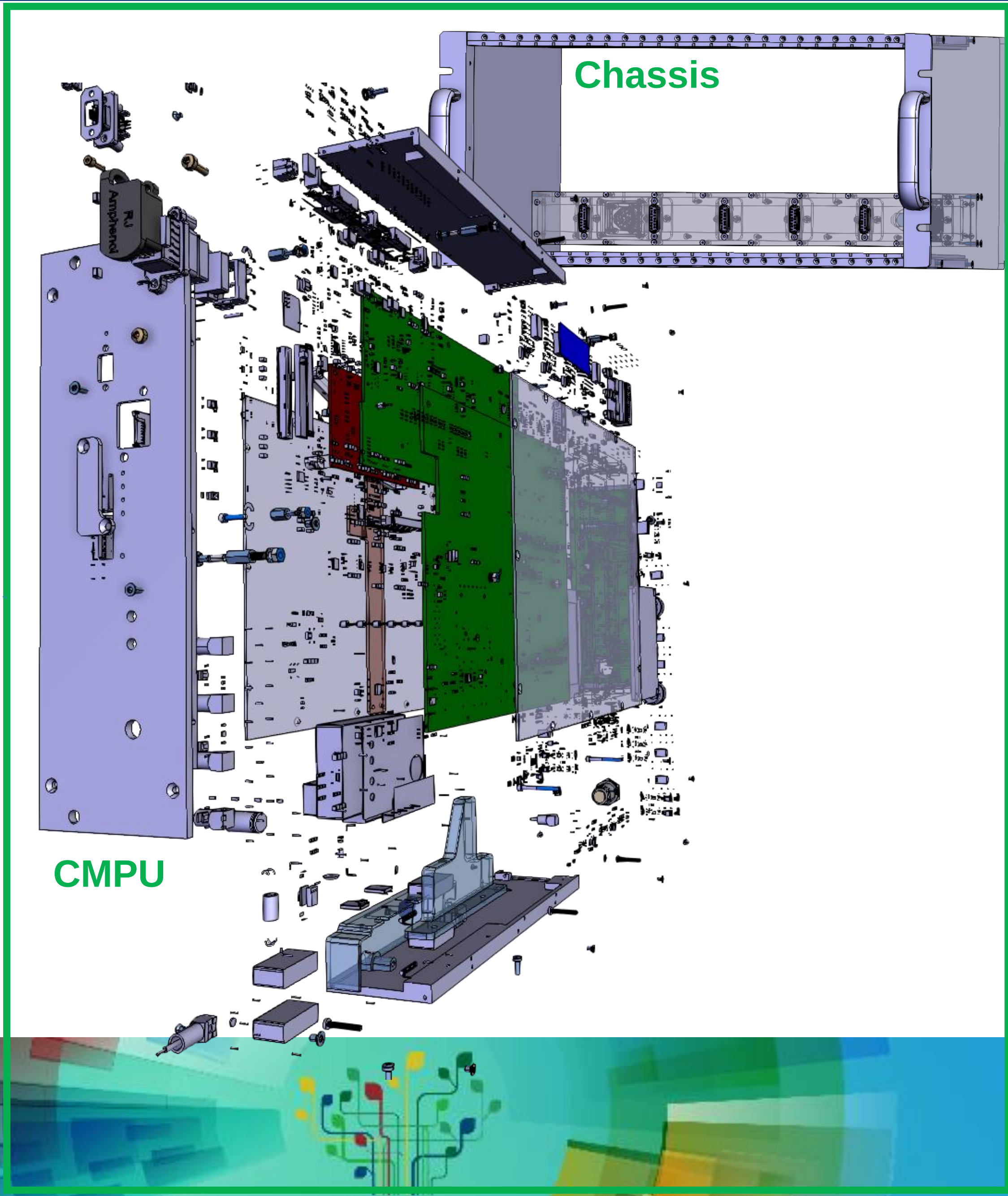
Processing Module :
- Running two MAX V in full redundancy
- Routing inputs to outputs :
  - PSS statues, gates or beam status to CROME CMPUs
  - Outputs of CROME CMPUs to Interlocking system
  - CROME CMPUs to CROME CMPUs
  - ….
- **Combinatory logic (Decision delegation)**

CERN Radiation Monitoring Electronics

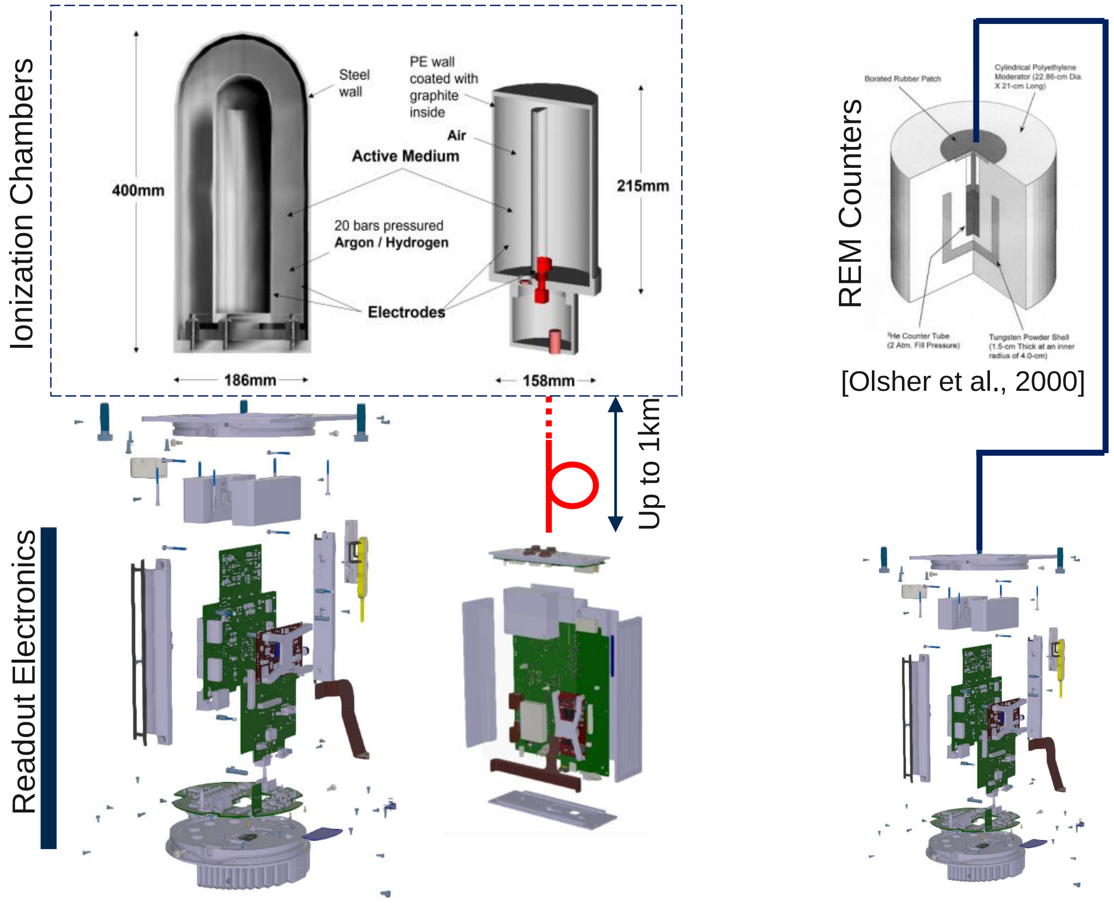
CROME Rack System for high radiation areas :

