Zertifizierung und modellgetriebene Entwicklung sicherer Software (ZeMoSS 2012)

Michaela Huhn [1], Stefan Gerken [2], Carsten Rudolph [3]

[1] TU Clausthal
Julius-Albert-Str. 4, 38678 Clausthal-Zellerfeld
Michaela.Huhn@tu-clausthal.de
[2] Siemens AG
Ackerstr. 22, 38126 Braunschweig
Stefan.Gerken@siemens.com
[2] Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstraße 75, 64295 Darmstadt
carsten.rudolph@sit.fraunhofer.de

Mit dem vielfältigen Einsatz softwaregesteuerter Produkte und Infrastrukturen in unserem Alltag wachsen die Software-Qualitätsanforderungen, insbesondere in den Bereichen funktionale Sicherheit und Informationssicherheit. In der Luft- und Raumfahrt, der Energieerzeugung und im Schienenverkehr, aber auch in der Medizintechnik, der Automobiltechnik und bei mobilen Systemen sind Zertifizierung und der Nachweis der Sicherheit kritischer Systeme und softwarespezifische Sicherheitsnormen international etabliert und bindend. Zwei aktuelle, domänenübergreifende Herausforderungen bei der Entwicklung sicherer Software sollen im Workshop adressiert werden:

(1) Modellgetriebene Entwicklung eingebetteter Software wird in der Industrie immer wichtiger und in ihren Grundlagen für höhere Sicherheitsanforderungsstufen seit langem in Sicherheitsnormen als dringend empfohlen klassifiziert. Da Normen aber immer nur die etablierten Regeln der Technik darstellen, entsteht für den Hersteller mit jedem Schritt hin zum erweiterten Einsatz modellgetriebener Methoden und Werkzeuge die Herausforderung, dass diese im Zertifizierungsprozess neu akzeptiert werden müssen, selbst wenn noch keine normativen Aussagen zu ihnen vorliegen.

(2) Durch die zunehmende Vernetzung kritischer Infrastrukturen und die Anbindung mobiler Endgeräte entstehen neue Risiken aus der wechselseitigen Abhängigkeit von Informationssicherheit und funktionaler Sicherheit. Hier sind eine Integration von Safety- und Security-Prozess und neue Methoden gefragt, die eine verbindende Behandlung von funktionaler Sicherheit und Informationssicherheit in der Risikoanalyse, der Entwicklung und beim Sicherheitsnachweis unterstützen.

Der Workshop soll den Austausch über gewonnene Erfahrungen und neue Ansätze zur Entwicklung zertifizierbarer, sicherheitskritischer Software und insbesondere zu den Herausforderungen Modellgetriebene Entwicklung und Integration von Informations- und funktionaler Sicherheit zwischen Teilnehmern aus Industrie und Forschung fördern.

analyses with respect to development-related and evolution-related issues. Moreover, the concept is to a large extent constructed tool-independent as both artefacts to analyse and the related annotations are kept in an external repository.

To analyse the information specified by these annotations we can export them from Matlab/Simulink into our external framework and link them with representatives of the Simulink model. We have exemplified one analysis of meta information with the help of annotations in Section 2.3.

Up to now, we are able to import Simulink models and requirements into the external framework. Furthermore, we implemented the annotation concept for Simulink models. However, in order to establish traceability using the annotation concept we have to integrate annotations into the other artefacts as well. Last but not least the annotation concept is currently just a prototype. In order to put the concept into practice it has to be extended and restructured to make annotations more expressive. For instance, annotations are currently appended to blocks in a linear, i. e. flattened, manner. That way information about relationships among themselves cannot be captured and hence, we loose information compared to the free text approach where information can be grouped textually. This requires a deeper analysis of the kinds of information to be annotated and a different way to specify them in a user-friendly manner. After restructuring annotations a graphical user interface will be needed to support the engineers during evolution of the product line.

Acknowledgement

This work was funded, in part, by the Excellence Initiative of the German federal and state governments as well as Daimler AG. Moreover, we would like to thank Christian Dziobek, Thorsten Stecker, Uwe Spieth and the anonymous reviewers for useful inputs and constructive feedback about the presented concepts.

