COMPACT

Faster, more efficient software through automation

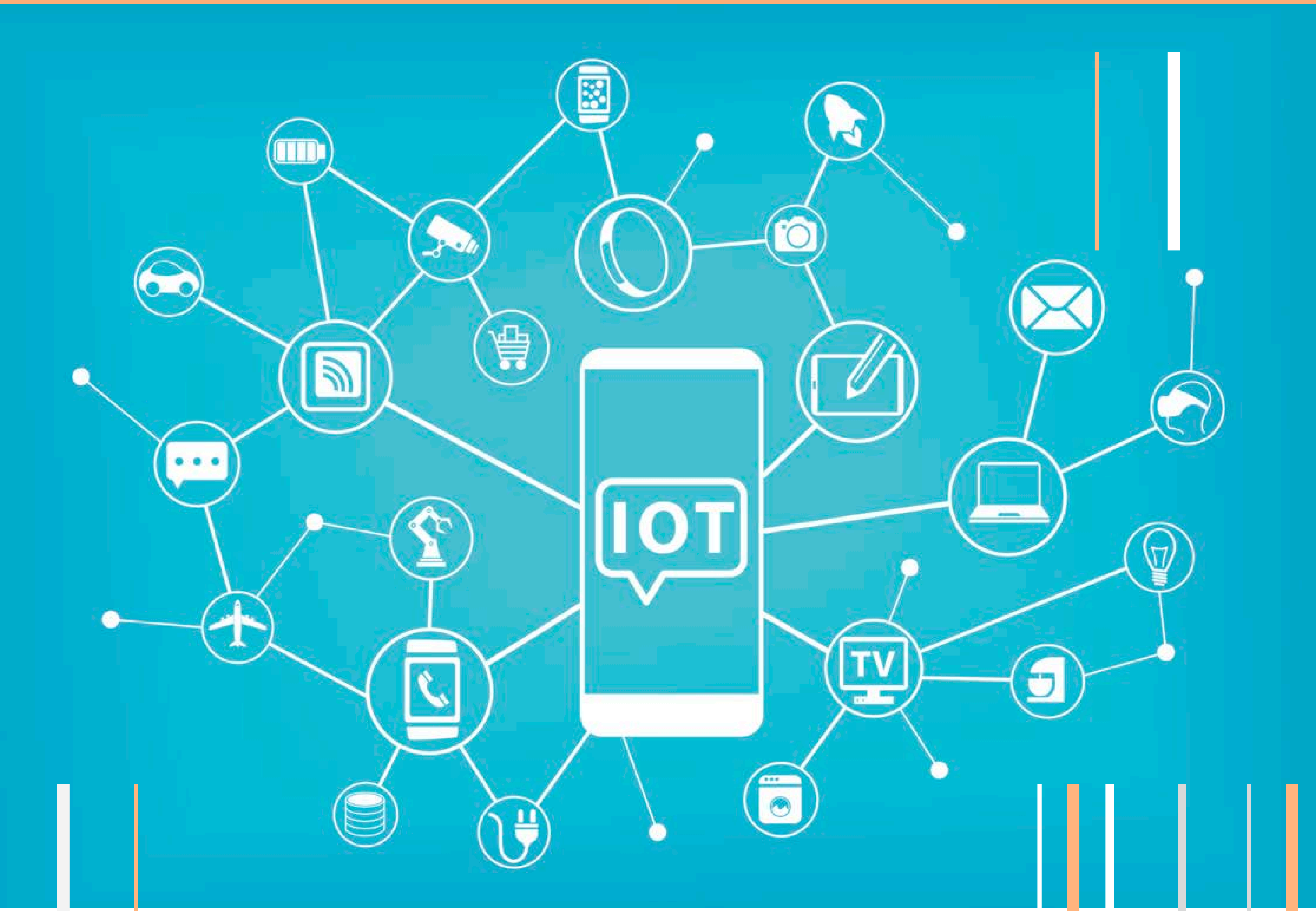
Success story

From industrial automation to healthcare, Internet of Things (IoT) has impacted every aspect of our lives. However, the cost pressure of making IoT devices as smart, cheap and energy efficient as possible affects both manufacturing and design costs, with software design accounting for around 45% of the overall System-on-Chip (SoC) development effort. Fast and efficient software development is thus a key enabler of future growth within the IoT domain.

