Configurable real-time emergency pulse termination system for investment protection in ITER's interlock architecture

D. Karkinsky[1], Ivo. Carvalho[1], E. Barrera[2], **I. García-Siguero**[3] , D. Grillot[1], Joao Lourenco[4], Alvaro Lopez[4], Ruben Lopez-Villanueva[1], Alvaro Marqueta[1], Isabel Nunes[1], Peter de Vries[1], Pablo Rebollo[2], Mariano Ruiz[2], Pierre Petitpas[1], Luca Zabeo[1], Maximos Tsalas[1]

[1]ITER Organization, St. Paul-lez-Durance, 13067 France.

[2]Instrumentation and Applied Acoustic Research Group (I2A2), Universidad Politécnica de Madrid, Madrid, Spain.

[3]VERSE EUROPA S.L., Rambla de Cataluña 72, 08007, Barcelona, Spain.

[4]Critical Software, Pq. Industrial de Taveiro Lote 49, 3045-504 Taveiro, Portugal

ACKNOWLEDGEMENTS

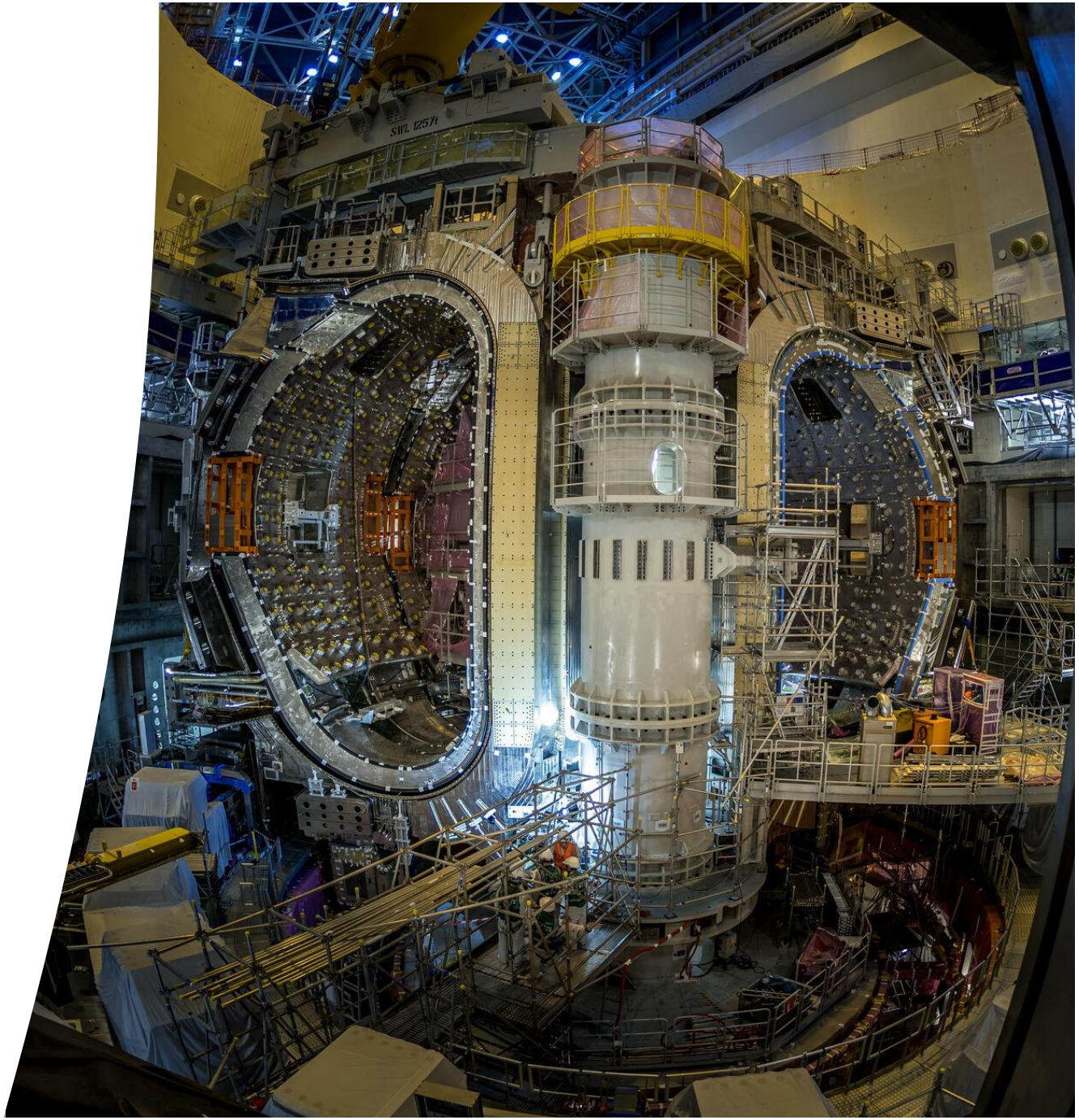
This work was supported under grant PID2022-137680OB-C33 funded by MCIN/AEI/10.13039/501100011033

