Integrated supervision for conventional and machine-protection configuration parameters at ITER

D. KARKINSKY, W. VAN HERCK, I. PRIETO DIAZ, J. SONI, A. MARQUETA

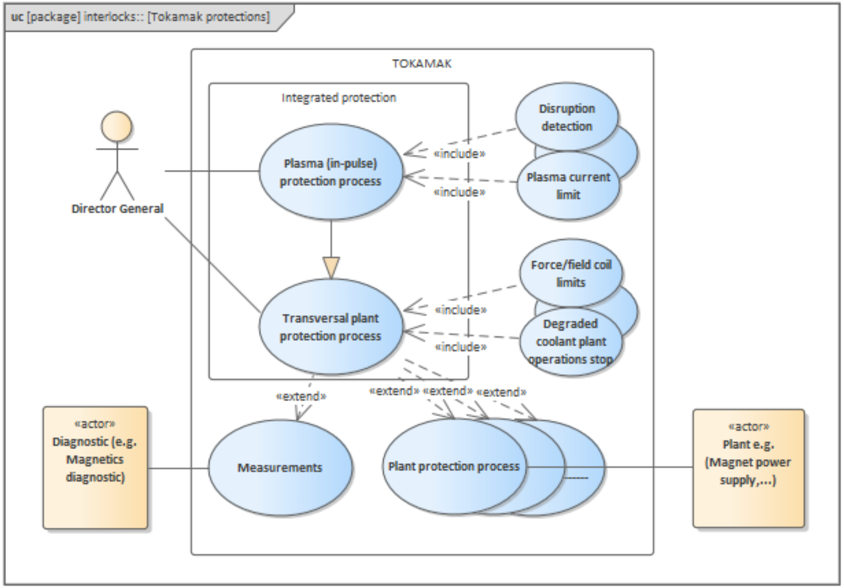
ITER

ICALEPs

20/10/2021

Introduction

- Integrated protection functions – plant protection functions – configuration coupling.



- At ITER,
  - Plant Interlock Systems /diagnostics configured by SUPervision and Automation System – translates physics to plant values.
  - Central Interlock System configured by a separate Supervision Module.
- Protection functions need to meet IEC61508 goals on system configuration.
- **Need:** Integrated configuration mechanism that is IEC61508 compliant.
- **Constraint:** Cannot have a duplicate configuration mechanism.
- **Approach:** Identify gaps in compliance, address in an integrated manner, provide a central technological solution to plants.

Example of configuration parameters coupling

- Pulse Schedule A
  - Plasma current = 15MA
  - Toroidal field = 5.3T
  - Auxiliary heating = …
  - Magnetic shape (CS/PF)
  - …