CROME Rack-mount Version at CERN at the PS Booster

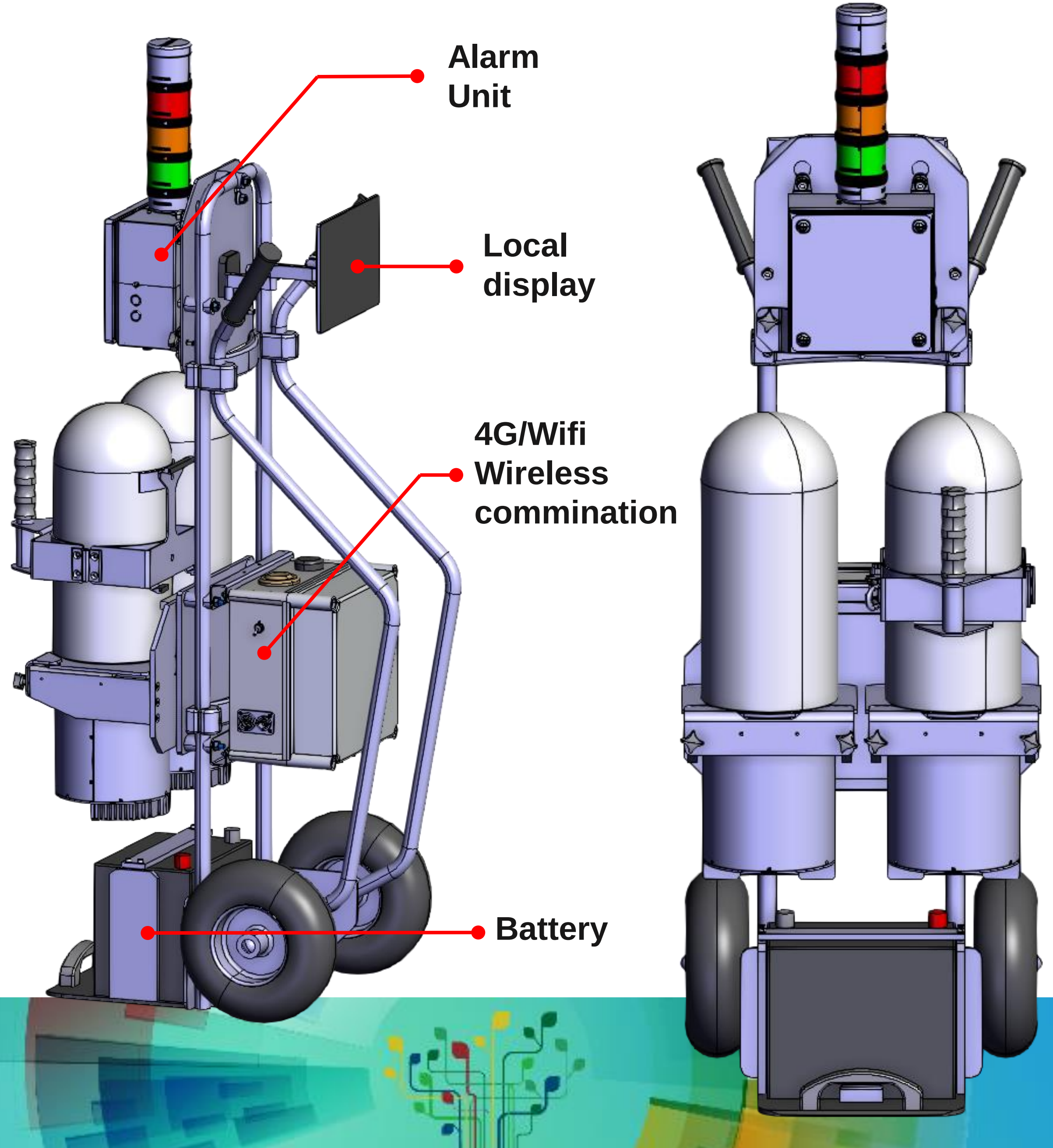




CERN Radiation Monitoring Electronics



CROME Fixed Installations



CROME Manufacturing

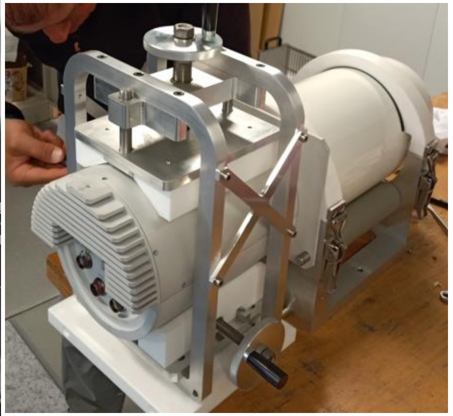
Assembly and integration of CROME Bulk version