china eu india japan korea russia usa

science + engineering

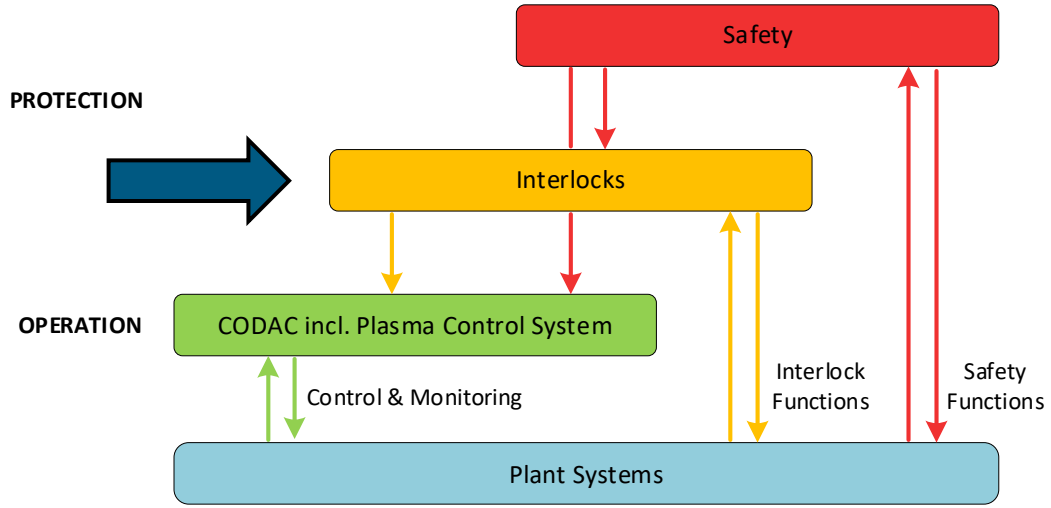
OUTLINE

- Background
- Motivation
- Emergency Pulse Termination at ITER
- CIS Critical Gateway
- CIS Critical Gateway Prototype
- Results & Conclusions



