Strategic alignment for the protection of IoT systems

How the US Department of Defense wants to protect critical infrastructure – and what conclusions IT experts can extract from this.

Michael Kallus

It counts as one of the technologically leading organizations, yet it only employs 140 experts. However, these experts engage university, military and industrial research institutions and network their leading employees with one another. This network is often described as “100 geniuses that are networked through a travel agent.”

And that ‘travel agency’ is DARPA, the Defense Advanced Research Projects Agency. On behalf of the US Department of Defense, it invests in research projects that are in the interest of national security and, in doing so, supports innovation in almost every field - from biology to microelectronics as well as unmanned aircraft. In this fashion DARPA created the foundation of today’s Internet. In the late 1960s, the DARPA pulled together researchers who developed ARPANET (Advanced Research Projects Agency Network), which was the precursor for the Internet.

Its tasks also include safeguarding critical infrastructure such as hospitals or industrial systems. For this reason, at the end of 2016 DARPA commissioned UL - a research and auditing company - to research the cyber security of IoT gateways for industrial control systems.

“Our contract spanned nine months,” reports Alexander Köhler, Business Development Manager at UL Cyber Security. In order 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 checked how systems access remote devices and how they process software updates,” Mr. Köhler explains.

Why the lifecycle is essential in IoT

Through this research, UL will be able to recognize at an early stage in which direction the IoT systems are currently developing. A significant part of this is the consideration of the lifecycle. If, for example, a product algorithm was hacked, then it must be replaced. “So, a component supplier must keep an eye on the early development of a product and must define what happens when the components are used in specific systems,” explains Köhler.

For this, UL is also the partner that can offer the corresponding tools. A UL 2900 standard validates whether or not the component manufacturer has integrated lifecycle management processes,” remarks Mr. Köhler. This enables us to identify manufacturers willing to assume this responsibility Another example: the IEC 62443 Series of Standards offers criteria that ensure the development of secure products and processes UL 2900-2-2 is designed to enable the application of these safety criteria from IEC 62443 to products and systems.

UL 2900-2-2 further defines the requirements in such a manner that certifiable component tests can now be executed.

These types of services support IT managers who require new processes to be able to react to product changes. “Here we are expecting a corresponding level of automation to manage IoT devices,” says Köhler. “Today, IT managers require a continuous monitoring of their IoT infrastructure.”

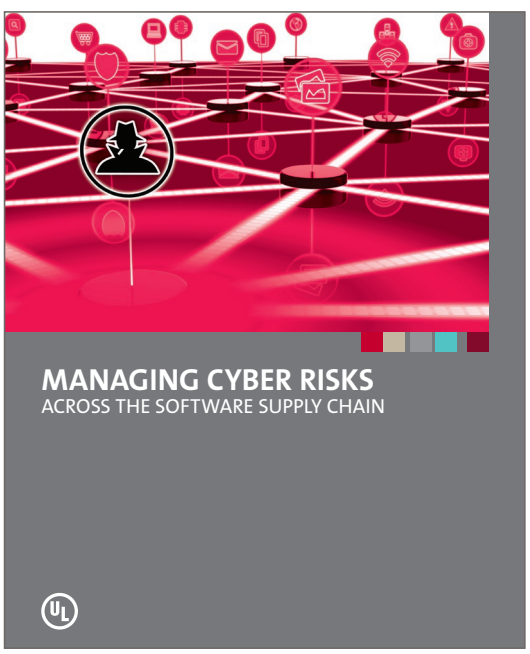
Strategic recommendations from the DARPA project

It its tests, UL has long been following how patches for components and management software affect the safety of IoT systems. “That is a part of our risk analysis, even updates must be cyber safe,” explains Köhler. The patch management is also a component of the UL Standard 2900 and regulates how a component manufacturer must deal with this.

UL has been working on securing cyber physical systems for around 10 years. In order to bundle these efforts, the company initiated its Cyber Assurance Program (CAP). The program analyses risks of Industry 4.0 companies in the segments of automotive, factory automation, medicine and illumination and bases its work on the UL 2900 Series of Standards.

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 expertise of UL in the cyber security segment,” says 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



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

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