Building an Experience Factory for a Model-based Risk Analysis Framework

Chingwoei Gan, Eric Scharf

Department of Electronic Engineering,
Queen Mary University of London
E1 4NS, United Kingdom
{chingwoei.gan, e.m.scharf}@elec.qmul.ac.uk

This paper introduces the CORAS[1] Experience Factory (EF), which is the first known application of EF in the field of model-based risk analysis. Risk analysis has long been recognized in the process, finance and engineering industries as an effective means of gaining an unambiguous understanding of the limitations of an asset or property at risk [Di02]. In fact risk analysis is now considered a prerequisite to deploying, as well as maintaining both new and existing services, especially when security is of high importance. With the increased reliance of modern businesses and corporations on IT-related services, we are witnessing new and increasingly more demanding requirements on the underlying infrastructure. However traditional risk analysis of security critical systems is performed on the basis of informal descriptions of the target of evaluation. Such an approach is prone to misunderstandings [St02]. Further, the growing complexity of today's systems urges the improvement of existing methods of analyzing systems and their security specification in order to increase the likelihood that all possible security threats are taken into consideration.

CORAS introduces an improved methodology for security risk assessment [Aa02, St02, Gu02, Iv02]. Its core innovation is on the integration of Unified Modelling Language (UML) based methodology and conventional risk analysis techniques - including Fault Tree Analysis (FTA), Failure Mode and Effect Criticality Analysis (FMECA) and Hazard and Operability study (HAZOP) - into a *model-based risk analysis framework*.

When risk analysis is performed using the CORAS framework, knowledge and experiences will be gained, computerized tools employed and numerous documents of different types produced by the risk analysis team. In the context of CORAS, this includes UML diagrams, textual report, tree diagrams, tables and guidelines. It is a non-trivial task when dealing with information of such volume and variety in a heterogeneous operating environment. Further, the risk management process is an elaborate process, involving both humans and computerized tools, and as such is prone to delays and errors. A system is needed which effectively manages, queries and reuses different types of risk analysis results according to a given assessment scenario.

[1] CORAS is a research and development project under the European Information Society Technologies Fifth Framework Programme (IST-2000-25031), to be completed by July 2003; website: http://www.nr.no/coras

A framework that attempts to operate within an organization and to realize the goal of organizational learning will require some measure of Knowledge Management (KM). We have decided to incorporate the concept of EF [BCR94] into CORAS. EF is an example of knowledge management approach initially designed for software organizations. In our work to carry out model-based risk assessment, we have found that an EF can be tailored and incorporated as part of our framework, for it can be beneficial for creating a learning organization even though the main subject of our project does not fall into the conventional category of software development.

So we adapted the EF concept to fit the needs in documenting and exploiting the risk analysis results, as well as to support the structured process of risk management. We adopted the *top-down approach* in building the CORAS EF, so any change will be driven and guided, *not* by experience, but by a set of best practices and the inherent organizational requirements. The result is an internet-enabled EF-driven *CORAS platform* that takes advantage of XML as the vehicle for data exchange, making it highly interoperable in a distributed environment that uses heterogeneous tools. One important ingredient of the CORAS EF is the CORAS Experience Packages (CEP). Basically the CEPs allow experience to be packaged in a systematic and structured manner thereby fulfilling our initial goals. Similar to the JCI EMS [Li02], the CORAS experience management system consists of only one package type, making it a specialized experience base, exclusively for risk analysis elements.

Though the EF approach seems like a good fit for CORAS, we have not incorporated the entire EF concept within our framework. One reason is that the EF/QIP approach remains a theoretical, abstract framework, which lacks explicit and easily applicable guidelines on implementation (as pointed out in [HSW98]). The time aspect is also a critical point, for instance the EF at NASA evolved over 15 years whereas our EF is supposed to be running within 6 months. Thus, our objective is to build a scale-down but functional EF, tailored to our specific organizational need within the shortest possible time-frame, without the overhead – both time and resources – that is normally required of an organization wishing to tap into the many benefits of EF.

References

[Aa02] Aagedal, J. Ø., Braber, F. den, Dimitrakos, T., Gran, B. A., Raptis, D., Stølen, K.: Model-based Risk Assessment to Improve Enterprise Security, 6th IEEE International Enterprise Distributed Object Computing Conference, September, 2002.

[BCR94] Basili, V. R., Caldiera, G., and Rombach, D. H.: The Experience Factory, Encyclopaedia of Software Engineering -2 Volume Set, pp. 469-476, 1994.

[Di02] Dimitrakos, T. et al.: Integrating Model-based Security Risk Management into e-Business Systems Development. 2nd IFIP Conference on e-commerce, e-business, e-government. Lisbon, 7-9 October, 2002.

[Gu02] Gustavsen, T.S., Houmb, S-H., Gran, B. A. Stølen, K.: Security Risk Analysis in e-Commerce, 7th Nordic Workshop on Secure IT Systems 2002.

[HSW98] Houdek, F., Schneider, K. and Wieser, E.: Establishing Experience Factories at Daimler Benz: An Experience Report, Proc. 20th Int'l Conf. on Software Engineering, Kyoto, May 1998.

[Iv02] Djordevic, I., Gan, C., Scharf, E., Mondragon, R. et al.: Model-based risk management of security critical systems. In Proc. Risk Analysis III, series: Management Information Systems, Volume 5, WIT Press, 2002.

[Li02] Lindvall, M., Frey, M., Costa, P., Tesoriero, R.: Lessons Learned about Structuring and Describing Experience for Three Experience Bases, Lecture Notes in Computer Science, 2001.

[St02] Stølen, K. et al.: Improving security through model-based risk assessment, Business CBSE Chapter 11, Kluwer Academic Publishers, 2002.