Background I

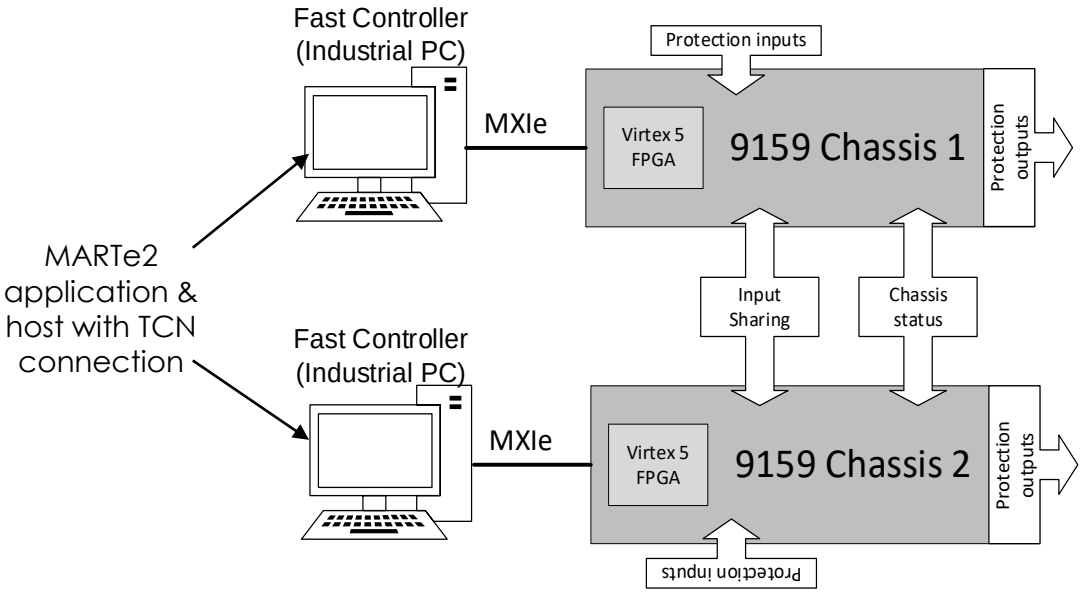
- ITER is a super-conducting tokamak capable of 15MA of plasma current – more than 350MJ of thermal energy alone.
- Control of ITER is divided into three layers based on the impact of events
  - **Plasma Control System (PCS):** This is the conventional control system in charge of operating ITER under normal conditions. It is responsible for controlling and maintaining the plasma in the ITER tokamak.
  - **Interlock Control System (ICS)** [1] **:** is the ITER system that implements the Investment Protection Functions and is responsible for protecting the integrity of the machine against any possible failure.
  - **Central Safety System:** layer that implements nuclear and personal protection functions.
- The ICS is structured as:
  - **Central Interlock System (CIS):** Modules in charge of implementing the Central Protection Functions coordinating the events and actions between plants.
  - **Plant Interlock System (PIS):** Modules implementing protection event/actions for individual plants.
  - **Advanced Protection System (APS):** Modules that implement plasma-related protection functions.



1. J.L. Fernández-Hernando, D. Carrillo, G. Ciusa, Y. Liu, I. Prieto-Díaz, R. Pedica, S. Sayas, J. Soni, A. Vergara, The ITER interlock system, Fusion Engineering and Design, Volume 129, 2018, Pages 104-108, ISSN 0920-3796,

Background II

- The ICS implements three different architectures depending the response time required: hardwired, slow (PLC) and **fast (FPGA).**
- The CIS Fast Architecure[1] (CIS-FA) is based on the use of two redundant NI9159 CompactRIO chassis in 1oo2D mode, each with its own Fast Controller connected.
  - Firmware development through the LabVIEW FPGA tool
  - Host software use MARTe2 framework on Linux RT kernel
  - Following the IEC 61508 standard guidelines[2]
  - Platform customized to meet hard real-time requirements[3]



1. E. Barrera et al., "*Implementation of ITER Fast Plant Interlock System Using FPGAs With CompactRIO*," IEEE Transactions on Nuclear Science, vol. 65, no. 2, pp. 796-804, Feb. 2018, doi: 10.1109/TNS.2017.2783243.
2. I. García-Siguero et al., "*Verification and Validation of ITER Interlock System Fast Architecture According to IEC 61508 Standard*" IEEE Transactions on Nuclear Science, vol. 70, no. 6, pp. 1164-1170, June 2023, doi: 10.1109/TNS.2022.3224780
3. D. Karkinsky et al., "Assessing NI FPGA-Based Platform With MXIe Interface for Use in ITER Hard Real-Time Investment Protection Applications," in IEEE Transactions on Nuclear Science, vol. 72, no. 3, pp. 530-537, March 2025, doi: 10.1109/TNS.2024.3474749.