HW integration automated tests

Temperature stress validation

Temperature compensation

Detector integration



Stability tests

Assembly and integration of CROME Rackable version

Automated current calibration

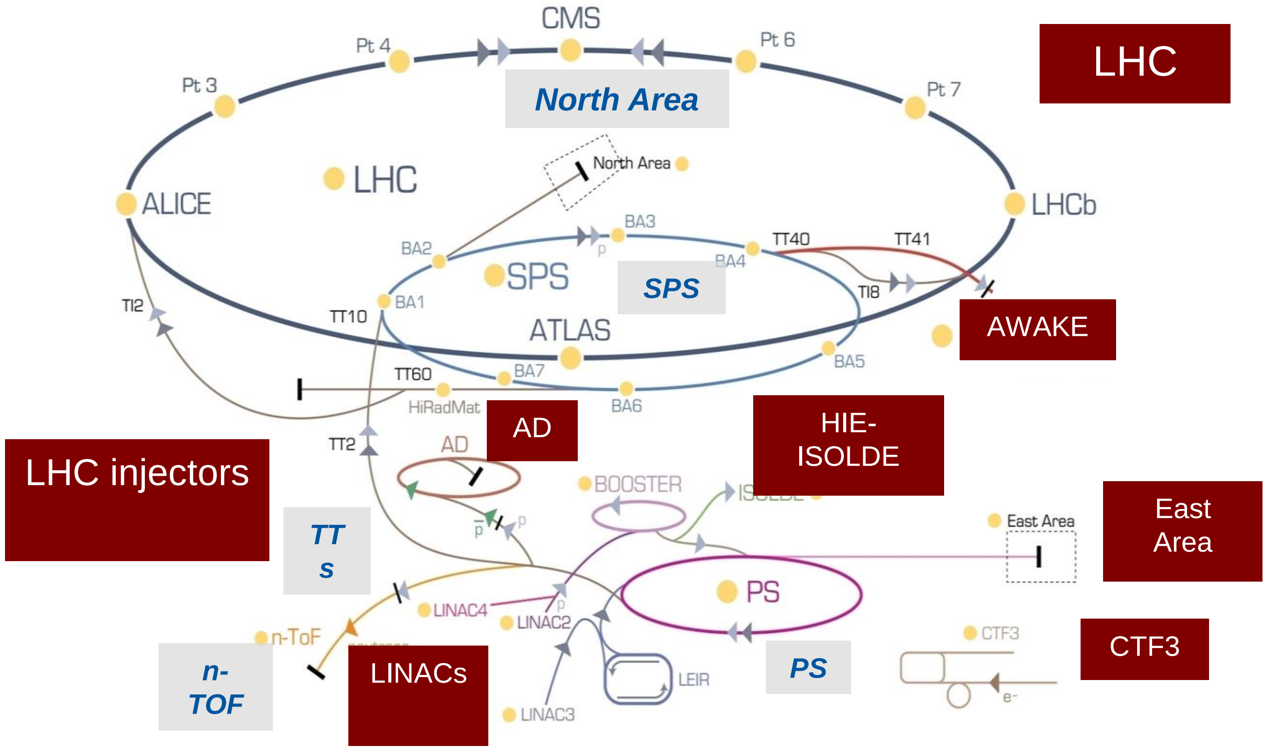
HW integration automated tests

Temperature tests of CROME Rackable versions

Long-term tests of CROME Rackable versions

Radiation & Environmental Protection After LS2 & LS3

CROME	2021 (A2C)
RAMSES	Will be replaced by CROME in 2028 (R2C)



Replacement during LS2 of

153 monitors and 70 alarm units

(532 pieces of equipment)

