Manager at Catena Wireless Electronics, explained that at the start of a typical project they assist customers in translating their system requirements into a suitable IC architecture with agreed target specifications. After that process they take care of the design, layout and validation of the integrated circuit. At the beginning of this process it is crucial to describe and model at system level the performance of the final product. For this the company applied the SYSMODEL methodologies into one of its developments, where the complexity of integrating hardware and software requires a new tools approach: the SYSMODEL 'Synchronous MoC' and the 'Continuous Time MoC' to verify the systems performance with respect to the requirements. These two system-level modelling possibilities offer new ways to model hardware and software together, which is crucial for reducing time to market and increasing the chance of first-time-right designs.

Finally, the ForSyDe framework significantly profited from the development and testing in SYSMODEL, with ForSyDe-SystemC modelling libraries proving valuable for other European projects: iFest (Artemis) , CONTREX (FP7) and EMC2 (Artemis). Thus SYSMODEL had a huge impact in the development of ForSyDe, which is gaining more and more acceptance in both academia and industry, and the work of Novelda, DA Design and AuditData is documented in papers published after the completion of the project.

By increasing the level of innovation in SMEs over the whole design innovation cycle, SYSMODEL will stimulate sustainable economic growth.

1.3 SHIELD

By Josef Noll | Movation, Norway
Project: SHIELD (pSHIELD Jun 2010 - May 2011 & nSHIELD Sep 2011 - Dec 2014)

Challenge

European industries need measurable security, privacy and dependability (SPD), risk assessment of security critical products, and configurable and composable security. The business-based starting point for SHIELD focused on the impact of embedded systems in the years ahead and the security requirements expected from these Internet of Things systems.

Achievement

The core SHIELD platform is a middleware, prototypes, metrics and validation approach. The SHIELD methodology enables a business to significantly improve the SPD quality of embedded systems while addressing the specific industrial requirements, with both design and development of embedded security, privacy and dependability (SPD) possible via standardised design methods.

Figure 1: Measurable security, privacy and dependability (SPD) applied in various domains

The size of the project allowed expertise to be brought together, which had not previously been possible, and for prototypes in totally different application areas, even extended with unplanned application areas. Through SHIELD we have *(i)* achieved a de-facto standard for measurable security, privacy and dependability, *(ii)* developed, implemented and tested roughly 40 security-enhancing prototypes in response to specific industrial requests, and *(iii)* applied the methodology in four different domains, proving how generic the approach is.

Having piloted measurable and composable security in pSHIELD, the methodology was successfully applied by SHIELD in four business areas and has thereby contributed to solving the specific societal challenge of measurable Security, Privacy and Dependability. With methodologies for measurable security far from being standard, new ground had to be explored and this led to the development of around 40 prototypes that enhance security, ranging from 'secure boot', 'trusted execution environments' and 'adaptable radio interfaces' to 'different implementations of middleware for measuring security'. The methodology for composable security provides the configuration needed to fulfil a security requirement.

Business Impact

The Biometric Face Recognition System by Eurotech is a good example of business impact in this privacy-compliant, IP-based recognition system that detects human faces and processes them automatically, monitoring the transit of people through checkpoints and access passages in restricted areas. Another is the Norwegian Centre of Excellence on Smart Grids, where measurable SPD was applied to monitor and control energy consumption due to the increasing use of car recharging at the same time as house heating (in weekend houses), which overloads the grid. The energy consumption profile shows what equipment people own and the SHIELD methodology keeps this information private and secure and thereby promotes the business model of the privacy-aware smart-grid provider. Another example addressed the need of the transport domain. Composable security with SHIELD can enable trains to continue operating, albeit at a reduced speed, if one signal is not working but the track (in a station) can still be observed.

The demonstration of a novel software concept for unmanned aerial vehicles (UAV/UAS or Drones) has proved to be a real breakthrough not specifically targeted when SHIELD began. Alfatroll's IQ_Engine, a search-engine based steering system for UAVs, was successfully prototyped together with the OMNIA communication unit of Selex ES. This has prompted specific requests from industry to use UAV for unmanned monitoring at sea (oil and fish) and for the power-line infrastructure in Norway. The project also demonstrated that embedded systems can be configured in compliance with the security, privacy and security goal of the operator of the system as well as enabled the introduction of measurable and composable security in a variety of market segments, with a large number of technology prototypes supporting the specific SPD requirements of industrial applications in the respective domain. These prototypes will help our partners to stay competitive and gain market share, something that Eurotech and Seek and Find have already experienced with their products. In terms of new products in existing markets, SHIELD has provided measurable security as a dimension to the world of embedded devices, thereby focusing more on enhancing products rather than creating new ones. However, the UAS collaboration has pushed the products closer to the market, and attracted customers looking for autonomous solutions.

The impact of security will only grow and in the shift from Internet to the Internet of Things and cyber-attacks on sensor networks, prevention is a key issue. ABI Research addressed the presence of mainstream M2M solutions within critical information infrastructure such as utilities, healthcare and finance, and estimated a market volume of USD 752 million in 2017. The market need for measurable SPD could run up to more than 5 billion euros.