Workshop on

Software Change Management and Approval Processes for Safety Critical Applications

Søhuset Conference Center in Hørsholm, 20 August 2014

The Danish National Safety Authorities for railways, the Danish National Railway Infrastructure Manager and the Technical University of Denmark welcomes you to this workshop on Software Change Management and Approval Processes for Safety Critical Applications.

Within the Danish railway, a need for formalizing software change management for safety critical applications has been identified. The Danish National Safety Authority (NSA) for railways together with the Danish National Railway Infrastructure Manager (Banedanmark) are therefore currently investigating existing strategies for managing software changes in safety critical applications in the railway domain and in other similar domains such as biomedical systems and nuclear plants.

The Technical University of Denmark (DTU) is supporting the initiative and has organized a workshop with guest speakers possessing relevant expertise within nuclear power, space missions and railways. The guest speakers will provide insights and inspiration that can be used to form a basis for a dialogue between the different actors in the railway domain.

The objective of the workshop is to evaluate the relevance of experience and research from different safety critical domains concerning software change management. Furthermore it is the objective to determine whether the experience and research represents a basis for further studies into practical application of formalized software change processes that could ultimately lead to criteria of self-management of software changes in the railway sector.

The workshop is arranged as a dialogue between the main actors in the railway domain and other relevant sectors, and will thus facilitate active participation and knowledge sharing among the participants. The results obtained at the workshop will inspire future research initiatives.

Agenda

08:30-09:00	Registration and breakfast buffet.
09:00-09:30	Welcome.
09:30-10:10	Development and Maintenance of Software for Space Missions. *Poul Hougaard, Senior Analyst at Terma A/S, Denmark* *Jan Storbank Pedersen, Senior Software Engineer at Terma A/S, Denmark*
10:10-10:30	Questions and discussion.
10:30-11:00	Break.
11:00-11:40	Developing Maintainable Safety-Critical Software in the Nuclear Industry. *Alan Wassyng, Director, McMaster Centre for Software Certification, Canada*
11:40-12:00	Questions and discussion.
12:00-13:00	Lunch.
13:00-13:40	On Validating Software at Layout Changes in Interlocking Systems. *Alessandro Fantechi, Professor at University of Florence, Italy*
13:40-14:00	Questions and discussion.
14:00-15:00	Discussions in groups.
15:00-15:30	Break.
15:30-16:25	Presentation of group work and discussions & wrap up in plenum.
16:25-16:30	Closing.

Developing Maintainable Safety-Critical Software in the Nuclear Industry

Alan Wassyng, Director, McMaster Centre for Software Certification, Canada

The talk will present an approach that was used successfully in the nuclear industry in Canada to developing safety-critical software for the Darlington Shutdown Systems. One of the key attributes of the methodology was that it be maintainable in the sense that changes to functional behaviour and constant setpoints should not adversely affect the safety and dependability of the system. The methodology included an extremely rigorous approach, so that requirements are described in a mathematically precise notation, and the implementation is not only tested against requirements, but mathematically verified as well. This approach was primarily manual with some support from tools such as theorem provers (PVS). The talk will also discuss extensions that are now possible with modern analysis techniques and tools, as well as some indication of the path ahead, since the Darlington Shutdown Systems are to be refurbished over the next few years.

Re-certification at Reconfiguration: The Case of Railway Interlocking Systems

Alessandro Fantechi, Professor of Computer Science Foundations at School of Engineering of University of Florence, Italy

Railway signalling systems exhibit a long service life, that can span over several decades. During their life, different (expected or unpredictable) events such as partial failures, service improvements or increases, and so on, may ask for a reconfiguration of the system. The typical example is an interlocking system that rules the traffic in a station: the addition of a new platform with new tracks to cope with traffic increase requires an addition to the implemented safety rules. With computerized systems, this reconfiguration amounts to a change somewhere in the software code. Since the running code is no more the certified one of the first installation, re-certification is mandatory for assuring safe operation. In the case of a turnkey system provided to an infrastructure company by a manufacturer, reconfiguration and re-certification may ask for the intervention of the manufacturer, with obvious vendor lock-in problems, especially in the long run.

In this talk, we will discuss, in reference to interlocking systems, to which extent such re-certification is needed and how can it be addressed, in accordance with EN50128:2011 guidelines. In particular, we will consider how formal methods can help at this regard. Although inspired by interlocking systems, the discussion can be extended to any topologically configurable system, hence covering other safety-critical signalling systems as well.

Development and Maintenance of Software for Space Missions

Poul Hougaard, Senior Analyst at Terma A/S, Denmark
Jan Storbank Pedersen, Senior Software Engineer at Terma A/S, Denmark

Terma A/S has been involved in space projects for more than 35 years. This includes all aspects of development and operation of scientific satellites. Terma has developed space software for numerous missions, following processes and standards required by the European Space Agency (ESA). These are characterized by a number of standards for software development and software product assurance (ECSS-E-ST-40C, ECSS-Q-ST-80C), but also by the fact that the customer (ESA) wants to control the actual development. The development standard prescribes a tailoring of the development, based on the software criticality, where increased criticality implies additional development activities and documentation.

Realising that it is not possible for developers to avoid all problems, the ESA standards for some types of software require the use of 'independent software verification and validation' (ISVV), depending on the software criticality level. The rationale is that by performing verification and validation by an entity, which is independent from the development organisation, focus for the verification and validation process will be orthogonal to the development focus. Also the ISVV process is tailored according to the characteristics of the software. The ESA ISVV process is described in a handbook, of which the main points will be covered at the workshop.

The software maintenance process is also detailed in the standards, and covers aspects related to software change management.

Workshop Location:

Søhuset Conference Center, Venlighedsvej 10, 2970 Hørsholm.

Link to the home page of Søhuset: http://soehuset.dk/
There is free parking close to the entrance of Søhuset.
Public transport: Bus 173E goes from Nørreport Station directly to Søhuset. Bus 150S goes from Nørreport Station to Hørsholm Kongevej, 5 min. walk from Søhuset.
Busplans can be found here: http://www.moviatrafik.dk/dinrejse/pages/dinrejse.aspx

Workshop Organisation Committee:

Marianne Clod Zauner, Trafikstyrelsen, MAZ@trafikstyrelsen.dk
Claus Lund Nørgaard, Banedanmark, XCSLN@BANE.dk
Bjarne Kjær Ersbøll, DTU Compute, Danmarks Tekniske Universitet, bker@dtu.dk
Anne E. Haxthausen, DTU Compute, Danmarks Tekniske Universitet, aeha@dtu.dk