Motivation

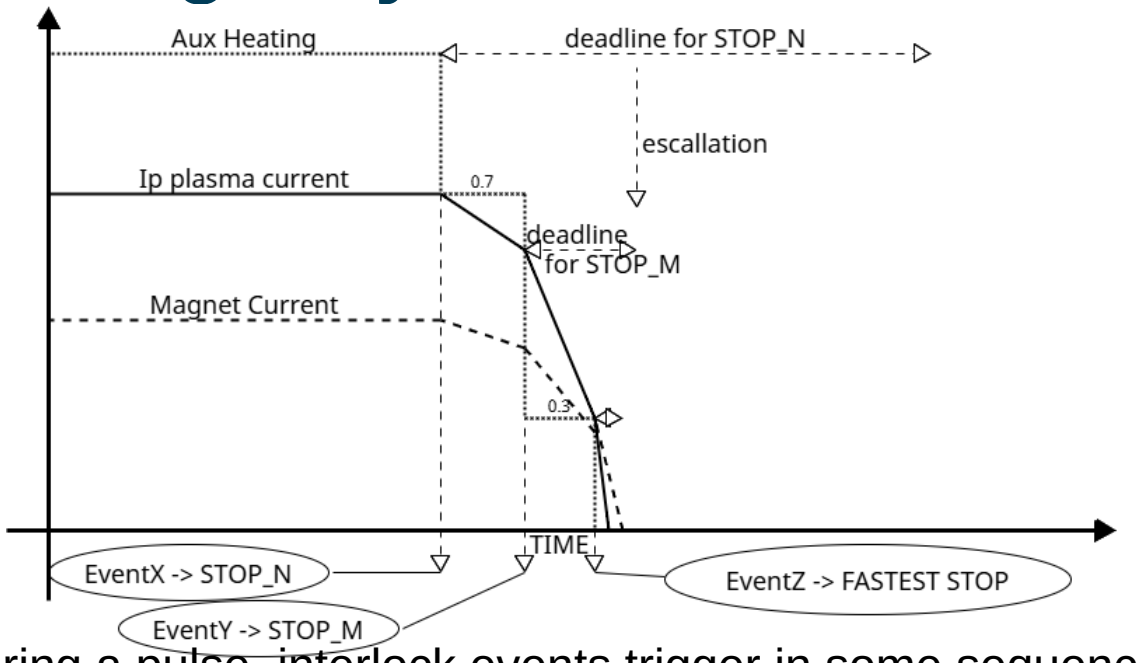
- Tokamak interlocks can terminate a pulse very fast through immediate actions of hardwired logic. → This induces large mechanical and thermal loads on the tokamak's structures. Availability is seriously reduced.
- There are some interlock events where interlock actions can be scheduled rather than triggered immediately → Allows time for conventional systems (e.g. Plasma Control System PCS) to lower tokamak stored energy in a controlled manner.