References

[ADS02] F. Altheide, H. Dörr, and A. Schürr. Requirements to a Framework for Sustainable Integration of System Development Tools. In *EuSEC '02*, pages 53–57, 2002.

[AUT] AUTOSAR. AUTOSAR AUTomotive Open System ARchitecture. `http://www.autosar.org/`.

[BDT10] M. Biehl, C. DeJiu, and M. Törngren. Integrating safety analysis into the model-based development toolchain of automotive embedded systems. In *LCTES '10*, pages 125–132, 2010.

[BFH+10] M. Broy, M. Feilkas, M. Herrmannsdoerfer, S. Merenda, and D. Ratiu. Seamless Model-Based Development: From Isolated Tools to Integrated Model Engineering Environments. *Proceedings of the IEEE*, 98(4):526 –545, April 2010.

[dSp] dSpace. Target Link. `http://www.dspace.com/en/ltd/home/products/sw/pcgs/targetli.cfm`.

[EFa] Eclipse-Foundation. EMF - Eclipse Modeling Framework. http://eclipse.org/modeling/emf/.

[EFb] Eclipse-Foundation. GMP - Graphical Modelling Project. http://www.eclipse.org/modeling/gmp/.

[EFc] Eclipse-Foundation. Xpand. http://www.eclipse.org/modeling/m2t/?project=xpand.

[EFd] Eclipse-Foundation. Xtext. http://www.eclipse.org/Xtext/.

[IC] IBM-Corporation. IBM Rational DOORS. http://www-01.ibm.com/software/awdtools/doors/.

[KCH+90] K. Kang, S. Cohen, J. Hess, W. Novak, and S. Peterson. Feature Oriented Domain Analysis (FODA) Feasibility Study. SEI Technical Report CMU/SEI-90-TR-21, ADA 235785, Software Engineering Institute, 1990.

[Mata] The MathWorks, Inc. Function Reference (MATLAB). http://www.mathworks.de/help/techdoc/ref/f16-6011.html.

[Matb] The MathWorks, Inc. Simulink – Simulation and Model-Based Design. http://www.mathworks.de/products/simulink.

[MD08] T. Mens and S. Demeyer. *Software evolution*. Springer, 2008.

[MPBK11] D. Merschen, A. Polzer, G. Botterweck, and S. Kowalewski. Experiences of Applying Model-based Analysis to Support the Development of Automotive Software Product Lines. In *VaMoS '11*, pages 141–150, 2011.

[MZV+03] P. Mulholland, Z. Zdrahal, M. Valasek, P. Sainter, M. Koss, and L. Trejtnar. Supporting the sharing and reuse of modelling and simulation design knowledge. In *ICE 2003*, 2003.

[PMT+10] A. Polzer, D. Merschen, J. Thomas, B. Hedenetz, G. Botterweck, and S. Kowalewski. View-Supported Rollout and Evolution of Model-Based ECU Applications. In *MoMPES '10*, pages 37–44, 2010.

[Som07] I. Sommerville. *Software engineering*. International computer science series. Addison-Wesley, 2007.

[SVSZ01] P. Steinbauer, M. Valasek, Z. Sika, and Z. Zdrahal. Knowledge supported design and reuse of simulation models. In *MATLAB 2001*, pages 399–406, 2001.

[TD] TU-Darmstadt. MOFLON. http://www.moflon.org/.

[TDH11] J. Thomas, C. Dziobek, and B. Hedenetz. Variability management in the AUTOSAR-based development of applications for in-vehicle systems. In *VaMoS '11*, pages 137–140, 2011.

[WDR08] F. Wohlgemuth, C. Dziobek, and T. Ringler. Erfahrungen bei der Einführung der modellbasierten AUTOSAR-Funktionsentwicklung. In *MBEFF '08*, pages 1 – 15, 2008.

[ZMV+03] Z. Zdrahal, P. Mulholland, M. Valasek, P. Sainter, M. Koss, and L. Trejtnar. A Toolkit and Methodology to Support the Collaborative Development and Reuse of Engineering Models. In *DEXA 2003*, pages 856–865, 2003.