Secure your IoT business model

How the US Department of Defense wants to protect critical information – and what German companies can learn for their IoT platforms.

Michael Kallus

It was a US agency that created the technical foundation for today's Internet. In the late 1960s, this agency brought researchers together who developed ARPANET (Advanced Research Projects Agency Network), which was the precursor for the Internet. The agency is DARPA (Defense Advanced Research Projects Agency). On behalf of the US Department of Defense, it invests in national security-related research projects and, in doing so, supports technical innovations in fields ranging from biology to microelectronics as well as unmanned aircraft.

Its tasks also include safeguarding critical infrastructure, such as hospitals or industrial systems, from cyber risks. For this reason, at the end of 2016 DARPA commissioned UL (Underwriter Laboratories) - a global research and auditing company - to research the cyber security of IoT gateways for industrial control systems. These gateways connect IoT components to the Internet and are a critical element in IoT environments.

Keeping an eye of the entire IoT stack

"Our contract spanned nine months," reports Heike Thomas, Business Development Manager, Automation, at UL in Germany. To keep an overview of all requirements, UL's Cyber Security Team had the entire IoT architecture in focus - in other words, all microchip software, the components and systems. "We conducted structured penetration tests and analyzed how systems access remote-controlled devices and how they process software updates," Ms. Thomas explains. Based on these tests, the engineers derived scientifically based and reproducible test criteria and developed test methods for IoT gateways. UL's goal is to develop a cyber security standard specifically for the software of industrial IoT gateways.

Through this research, UL will be able to recognize at an early stage in which direction the IoT systems are currently developing. "This knowledge has also proved itself in the German market in which we have been operating for close to 20 years," adds Thomas. Among its many customers, UL also advises and supports multinational corporations in cyber security-related topics.

Many German companies are currently planning on networking their production with an IoT platform or are already in the process of building one. "And lots of companies are concerned that their IoT projects will become too complex due to the increasing security requirements," explains Thomas. "However, companies that can rely on the standards that ensure a high level of cyber security for components, can focus on comprehensive safety concepts such as Network Behavior Analysis, Honeypots or centralized protocoling, thereby developing a 'defense in depth' security strategy."

UL has been working on securing cyber physical systems for around 10 years. To bundle these efforts, four years ago UL initiated its Cyber Assurance Program (CAP). The program analyzes the risks of Industry 4.0 systems in the automotive, factory automation, pharmaceutical and lighting industries and bases its work on the UL 2900 Series of Standards.

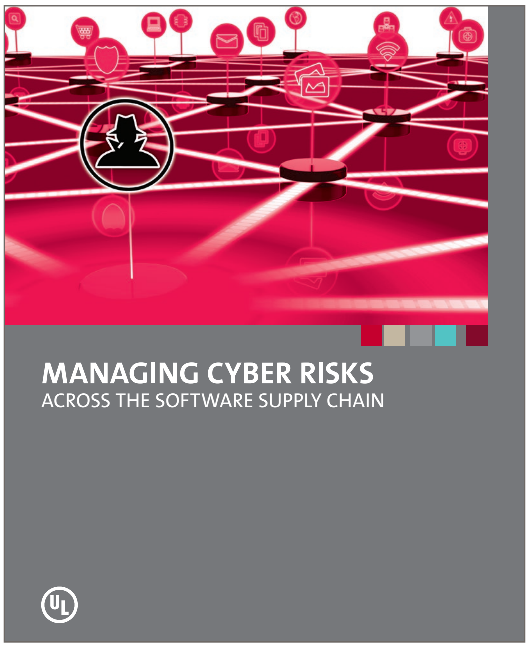
Cyber security is currently being discussed in depth at the component level. Says Ms. Thomas: "It is a huge challenge to retain an overview of the different application areas and geographical diversity of the components." "Once the components have been certified for cyber security, the complexity is significantly reduced."

Strategic recommendations from the DARPA project

"We recommend that companies include their existing security guidelines and best practices into the product lifecycle in order to include maintenance and support in the security efforts," explains Ms. Thomas. Practice has shown that it makes sense to test how attacks on IoT systems might transpire by modeling and simulating attack scenarios. "This way, risks can be better understood, and protective measures can be developed," Thomas explains.

Based on this research activity, it has become clear why UL considers itself to be a global company in the segment of security and risk science. "For us, the project with DARPA is recognition for the high level of expertise of UL in the cyber security segment," summarizes Ingo Rübenach, Vice President, UL DACH & Eastern Europe. "And it shows that our research is helping to fill Industry 4.0 with life."

germany.ul.com/en/industry-4.0


MANAGING CYBER RISKS
ACROSS THE SOFTWARE SUPPLY CHAIN

Learn more in our brochure "Managing Cyber Risks Across the Software Supply Chain". Download at: germany.ul.com/en/industry-4.0

MAKING INDUSTRY 4.0 FEASIBLE

"If one looks at all the fields in which new technologies are being developed due to IoT, then we are headed towards revolutionary upheavals. In the factory of tomorrow, the supply chains are continuous and transparent and new services with artificial intelligence will be structuring production processes in a highly efficient manner – keyword: advanced manufacturing. However, many ideas must still be analyzed – beginning with cyber security, and including interoperability and human-machine communication, which casts a new light on occupational safety. In all these cases, safety is the core of the implementation process. Our mission: UL wants to make Industry 4.0 feasible."
Ingo Rübenach, Vice President, DACH & Eastern Europe, UL International Germany GmbH

Ingo Rübenach
Vice President,
DACH & Eastern Europe,
UL International Germany GmbH
T: +49 69 489810 291
E: Ingo.Ruebenach@ul.com