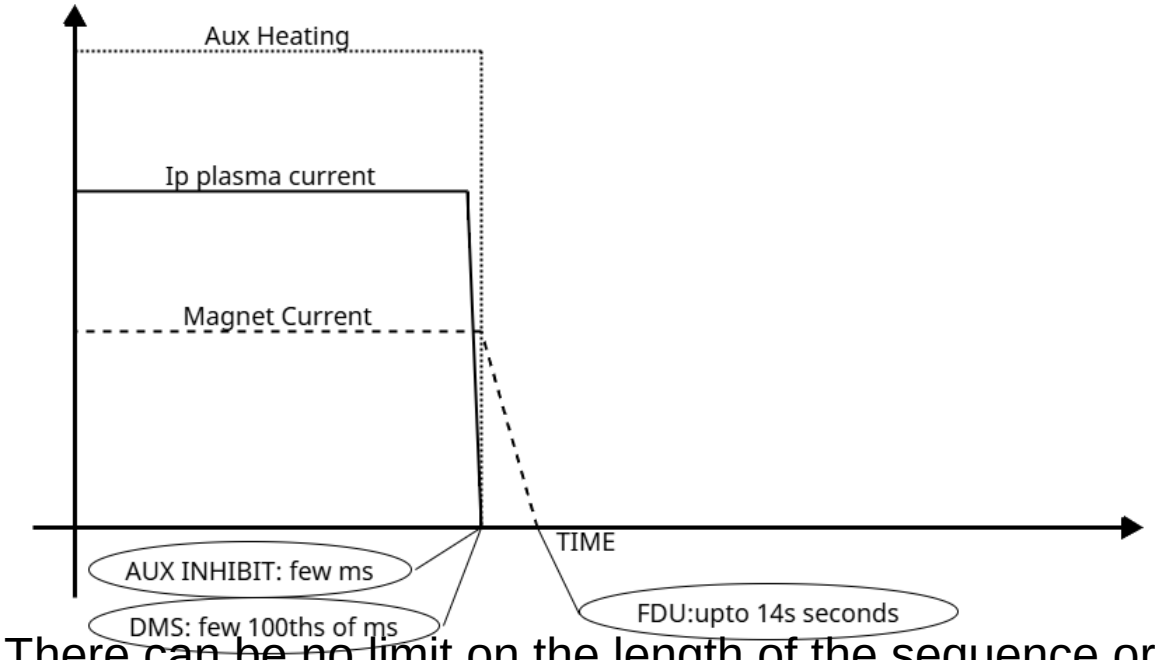
Within CIS, the central function that coordinates with PCS to terminate a pulse is called

<u>Emergency Pulse Termination (EPT)</u>

- EPT offers a period of time before interlock actions must trigger to **GUARANTEE** pulse termination → Interlocks trigger immediate termination only if the events **ESCALLATE** to conditions that requires it.
- EPT functional specification must cater for evolving tokamak plant requirements & design. → It must be general enough for scalable, cost-efficient integration and configurable enough for specific kinds of operation.