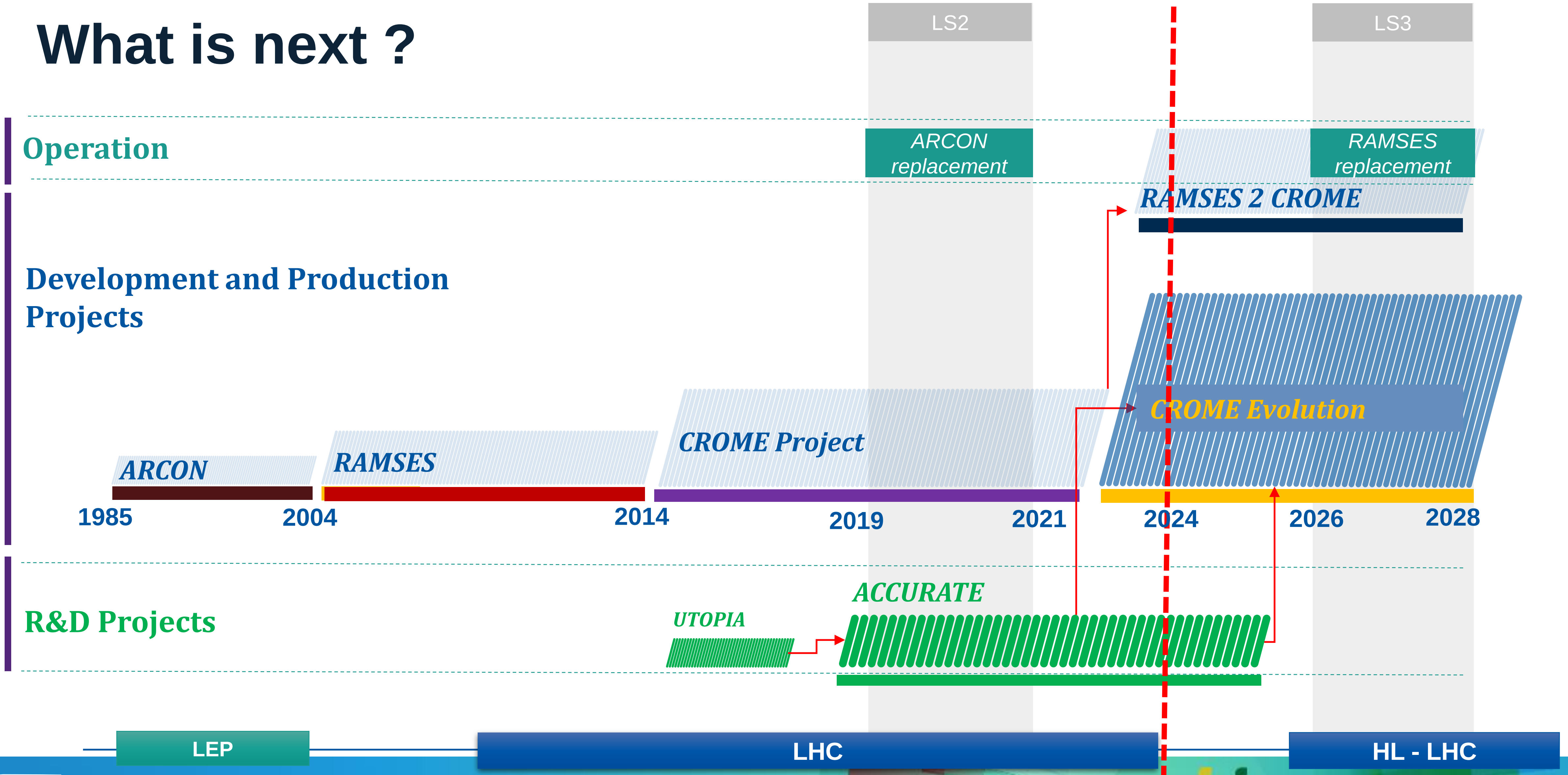
Replacement during LS23 of

436 of RAMSES monitors and 170 alarm units

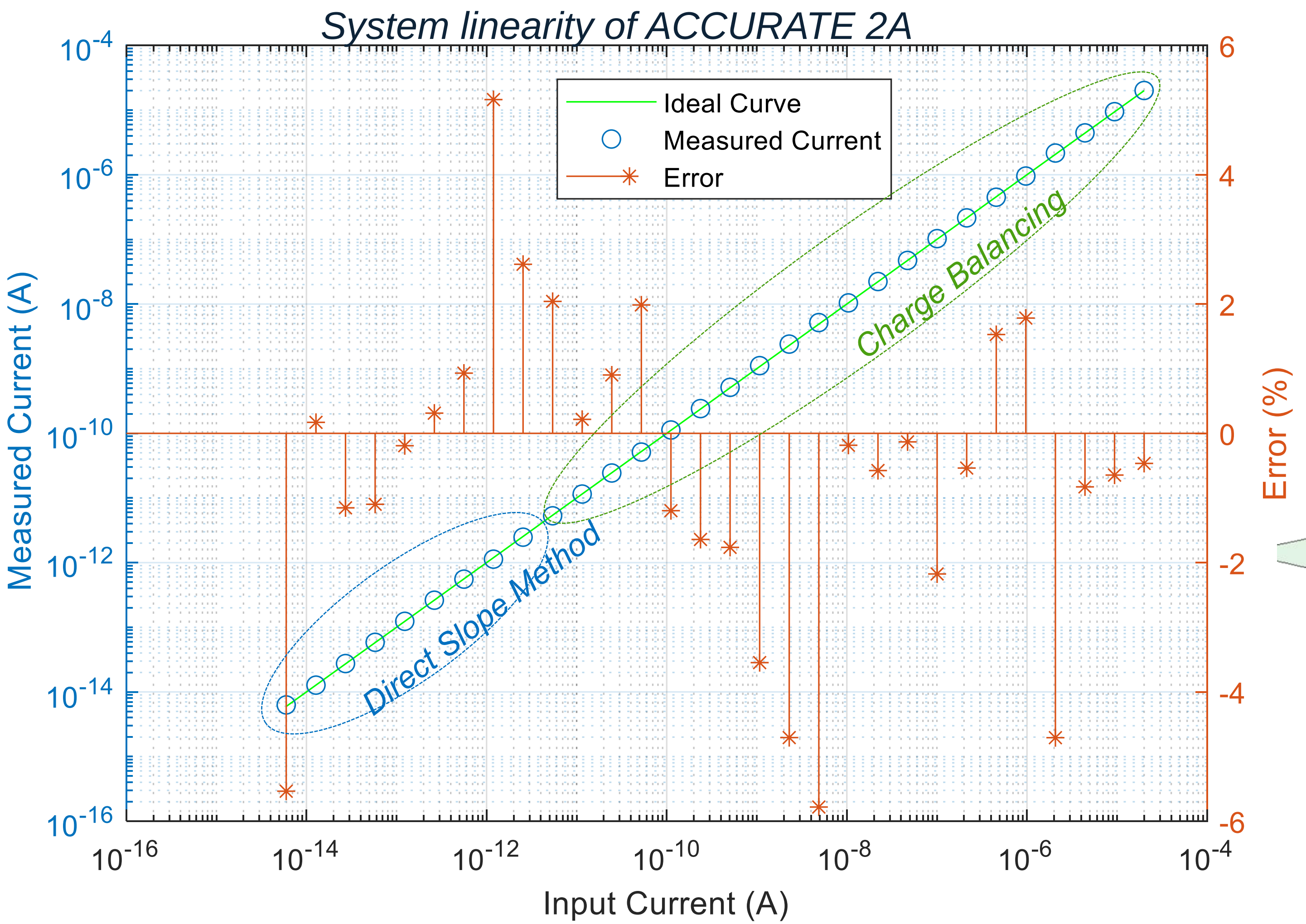
(1586 pieces of equipment)