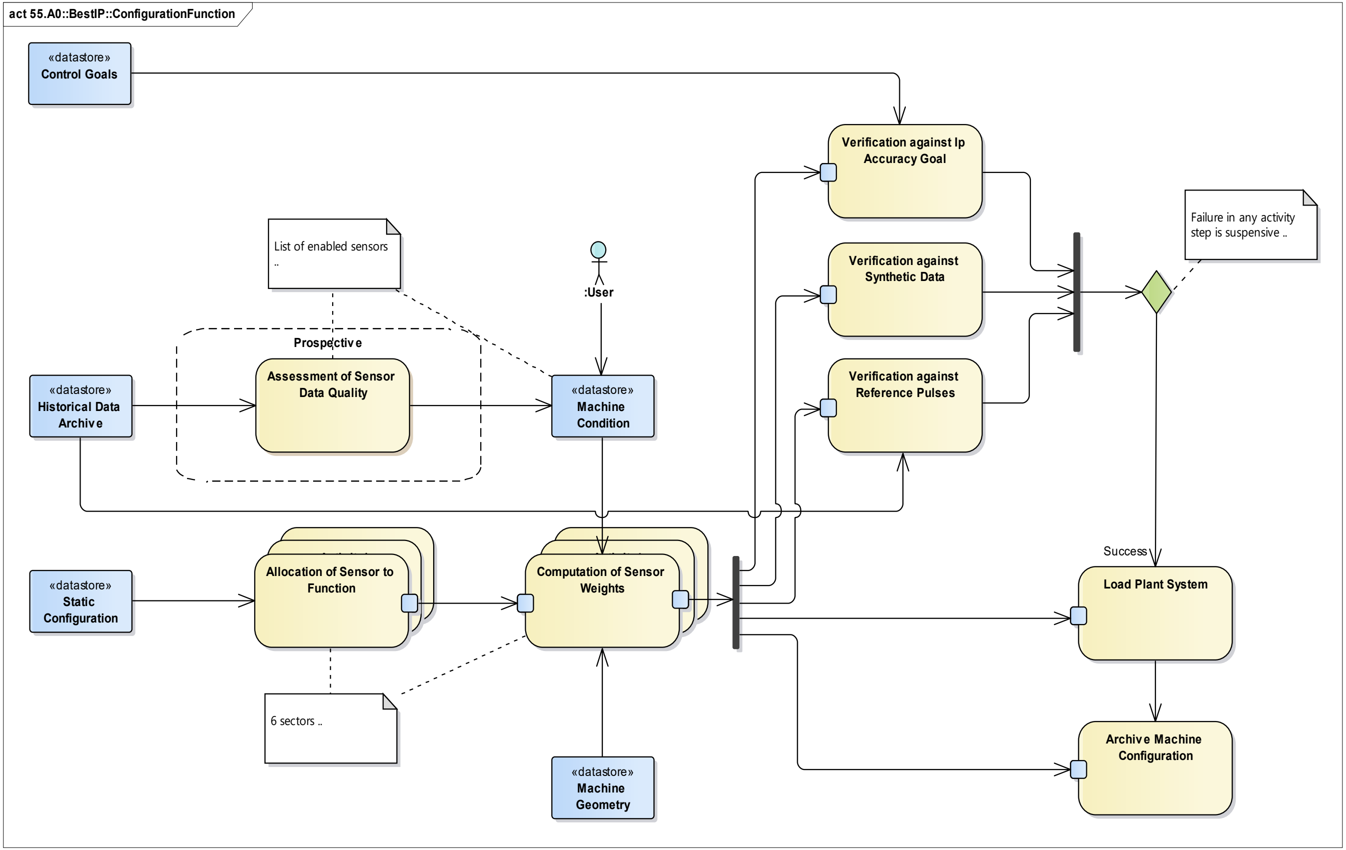
- Investment protection operational requirements
  - … and the magnetic diagnostic must be 1oo2D
  - Fast pulse-stop & pulse inhibit on non-fault-tolerant
  - All 6 sector magnetics must be functional.
  - Fast-pulse-stop & pulse inhibit on 3oo6 …

- Pulse Schedule w.o. plasma
  - Plasma current = 0MA
  - Toroidal field = 2.65T, 5.3T
  - Auxiliary heating = 0
  - CS/PF currents …
  - …