Emergency Pulse Termination at ITER I

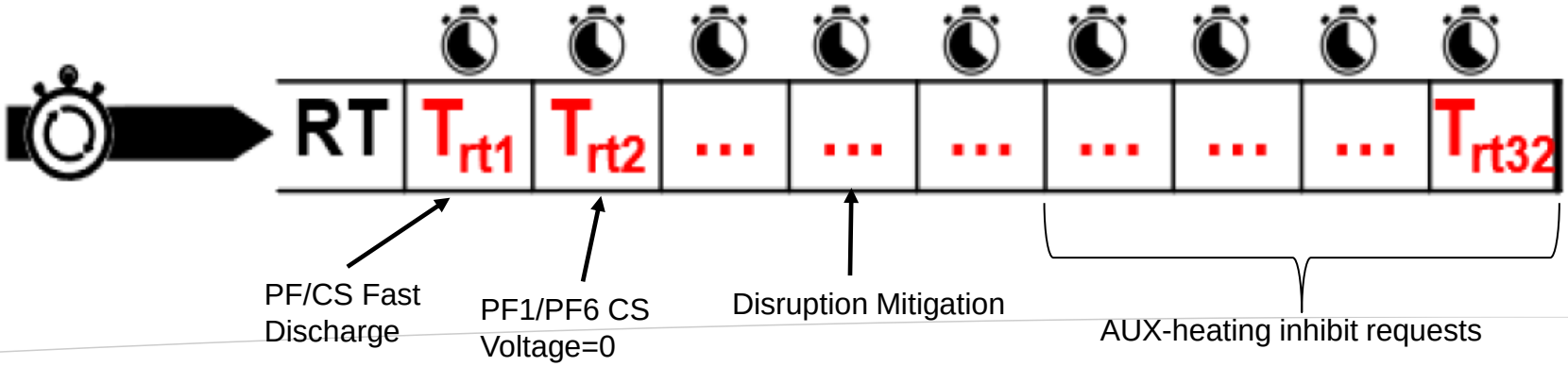




- During a pulse, interlock events trigger in some sequence. There can be no limit on the length of the sequence or any assumptions on the order in which events occur.
- All events have an associated deadline to achieve pulse termination. Pulse termination is defined as; no plasma current, Poloidal Field (PF), Central Solenoid (CS) and Correction Coils (CC) magnets fully discharged, auxiliary heating switched off and inhibited.
- Deadlines either remain in force until the end of the pulse or escalate towards immediate pulse termination.
- Immediate pulse termination is where PF/CS is discharged at the fastest possible rate through a bank of resistors and plasma needs to be shut down within a few 100ths of ms with disruption mitigation – PCS no longer in control.

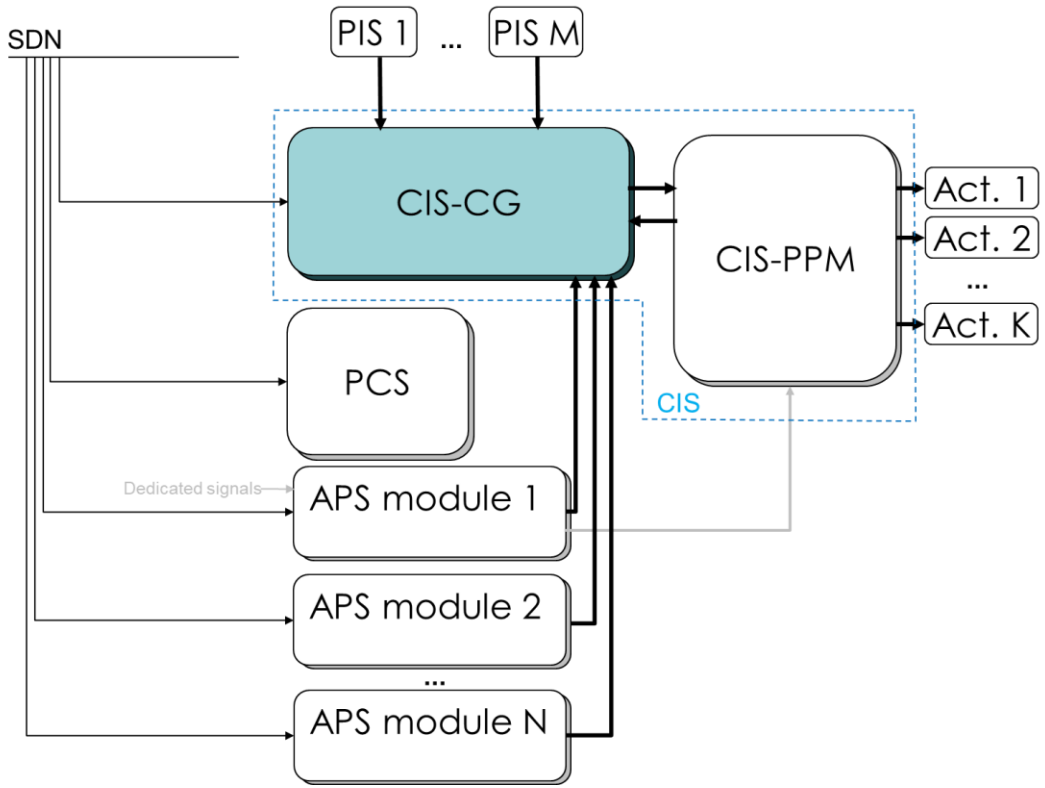
Emergency Pulse Termination at ITER II

- EPT has 32 interlock action requests governed by 32 counters updated in hard real-time.
  - This number is oversized to ensure future-proofing.
- When a counter reaches 0s, a corresponding interlock action is requested.
- Interlock events are mapped to a set of **stop-codes**, with associated deadlines specified in a table.
  - Deadlines are specified relative to event triggering time.
- Priority Evaluation - If an interlock event requests a stop-code with a shorter deadline than the counter's current time, the counter is advanced to the shorter deadline. Stop-codes latch until termination is achieved.
- Countdown – below 4000s, counters are updated with elapsed time with 500us precision.
  - Maximum ITER pulse time is 3000s. 4000s is the threshold for enabling the countdown.
- Initial state of the function - counters are initialized before start of pulse to 5000s.