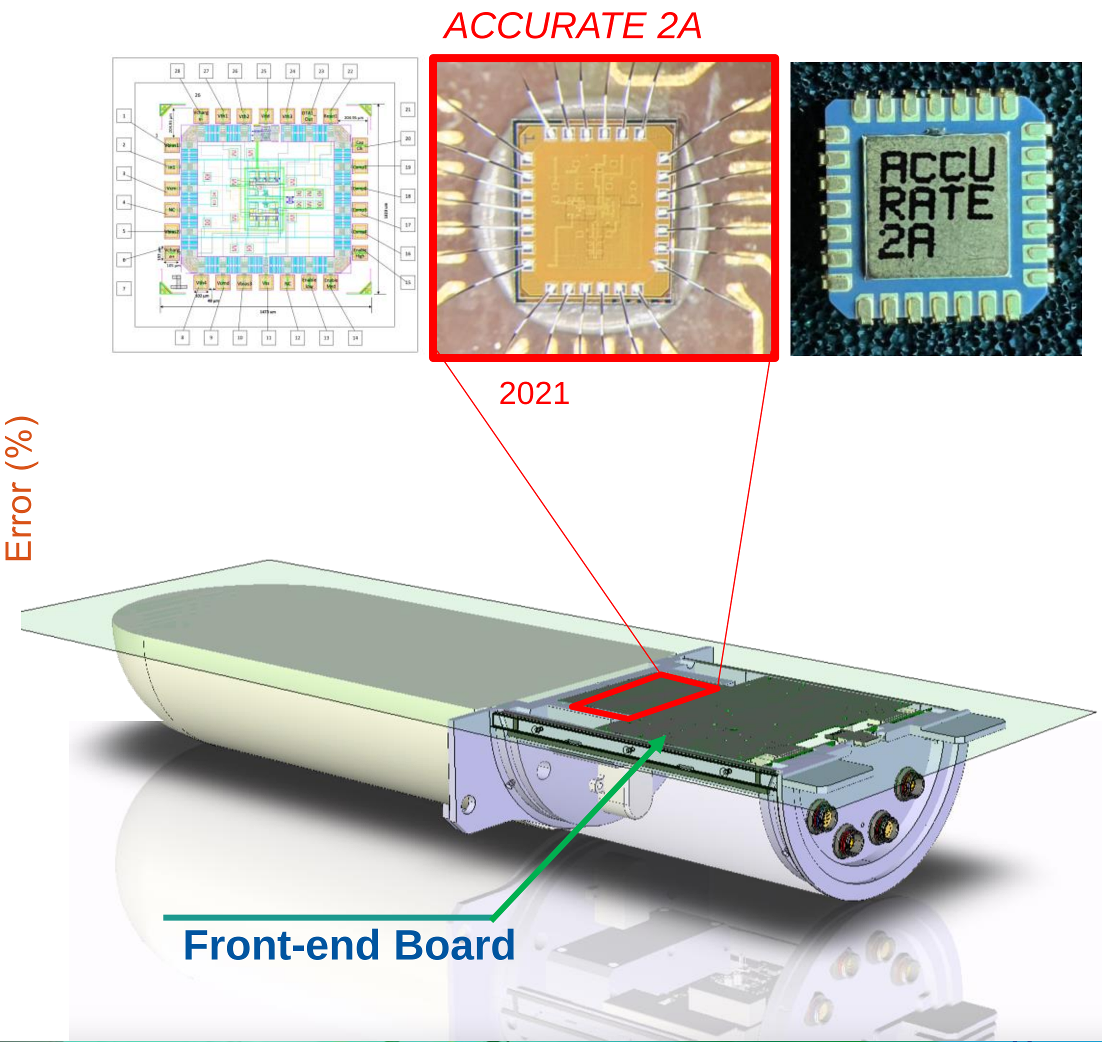
What is Next ?

What is next ?

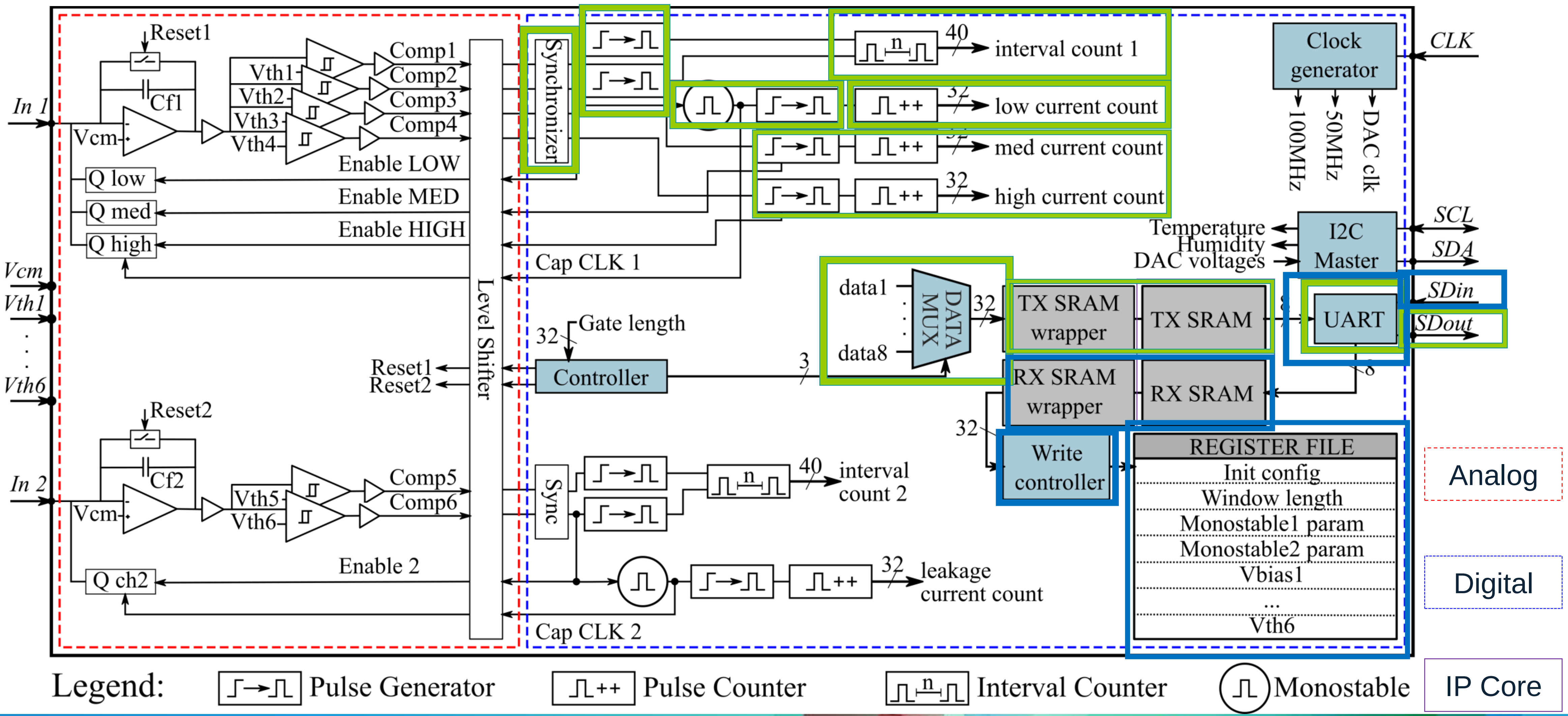

LS2
LS3
Operation
ARCON replacement
RAMSES replacement
RAMSES 2 CROME
Development and Production Projects
CROME Evolution
ARCON
RAMSES
CROME Project
1985
2004
2014
2019
2021
2024
2026
2028
R&D Projects
UTOPIA
ACCURATE
LEP
LHC
HL - LHC