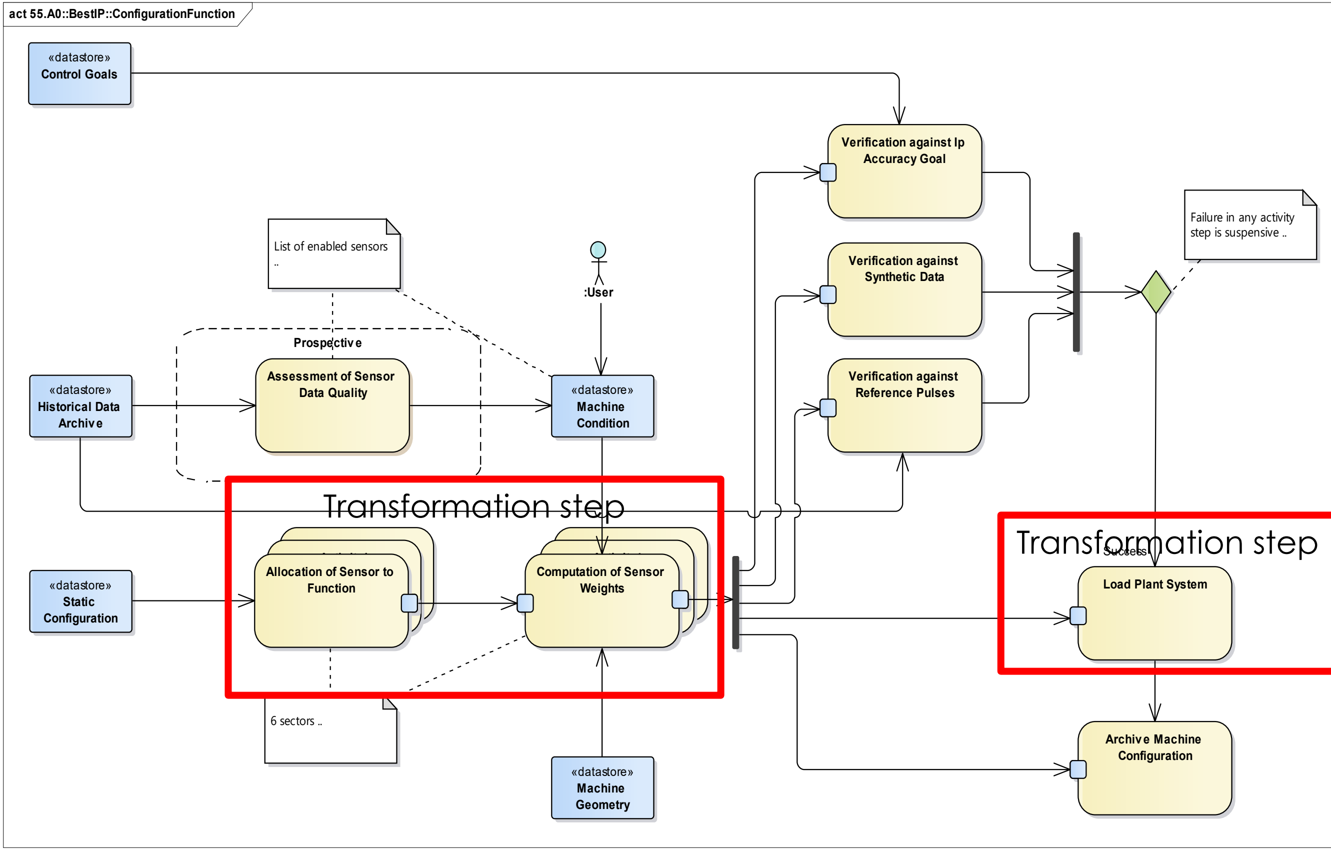
- Investment protection operational requirements
  - … and the magnetic diagnostic can be non-fault tolerant.
  - The sector being commissioned must be functional …

- Parameters of the pulse schedule affect the desired interlock behavior.