CIS Critical Gateway I – System Design

- At ITER ETP is implement in the CIS Fast Architecture – **CIS Critical Gateway (CIS-CG)**
  - One CIS-CG node is in the Main Server Room and the other is in Backup Server Room.
- Each node receives a fixed set of stop codes (42) through a hardwired 5Mbps Manchester Code link with error detection mechanism (CRC8, Sequence Number).
- Each node is time synchronized to ITER's central time coordination network TCN (PTP) with less than 1us jitter.
- Each node monitors the PCS through a heartbeat on the real-time network SDN.
- PCS receives the active stop codes via SDN from each node separately, performs exception handling and conventional control of the plasma.
- Nodes monitor their TCN synchronization and coordinate counter updates in lockstep so as to be correct even if one node is de-synchronized.



CIS Critical Gateway II – System Details

- Logic implemented entirely in FPGA firmware which operates 100usec control loop carrying out:
  - essential checks,
  - voting stops,
  - prioritizing deadlines and triggering a 500usec counter update process,
  - voting interlock action requests.
- MARTe2 receives PCS heartbeat from SDN, sends PCS heartbeat to the FPGA at 1kHz and reports the status of interlocks back to PCS and CODAC at same rate.
- RHEL 8.5 RT kernel with CODAC Core System distribution and running MARTe2 host application.
- Host interfaces with the other actors (CODAC/SUPervisor, CIS HMI) via OPC UA.

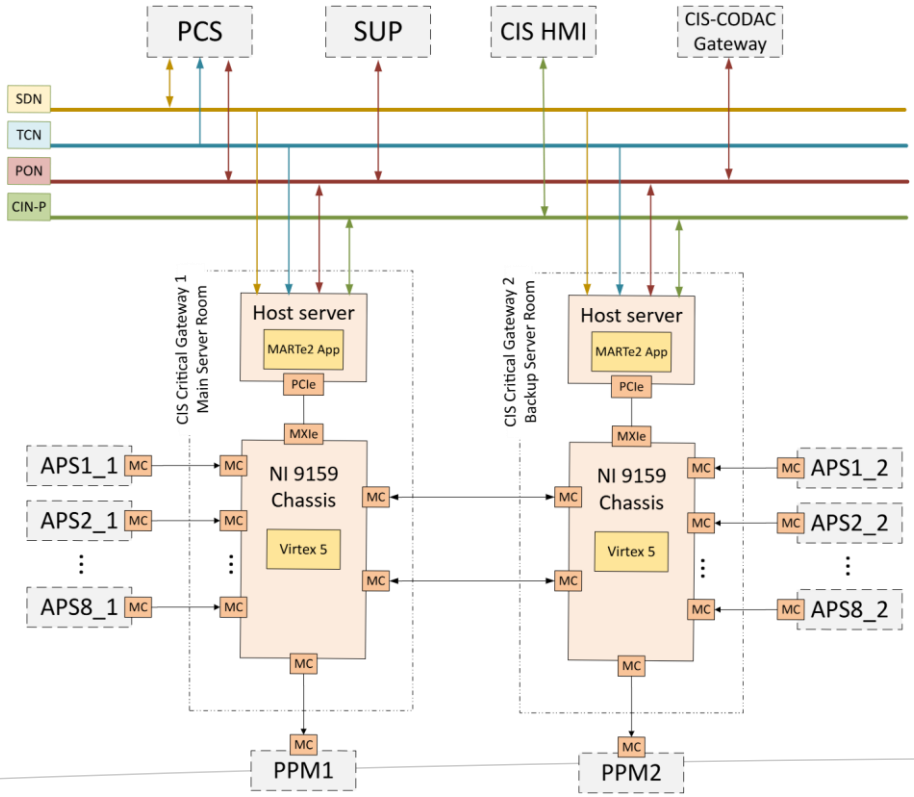
CIS Critical Gateway III – System Configuration