CROME Evolution

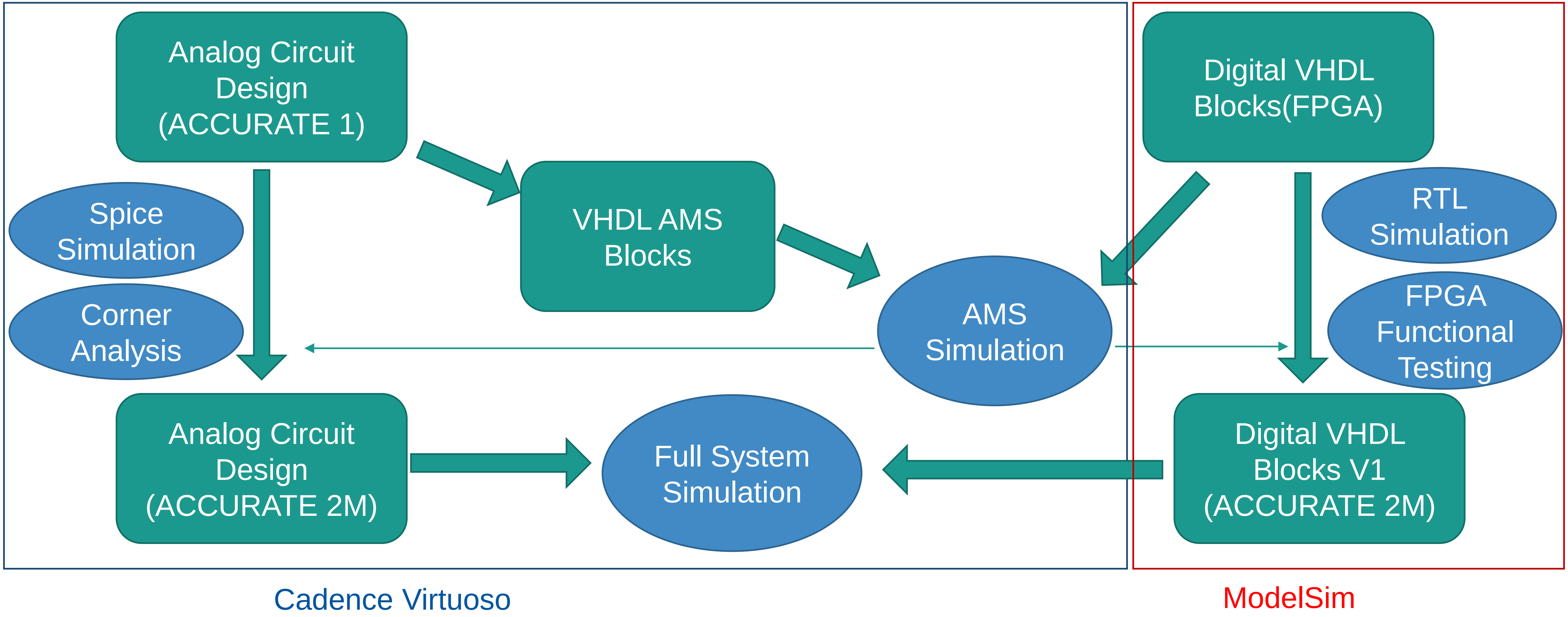




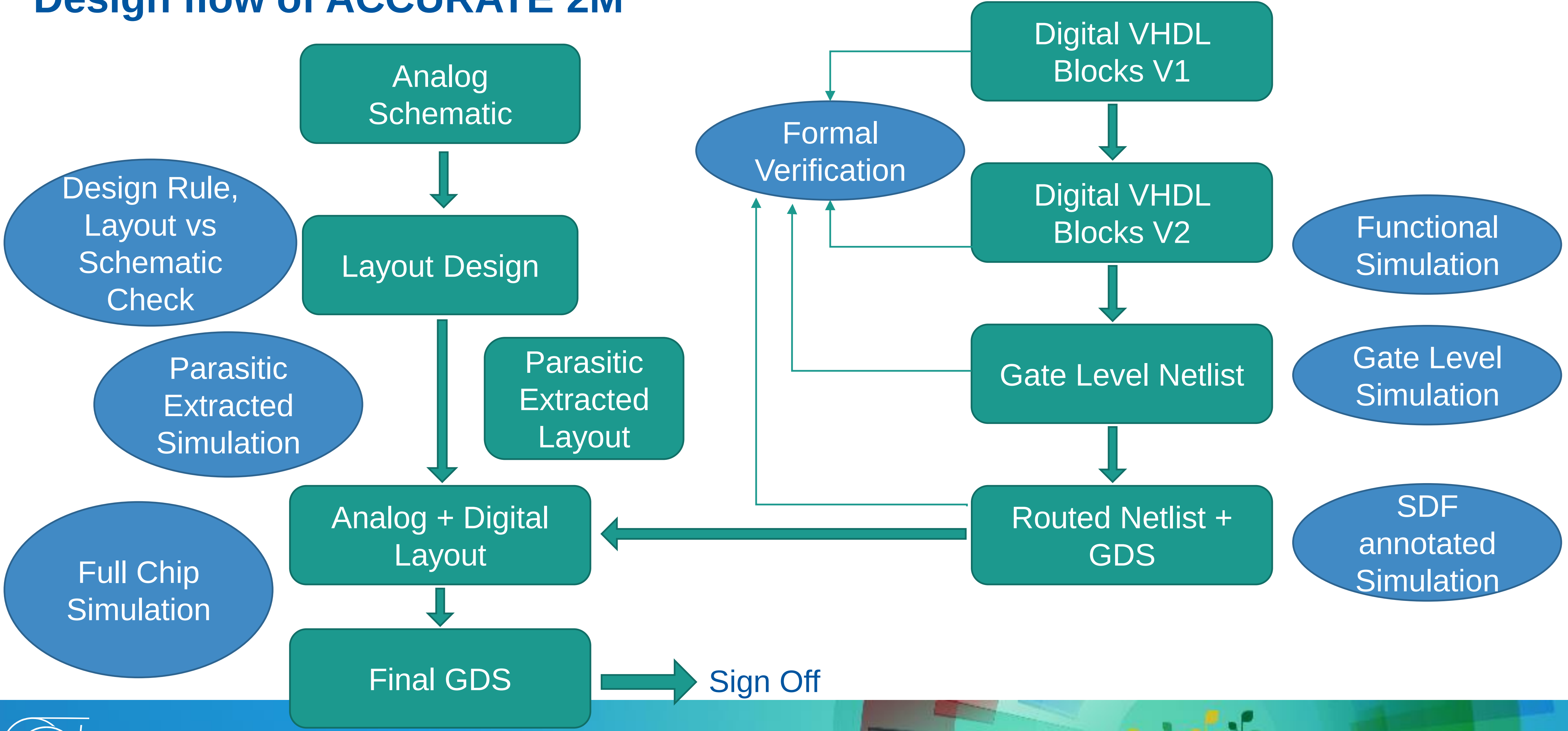
ACCURATE 2M system architecture



Design flow of ACCURATE 2M



Design flow of ACCURATE 2M



ACCURATE 2 Verification - Results

- **Exhaustively proved functionality of most blocks** end-to-end
  - Proved current measurement blocs
  - End-to-end proofs based on top-level inputs and outputs of full design were not feasible
- **Found and removed 30 bugs**:
  - 20 caused by ambiguous specification
  - 11 found by review of specification and natural language version of formal properties*

