Ontology-based Requirements Validation

Result of Catalogue of System and Software Properties (CSSP)

The ontology (alone) is a static Object-Oriented Model with structural restrictions: requirement boilerplates, system model, …

SPARQL queries can discover problematic cases regarding the requirements, the system model and the interaction between them

SPIN allows SPARQL queries to be stored within the ontology:

- **Rules** (fill-in the gaps, repair ontology)
- **Constraints** (check invariants): Check incompleteness, inconsistency of requirements / system model

Advantages: Transparency, Extensibility, Reusability

Price to pay: Ontology Engineer in the loop of requirement specification

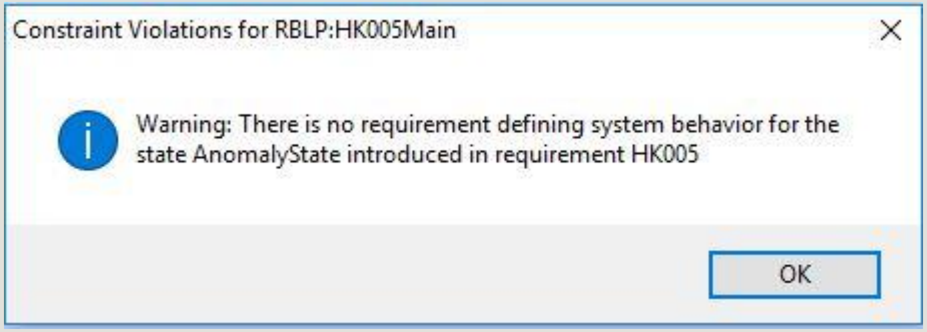
Checking Requirements incompleteness
System States not covered

Code	Requirement description
HK-005	A Housekeeping subsystem shall have the following states: NOMINAL, ANOMALY, and CRITICAL FAILURE.
HK-006	In NOMINAL state, the subsystem shall perform correctly.
HK-008	The subsystem shall enter the CRITICAL FAILURE state, after MAX seconds in ANOMALY.
HK-009	In CRITICAL FAILURE state, the subsystem shall contact the EPS and demand a restart of the malfunctioning subsystem.
HK-010	During NOMINAL operation, the subsystem shall be contacted to retrieve engineering data.

HK-005 defines 3 states for Housekeeping subsystems

- Behaviour in NOMINAL and CRITICAL FAILURE are covered by requirements
- ANOMALY state is not covered

SPIN constraint at CSSP:Requirement


Constraint Violations for RBLP:HK005Main

Warning: There is no requirement defining system behavior for the state AnomalyState introduced in requirement HK005

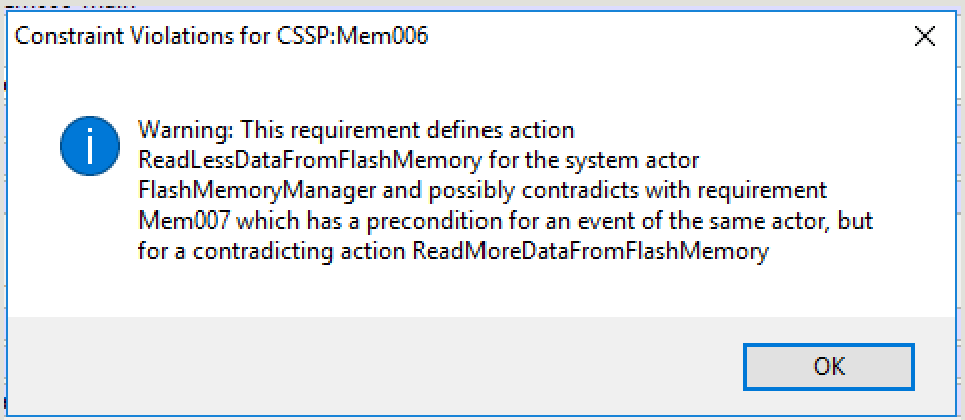
Checking Requirements Inconsistency
Contradicting Actions

Code	**Requirement description**
Mem-006	For the same read request, the number of attempts by the Flash Memory Manager to read data from the flash memory shall have a value **not larger** than the parameter MAX_FM_READS.
Mem-007	If the number of attempts by the Flash Memory Manager to read data from the flash memory **exceeds** MAX_FM_READS, the read operation shall be abandoned and a failure shall be reported.

Mem-006 and Mem-007 concern contradicting actions

- Mem-006 says that read attempts should not exceed limit
- Mem-007 says what happens when read attempts exceed limit

SPIN constraint at CSSP:Requirement



Constraint Violations for CSSP:Mem006

Warning: This requirement defines action ReadLessDataFromFlashMemory for the system actor FlashMemoryManager and possibly contradicts with requirement Mem007 which has a precondition for an event of the same actor, but for a contradicting action ReadMoreDataFromFlashMemory