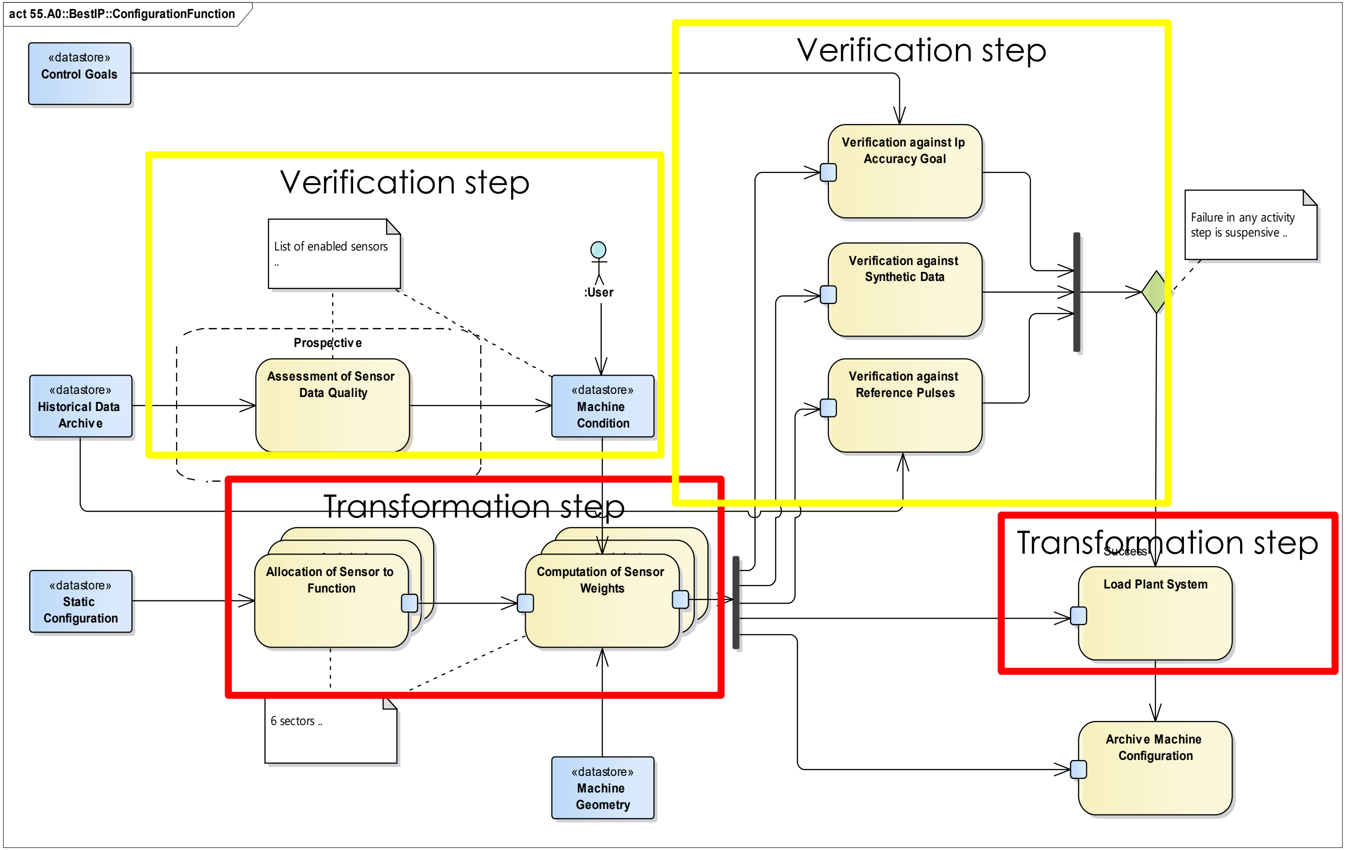
Configuration of plants at ITER (SUP)



Configuration of plants at ITER (SUP)