Block	Specification	Design	Verification requirement	Verification code	Total mismatch
Interval Counter	6	8	8	5	16
Pulse Counter	-	1	-	-	1
Pulse Generator	1	-	2	2	2
Synchronizer	1	-	-	1	1
Monostable	1	2	1	1	3
Channel2 Interface	1	1	2	2	2
TxSRAM Wrapper	1	1	3	3	3
Top Module	-	2	-	-	2
Total	11	15	16	14	30

Ceesay-Seitz, K., Kundumattathil Mohanan, S. Boukabache, H., Perrin, D.: Formal Property Verification of the Digital Section of an Ultra-Low Current Digitizer ASIC.
Proceedings of Design and Verification Conference and Exhibition Europe, DVCon Europe, Munich (2021)

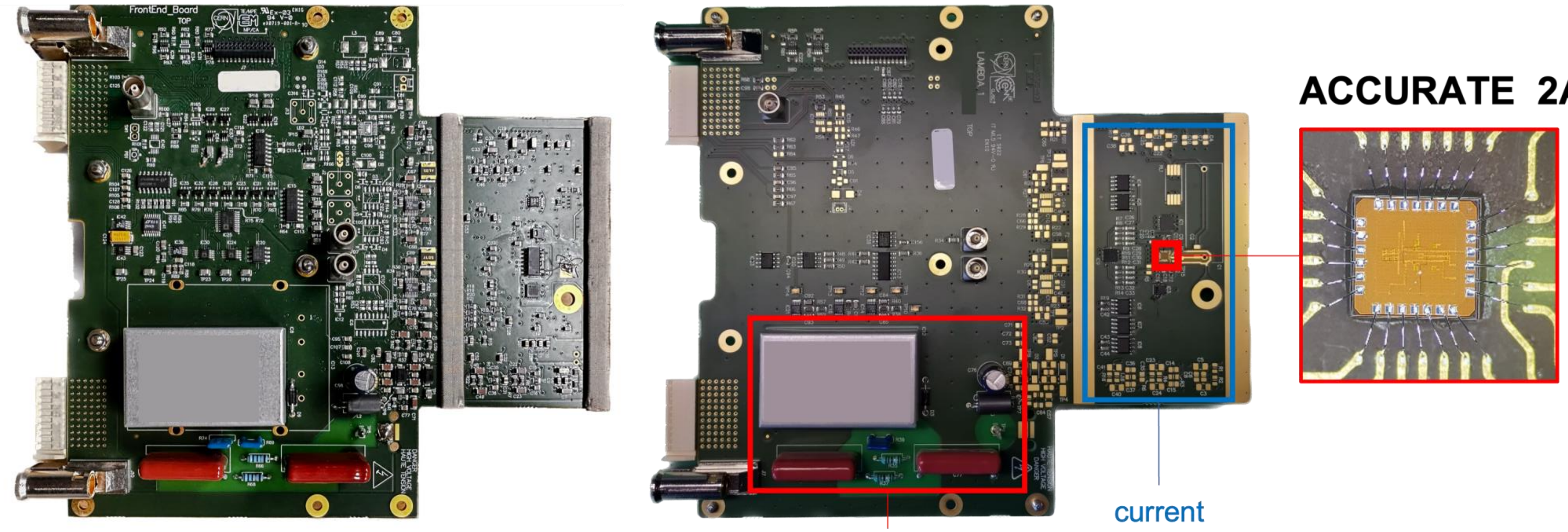
Ceesay-Seitz, K., Boukabache, H., Perrin, D.: Semi-formal reformulation of requirements for formal property verification.
In: Proceedings of Design and Verification Conference and Exhibition Europe, DVCon Europe, Munich (2019)

CROME Evolution

λ Lambda 1 Prototype

Reduction of **60% of the number** of components

CROME Q – Front End | **Lambda 1 – Front End**



ACCURATE 2A

High voltage generation

current measurement

Conclusion – Formal Methods

Huge benefits for critical systems:

- **Unambiguous specifications** → less faults
- **Model checking covers a larger state space** than tests → find more faults
  - Proofs are valid for all input combinations over all time (within the chosen constraints)
- **Fast detection of corner case faults** → hard to find with simulation or tests

It is a **powerful tool** that can be applied

- During many stages of a development project (specification, model generation, verification),
- For many different systems (PLCs, FPGAs/ASICs, Software, …)

It is now an integral part of our development process

→ Currently being integration into our CI pipeline (License issues …)

Challenges:

- State-space explosion: **not every design can be fully verified** within reasonable runtime
- Can be expensive in terms of engineering time for complex designs
- Difficulties to recruit in this field

Conclusion – Formal Methods

“Lessons learned and methodologies developed will pave the path for design and verification of next developments” www.cern.ch

Backup slides

Backup slides

- NLP

Natural Language Properties

- Requirement:

"It shall be possible to manually trigger a reset of a radiation dose alarm through the supervision software."

- Natural language property :

```
"(Cycle is no MC
 and (alarm was configured as latched at the previous MC)
 and alarm reset equals 1 and (dose value is less than (threshold at previous MC)
 or alarm function was deactivated at previous MC))

 implies that:
 (in one clock cycle, alarm is off)"
```

Ceesay-Seitz, K., Boukabache, H., Perrin, D.:
Semi-formal reformulation of requirements for formal property verification.
In: Proceedings of Design and Verification Conference and Exhibition Europe, DVCon Europe, Munich (2019)

Natural Language Properties

"(Cycle is no MC and (alarm was configured as latched at the previous MC) and alarm reset equals 1 and (dose value is less than (threshold at previous MC) or alarm function was deactivated at previous MC))
implies that:(in one clock cycle, alarm is off)"

- SystemVerilog property:

```
property pIntAlarmResetBetweenMT1();
     (mtValidxDI == 0 && latchedLastMC == 1 &&
integralAlarmResetxDI == 1 &&
     (signed'(integralxDO) < signed'(thresholdLastMc) ||
     alarmActiveLastMc == 0))
     |->
     ##1 (ALARMxDO == 0);
endproperty
```