Within the ITEA project COMPACT (Cost-Efficient Smart System Software Synthesis), 15 partners from Austria, Finland and Germany focused on enhancing IoT software by automating code generation from abstract models, thereby boosting productivity and reducing both manufacturing costs and performance issues. It also reduced embedded software costs in semiconductor-based products by selecting the best solution from multiple options based on system vision.

Automatic software generation based on models

COMPACT's technology focused on tiny IoT devices, like those similar to Arduino. It mainly dealt with low-level software components such as drivers and hardware



abstraction layers (HAL). The main goal was to make software for these small devices, where the hardware is limited in power and size because it has to be affordable. COMPACT sought to create a connection between how a device is modelled and how its software is developed. The solution is automatic software generation based on models, for which a complete chain of tools was developed.

Based on requirements, concepts and use cases from industrial partners, the project achieved major innovations in modelling, tooling & automation and analysis & optimisation. An IoT Platform Modelling Language (IoT-PML) defines the overall modelling approach and features various meta models for non-functional properties, specific functional behaviour and firmware configuration. This combines previously isolated modelling approaches and provides a foundation for the structuring and formalisation of the domain. For automatic code generation, various generators, libraries, plugins and tools for highly automated IoT software development were created and integrated into a framework. Static and dynamic methods can then analyse software properties (such as timing, power and memory footprint) and optimisation methods. Plugins enable software transformation to ensure that the generation overhead remains within an acceptable range.

Three demonstrators were also developed to illustrate the project's relevance to multiple applications: smart sensors (model-based code generation workflow and virtual prototype-based software analysis), vehicle detection (use of IoT-PML in the Enterprise Architect tool) and an IoT sensor device (model creation and support for system architecture and functional interface refinement). As a contribution to standardisation, a COMPACT extension to the IP-XACT standard was finalised in Accellera and submitted to the Institute of Electrical and Electronics Engineers (IEEE). About 90% of the proposals have been included in the new standard.

Faster and more compact than human-written code

In terms of results, COMPACT exceeded expectations by generating highly efficient software, up to 90% of which is faster and more compact than human-written code. This results in less memory usage, less energy consumption and lower latency. Depending on the degree of generation, a 20-70% reduction in

COMPACT exceeded expectations by generating highly efficient software, up to 90% of which is faster and more compact than human-written code.

Project start
September 2017

Project end
December 2020

Project leader
Wolfgang Ecker
Infineon Technologies AG,
Germany

More information
https://itea4.org/project/compact.html

software development costs can be expected without any performance loss or memory footprint of the software code. As designers can produce around 2,000 lines of code per year and a person-year costs roughly EUR 150,000, COMPACT predicts that each line of generated code will have a value of 75 euros. Generators for a new device family therefore pay off with their first use.

As the project adopted an open software implementation for better dissemination, one of its key strengths has been broad exploitation by various channels. SME software tool companies have been able to create new tools while large semiconductor companies and system houses have created software more efficiently. This enables them to retain or expand their positions within the IoT for semiconductors market, expected to grow from USD 20 billion in 2017 (the start of COMPACT) to over USD 61 billion by 2024. SparxSystems Software GmbH, for instance, has built the base for cybersecurity modelling which is now part of the core product, enabling access to the aviation and space industry.

In addition, cybersecurity modelling is available as a separate solution, including a form of automation named ThreatGet (www.threatget.eu). This is an award-winning product: Report eAward (1st place), Constantius Award (1st place in the category of IoT) and a nomination for the State Award for IT Consultancy. Targeted customer domains include automotive, industry, critical infrastructure, space and more. SparxSystems Software GmbH has increased its workforce by five employees and two trainees and is in the process of strategically taking over another company in the IoT domain. Revenues have increased by 15% in this domain. Further strategic investments in the direction of model transformation down to Model2Code have resulted in additional research projects (Eureka Penta project ECOMAI and ITEA project GenerIoT). SparxSystems Software GmbH aims to provide a compilable, debuggable open-source Model2Code implementation for RUST (based on the MIT License) as this seems to be the next big thing in the embedded domain.