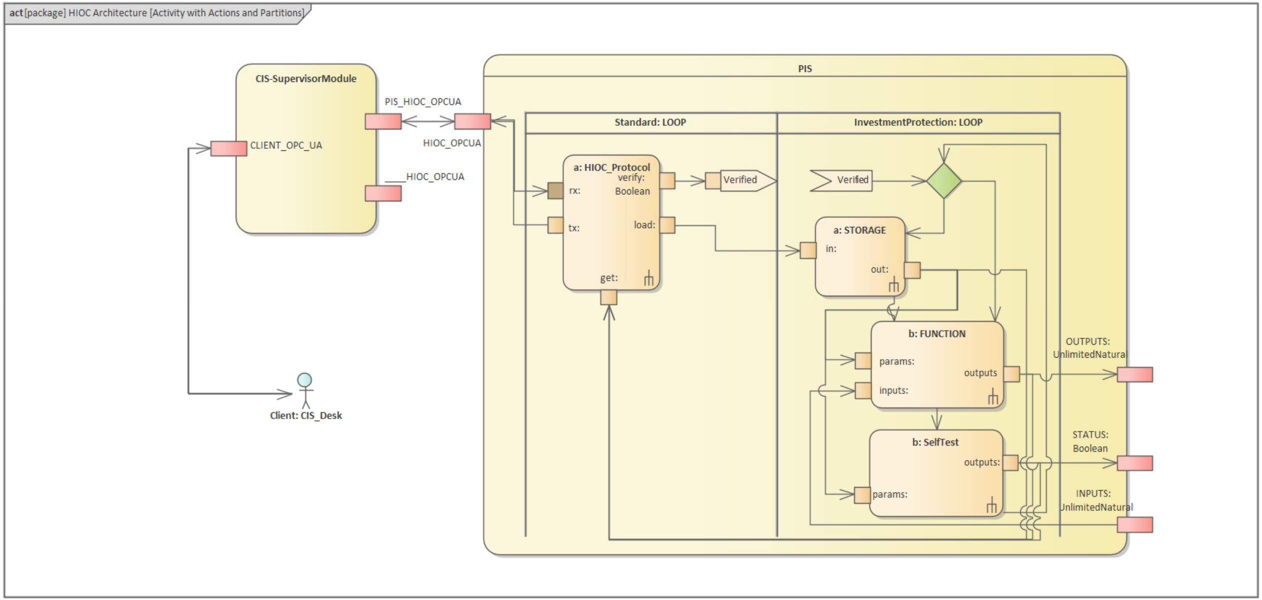


Configuration of plants at ITER (SUP)



Configuration of CIS (HIOC protocol)

- High Integrity Operator Commands – application layer protocol, built to IEC61508 black channel principles. Standard FMEA IEC61784: functional safety fieldbus.
- Measures: controller & function authentication, sequence number, timeout, feedback messages.
- Guarantees (3-step verification process):
  - Controller identify being modified is as intended by the operator; the function being modified is as intended by the operator; the value being changed is as intended by the operator .



Interpretation of IEC61508 goals

- Analyzed IEC61508 goals w.r.t. inv. protection parameters during integrated operation, integration points identified with SUP.
- SUP classified as T3 support tool – can affect the execution of a PIS; must assess risks & define coherency to development process.

SUP

1. Execute workflows consisting of verification/transformation steps.
2. Log inputs/outputs/roles per workflow per step relating data-source to final loading of parameters to PIS.
3. Implement verification/transformation steps at various levels of integrity.
4. Digitally sign outputs with hash.

