Catalogue for System and Software Properties - CSSP

The CSSP introduces a model-based specification approach in the System & Software Development Lifecycle, for the early discovery and resolution of design correctness and consistency issues. The ultimate aim is to reduce the high cost of corrective measures applied in the late phases of the lifecycle.

According to the current industrial practice, the system and software requirements are conditions or capabilities specified in natural language. Each requirement has to be met by the system or a system component under design, in order to solve a problem or to achieve an objective. Requirements can be formally captured by one or more properties, which constrain the structure and the behaviour of the system under design to ensure that the corresponding requirements are properly covered. Within the CSSP approach, design correctness and consistency is achieved through the enforcement by construction and when needed the formal verification of design models against the properties derived from the requirements. The used design models are abstract representations of the real world “physical” system. Properties are verifiable only if they refer to entities and events given as identifiable elements of such a model. Only the model elements representing valid entities for the current phase of the development process may be used. Therefore, the CSSP approach can be applied to different abstraction levels of design along the development lifecycle (e.g., system, avionics, software). The consistency between the properties specified at a particular level will have to be ensured, as well as the preservation of the already established properties at the lower abstraction levels. Finally, the allocation of properties at the software level takes place over a model of the software component architecture. In addition to external interfaces, component (type) definitions must comprise information about their behavior.

Specification of requirements is based on a Catalogue of Requirement Categories per abstraction level that guides the engineers throughout the requirements decomposition and their coverage check. The Catalogue comprises boilerplates, which are requirement patterns with placeholders for entities mapped to a concrete semantic model. Such a model is encoded in the CSSP Ontology that records all logical relationships and facts for a system’s domain. This is an aid to avoid indeterminate references, to validate specifications by automated reasoning and can capture implicit assumptions that have to be made explicit to ensure verifiability of the requirements.

The systematization of the properties’ formalization is based on a natural-like pattern language with implicit formal representations for the properties. Patterns are an aid to capture properties, in terms of events and state variables of a design model in the BIP (Behaviour-Interaction-Priority) language. In the underlying theory, a formal architecture encodes a solution to a coordination problem, for how to enforce a characteristic property. A set of reusable formal architecture styles was introduced, thus having provided a taxonomy of enforceable properties. The CSSP tool implements property-preserving BIP model manipulations to enforce the properties on a BIP model. All relevant information to build the BIP model is retrieved from the CSSP Ontology. The model can be used for simulation and all verifiable properties can be model checked by transforming it into the input language of the nuXmv model checker. The CSSP process and tool framework have been successfully applied to a set of requirements from the software Requirements Baseline of the Sentinel 3 mission provided by Thales Alenia Space.