Similarly, Kasper & Oswald GmbH has presented its new COMPACT Crypto API (CCAPI) to several customers in the automotive and home automation domains and used parts of this in internal product development. Kasper & Oswald GmbH has trained two junior engineers to further extend platform support, one of whom is now moving to a full-time role in the company. The results of COMPACT also feed into two follow-up projects, DevToSCA and FreeSBee, both funded by the German BMBF.

Finally, Visy Oy's demonstrator of a vehicle model classifier and license plate recogniser is in use at four customer sites and they expect orders worth EUR 1.8 million for systems with technologies developed in COMPACT. The vehicle model recognition also led to vehicle colour recognition and is currently operational at 20+ customer checkpoints. More importantly, the newly developed computational technologies are an essential part of Visy Oy's offering to all customer sites, enabling more efficient edge computing.

The ITEA project GenerIoT and the PENTA project ECOMAI serve as vivid examples that use the research outcomes of COMPACT.

IoT to benefit our daily lives

As for the future, the project showed that automated model-based code generation works efficiently, which will encourage work to bring model-based code generation to the next abstraction levels, such as runtime systems and applications focused on digital signal processing (DSP). COMPACT also demonstrated the power of using AI for software optimisation in combination with code generation and compiler configuration.

The COMPACT project significantly benefits society by automating IoT software development, thereby reducing costs by 20-70%, enhancing energy efficiency, improving security and fostering industry growth. Its contributions to standardisation and technological advancements strengthen the IoT sector, opening new markets and research opportunities, in turn opening up new uses for IoT to benefit our daily lives.

More information

https://itea4.org/project/compact.html

Internet-enabled fraud has become a bit harder

Many aspects of our daily lives have moved to the internet – including the less pleasant aspects, like forms of frauds such as phishing or criminal financial transactions. To address this, the DEFRAUDify project decided to look into new data sources and advanced analytics.

Phishing attempts are annoying, but the 'spearphishing' variety is especially dangerous: these are handcrafted emails that contain lots of specific information elements that relate to the recipient, so they are very convincing. And now, with the advent of services like 'FraudGPT', it's even easier for cyber criminals to create those emails. Companies that want to be aware of these threats, want to know what the spearphishing 'attack surface' looks like: which key employees can be targeted and which information about those potential victims can be used by criminals? The DEFRAUDify 'cyber threat monitoring dashboard' collects this information and presents it to security officials of the company when needed. This is combined with information from the dark web that indicates whether the company is being discussed there. Advanced techniques like honeytokens, dark web crawlers and natural language processing are used to do this, developed by partners Almende, TU Eindhoven, CFLW Cyber Strategies and TNO. DEFRAUDify partner Web-IQ has included this solution in their portfolio, which has already raised considerable interest from their customers, especially the functionality that identifies dark web threat levels and trends. This has already been implemented a couple of times. They now know much more precisely what types of threats they need to anticipate.

Another area of internet-enabled fraud is criminal financial transfers. Cryptocurrencies are frequently used to collect ransomware payments, to evade taxes or to launder money. Lots of tools are already available to analyse cryptocurrency transactions, but some crucial points are missing. A special version of crypto transactions, known as 'Layer 2' or 'Lightning network' payments, evades normal analysis. Another crucial point is the interface between the 'normal' financial world and the crypto world: the Crypto Asset Service Providers (CASP). DEFRAUDify partners have created the CARE result: CASP Risk Estimation, whereby banks can easily assess how risky it is to accept transactions from crypto service providers. DEFRAUDify partner bunq (a fintech company) has defined the requirements for this solution, which is built upon results from partners NetSearch, CFLW Cyber Strategies and TNO. In their business, bunq is now much better able to assess risks for new customers who also use cryptocurrency transactions. The inherent explainability of the results is a distinguishing factor in the market. Partner BEIA will use the results to help the Romanian government fight tax evasion.

^ The DEFRAUDify 'cyber threat monitoring dashboard'

Besides the joint results outlined above, many more individual results were presented in the final review meeting on 18 September. The DEFRAUDify partners continue to exploit those results in the context of their product portfolio because the cyber world is constantly evolving. Any new tool that helps to detect or avoid cyber crime will create a reaction from the dark side: a new modus operandi, a new vulnerability, a new technology. So, while DEFRAUDify has taken an important step and the project is finished, the work continues.

More information

https://itea4.org/project/defraudify.html