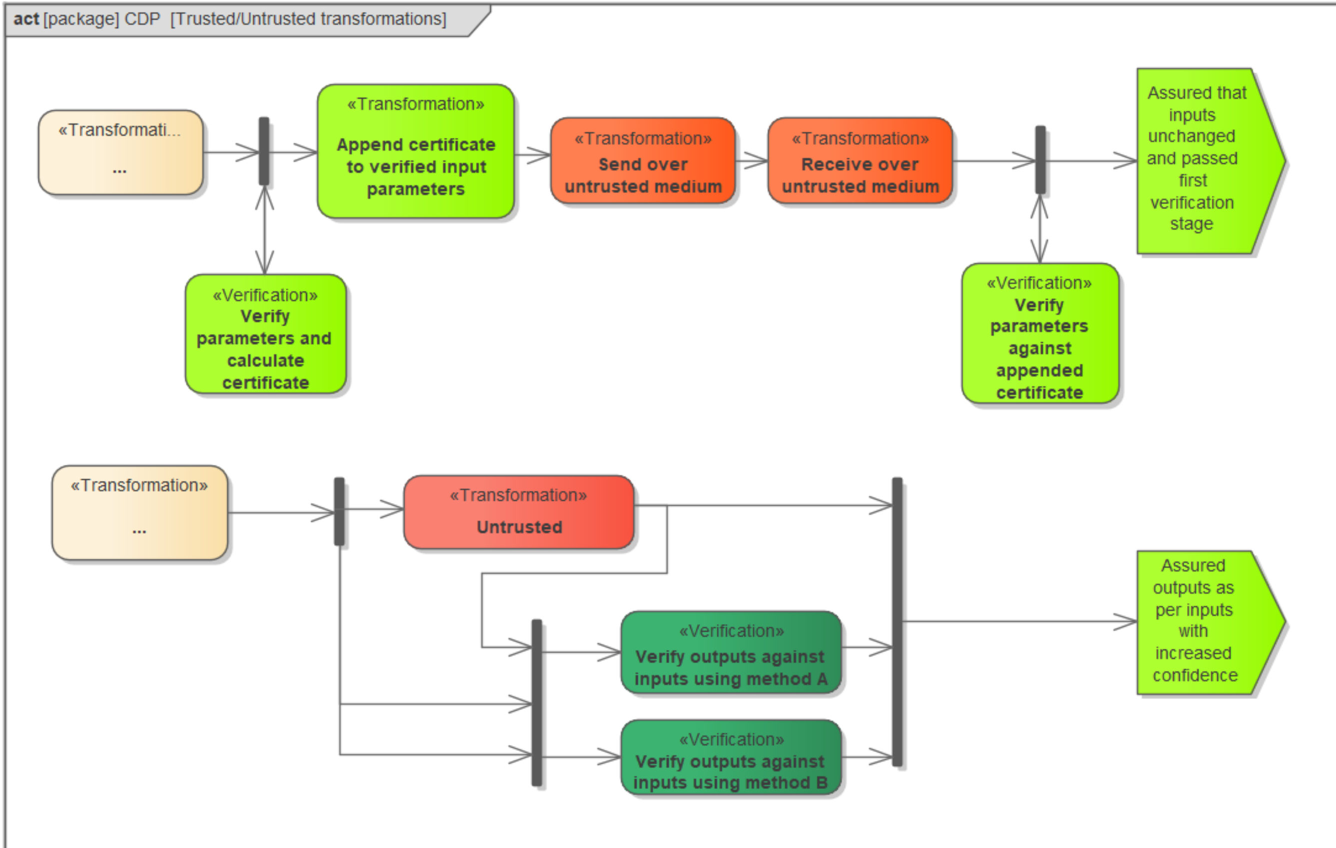
CIS

1. Mask parameter change of PIS at inappropriate time.
2. Operate related interlocks to a state where the PIS can be modified.
3. Transfer the hash from SUP to PIS with HIOC.
4. Issue unique Controller IDs and Function IDs to PIS as per HIOC to be used in configuration process.
5. Log hash, seed to link the parameter change request to a workflow execution in SUP.

