Practical formal validation method for interlocking or automated systems

Marc Antoni
SNCF
Infrastructure Direction

Abstract—**Today, a main question is to answer to the following problematic: have we recognized that for software, the delivery of absolute numerical safety targets is considered to be impossible, and the methods contained in the CENELEC standard produce a "probability" that certain (unsafe) failure rates will be archived rather then an absolute assurance? We know that checks before putting safety signalling facilities into service as well as the results of tests are essential but time consuming without guaranty of exhaustiveness in particular for the case of computerised equipments. In the context of greater economic constraints and increasing complexity of computerized tools, the capacities of the classic approval process are today attained. We see in actual practice a reduction of the validation cover rate and more and more numerous unsafe failures as results. This paper assumes that it is possible in practice to give an exhaustive formal proof that the "functional" of the signalling application (functional "white box") is safe in the context of use (over-system). The presented method makes it possible, after a rigorous and cost effective design, to validate formally the "functional" software of critical computerized systems. The aim of our project was to provide the SNCF (today for delegated infrastructure manager, and tomorrow for rolling stock departments of railway undertaker) with an operating method for the formal validation of critical computerized systems, especially for the Interlocking and ETCS/ERTMS systems. A formal proof method by assertion, applicable to these critical systems, which covers equally the specification and its real software implementation, is presented in this paper. With the proposed method and its associated tools we completely verify that the system follows all safety properties at all time and does not show superfluous conditions: it replaces the platform checks and is in accordance with the existing SNCF testing procedures. The advantages are a significant reduction of testing time and of the related costs, an increase of the tests cover rate (deterministic safety vs. probabilistic safety), The paper assumes that the formal methods mastery by infrastructure engineers is a main key to prove that, during the life of the system, more safety is not more expensive.**

Anomaly detection in event-based manufacturing systems using model generation

Dawn Tilbury
Mechanical Engineering Department
University of Michigan

Abstract—**Discrete manufacturing systems commonly produce streams of events – parts arrive, machines start and finish, etc. With dozens of concurrent processes, these events do not have a well-defined order. Faults and other anomalies may manifest themselves in these data streams, but not be visible to even an expert observer. This presentation describes a method for detecting anomalies in streams of event data, for systems which do not have a pre-defined formal model. Commonly-available information about the system is required as input to the method (e.g., which events are associated with which processes and resources). Since it is not known whether a formal model exists that can accurately characterize the manufacturing system, the method builds a set of models, thereby allowing uncertainty about the "true" behavior of the system to persist through the anomaly detection process. The performance of each model in the set is evaluated based on known "good" and "bad" streams of events; new streams are scored using a weighted average of the individual model's scores, based on whether each model accepts the new stream. The method has been applied to a Ford machining line to find an anomaly associated with a gantry incorrectly waiting for a machine to become available.**

GENESYS – A generic architecture for embedded control systems

Hermann Kopetz
Vienna University of Technology

Abstract—**Recognizing the strategic importance of embedded computing and control systems for industry and society, the European Commission formed, together with industry, academia, and national governments, the European technology platform ARTEMIS (Advanced Research and Technology for EMbedded Intelligence and Systems) in 2004. It is one goal of ARTEMIS to develop a cross-domain embedded system architecture, supported by design methods and tools, to significantly improve the functionality, dependability, and cost-effectiveness of embedded systems. The GENESYS (GENeric Embedded SYStems) project, carried out by a consortium of twenty industrial and academic partners coming from different embedded system domains, developed a blueprint for such an architecture that should be applicable in the control-system domain as well as in the multimedia domain. This blueprint (GENESYS) has been strongly influenced by the concepts of and the experience with the time-triggered architecture. It is the objective of this contribution to give an overview of the cross-domain architecture GENESYS.**