- CIS-CG configuration must be coordinated with ITER pulse schedule.
- Configuration is achieved through an IEC61508 compliant approach with ITER's CIS High Integrity Operator Commands (HIOC) protocol and the pulse schedule managed by CODAC-SUP's Chain Data Processing (CDP) & Configuration Validation & Verification Framework (CVVF) [1]
- The critical parameters are the 42×32 stop-code table (~6kB) holding the deadlines for each stop-code.
- The table is stored on the FPGA in dual redundant Error Correcting Code (ECC) BlockRAMs that implement a custom secure access protocol.

1. Karkinsky, D., Van Herck, W., Diaz, I. P., Soni, J., & Marqueta, A. "Integrated supervision for conventional and machine-protection configuration parameters at ITER.", ICALEPCS2021, Shanghai, China, doi:10.18429/JACoW-ICALEPCS2021-WEBR05.

CIS Critical Gateway Prototype

- Prototype developed with requirements close to the final system.
- Includes full implementation of the most critical requirements required for the start of ITER integrated commissioning.
- Includes all defined interfaces at this moment covering the Advanced Protection System (APS)
- The system has been deployed and validated on a test platform that maximally replicates real operation.



Results & Conclusions

- Explained and motivated a concrete definition of Emergency Pulse Termination for ITER.
- First hard real-time system implemented on CIS Fast Architecture → thus validating the CIS-FA platform capabilities.
  - A system that provides guaranteed pulse termination in a fault-tolerant manner coordinated with the PCS.
- The system will be required during the start of ITER integrated commissioning when PCS is expected to attempt magnet operation.
- Meanwhile we will carry out extensive verification of the fault-tolerance properties.
- Define plant guidelines for interfacing the CIS-CG in a scalable manner – plants map their events to stop codes which can be combined upstream. This offers a scalable solution that can be rolled out client systems who have diverse event requirements.
- We plan to define operational procedures for stop-code table configuration, based on hazard analyses.
- The first likely client will be ITER's Coil Power Supply System (CPSS) which has many events that must be precipitated by EPT so-as to prevent long term delays in operation.
- EPT generality and configurability facilitates its adaptation to other tokamak environments (or even other kinds of physics experiments).

Thank you!

Configurable real-time emergency pulse termination system for investment protection in ITER's interlock architecture

D. Karkinsky[1], Ivo. Carvalho[1], E. Barrera[2], **I. García-Siguero**[3] , D. Grillot[1], Joao Lourenco[4], Alvaro Lopez[4], Ruben Lopez-Villanueva[1], Alvaro Marqueta[1], Isabel Nunes[1], Peter de Vries[1], Pablo Rebollo[2], Mariano Ruiz[2], Pierre Petitpas[1], Luca Zabeo[1], Maximos Tsalas[1]

[1]ITER Organization, St. Paul-lez-Durance, 13067 France.

[2]Instrumentation and Applied Acoustic Research Group (I2A2), Universidad Politécnica de Madrid, Madrid, Spain.

[3]VERSE EUROPA S.L., Madrid, Spain.

[4]Critical Software, Pq. Industrial de Taveiro Lote 49, 3045-504 Taveiro, Portugal

Responsible: Damien.karkinsky@iter.org

Presenter: ignacio.garcia@verse-europa.com

iter

china eu india japan korea russia usa

INSTRUMENTATION & APPLIED ACOUSTICS RESEARCH GROUP

UNIVERSIDAD POLITÉCNICA DE MADRID

POLITÉCNICA

VERSE

science + engineering

Critical software