Ceesay-Seitz, K., Boukabache, H., Perrin, D.:
Semi-formal reformulation of requirements for formal property verification.
In: Proceedings of Design and Verification Conference and Exhibition Europe, DVCon Europe, Munich (2019)

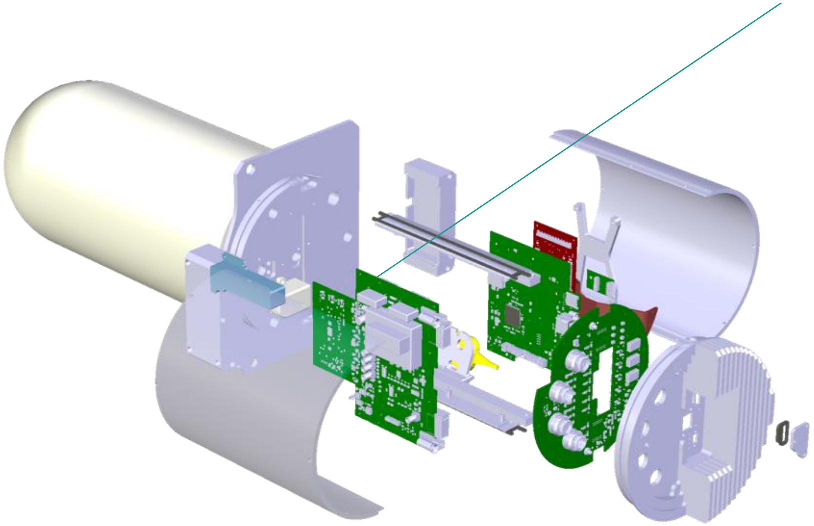
Backup slides

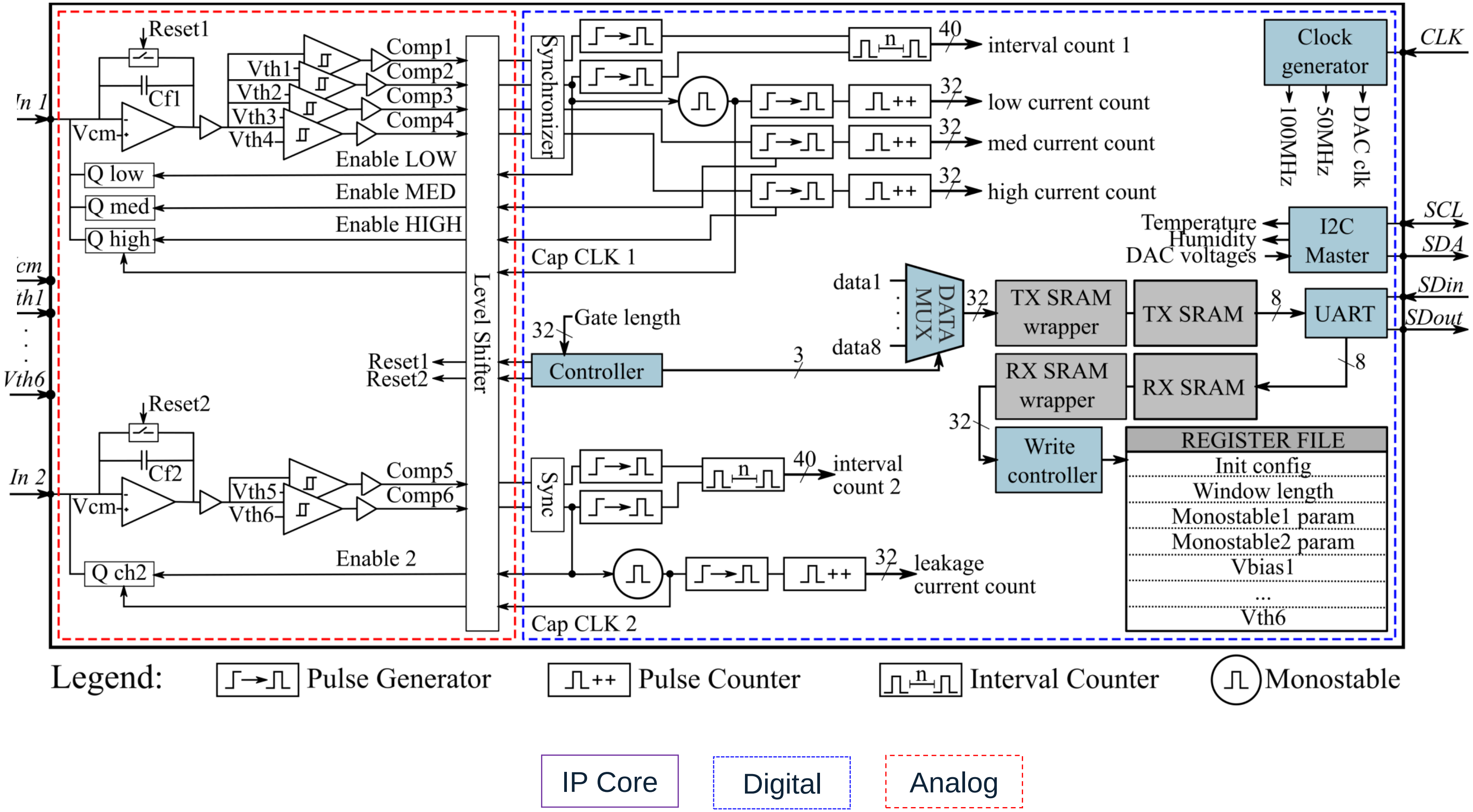
- Counters

Verification Example – ACCURATE2 Mixed signal ASIC

Prototype for new read-out front end for CROME

- Several up to 40 bits wide counters
- Many corner cases





S. K. Mohanan, H. Boukabache, V.Cruchet, D. Perrin, S.Roesler, and U. Pfeiffer, "*An Ultra Low Current Measurement Mixed-Signal ASIC for Radiation Monitoring Using Ionisation Chambers*", (IEEE sensors)

Simple properties – action caused by an event

Prove that for **all** 2^{32} possibilities of the target value and **any combination** with other input signals, any time the counter equals the target value, the design generates a pulse.

```
assert property (
        counter == target_value
    |=>
    $rose(pulse)
);
```

Proven for ALL value combinations of ALL signals that are not explicitly mentioned.