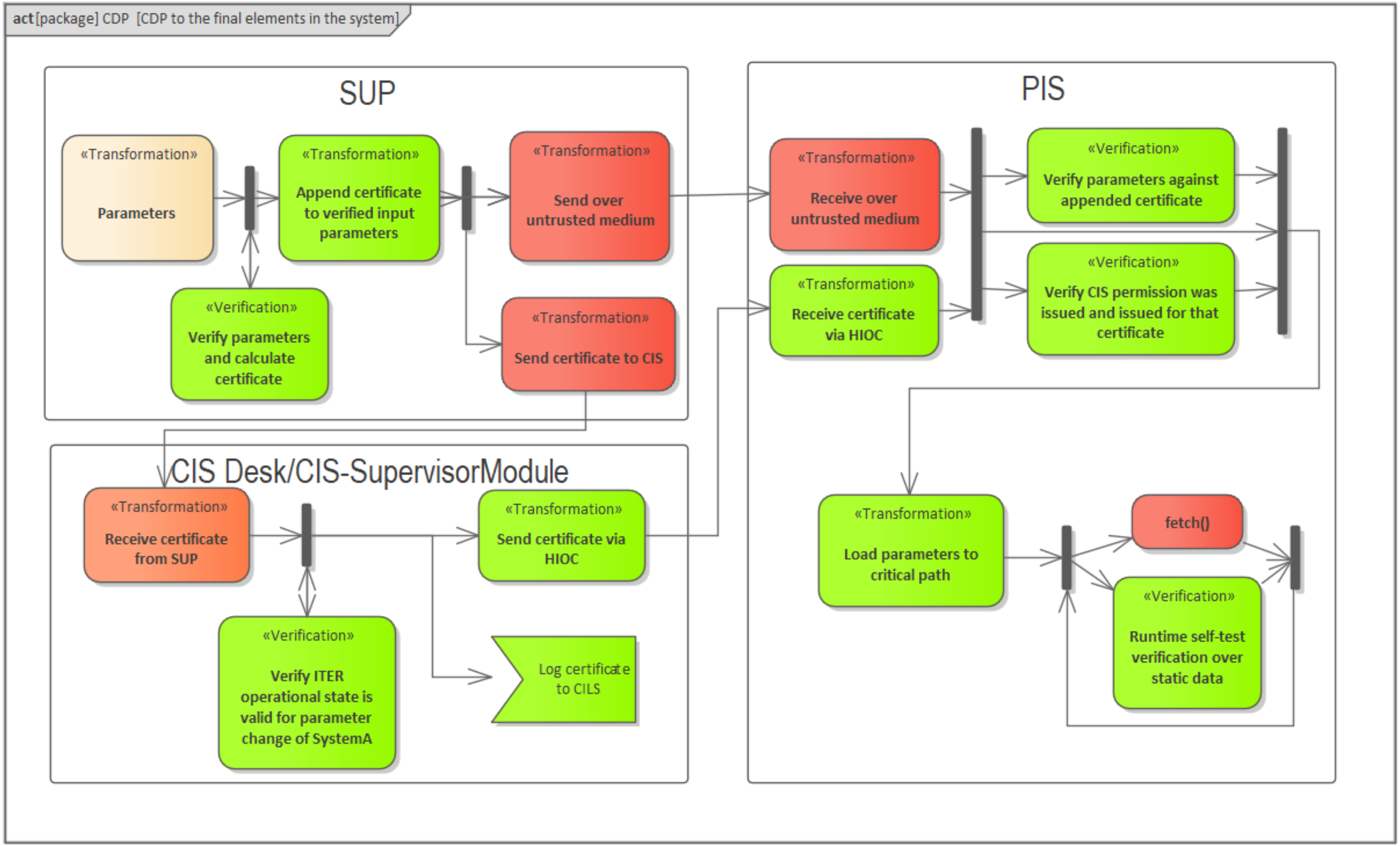
PIS

1. Define workflow requirements from a risk analysis on its configuration needs.
2. Define integrity levels for SUP transformation and verification steps.
3. Provide an interface to mask parameter changes at inappropriate times with a HIOC function.
4. After unmasking set target function to unavailable.
5. Provide run-time verification over final parameter storage (depending on risk & technology) and aggregate into its status flag.

Step integrity in a workflow



SUP/CIS integrated configuration workflow



Conclusion

- Demonstrated approach for integrated configuration of ITER investment protection systems that is compliant to IEC61508.
  - Approach solves the parameter coupling issues typical to tokamak operation, can cope with any parameter stream.
  - Configuration process fully auditable plant to data source.

- IEC61508 is goal based standard, there is no compliance per-se.
  - Why is IEC61508 asking for this? What is sufficient & necessary to meet the goal.

- Investment protection does not have the same stakeholders as safety.

- In the future we plan to roll out across all plants:
  - Implementation of HIOC for PLCs is readily available as a user library.
  - Implementation on FPGAs shall be available for LabView and possibly VHDL implementations.
  - SUP CVVF engine is being developed => integrated demonstration starting with the ITER magnetic diagnostic.