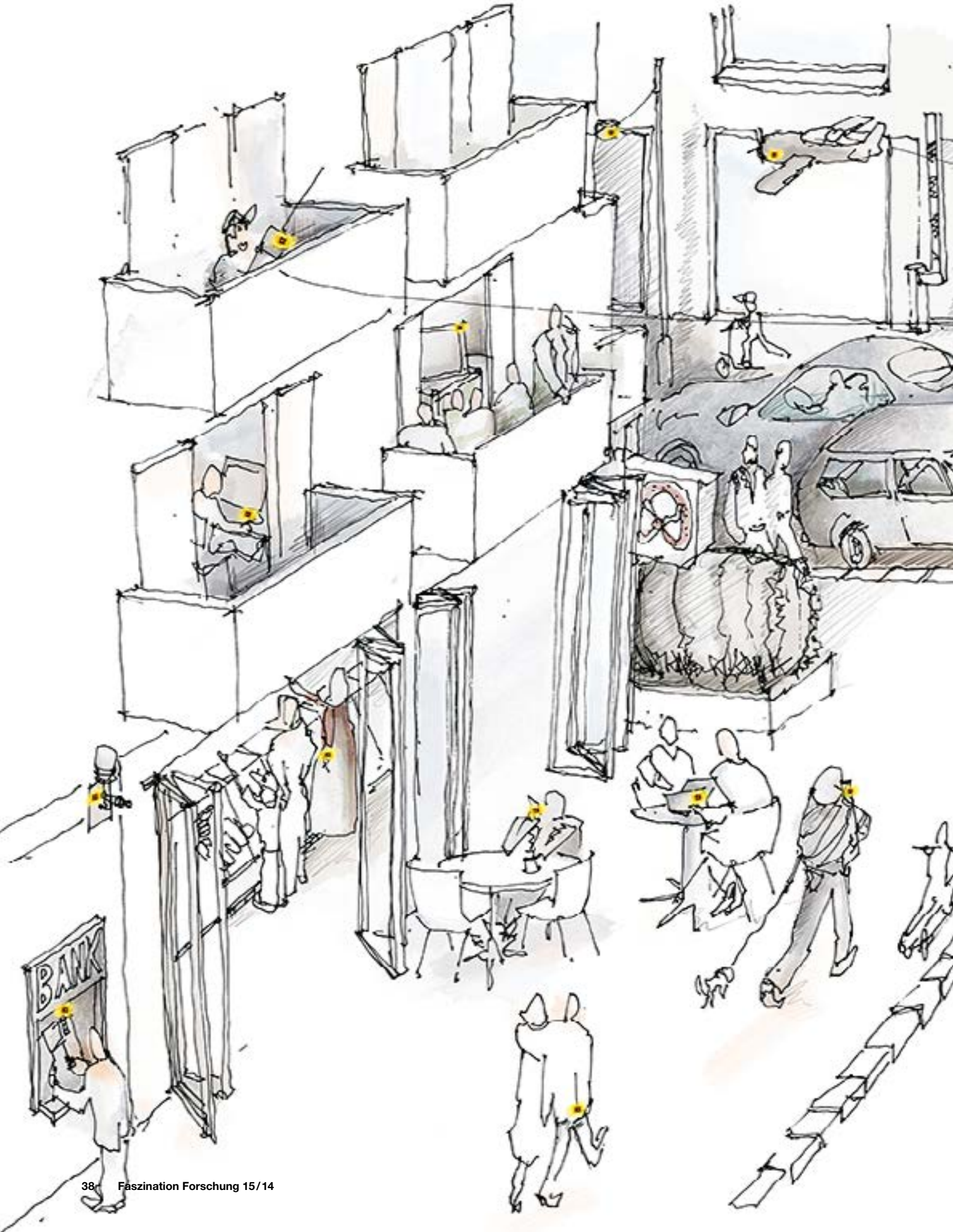
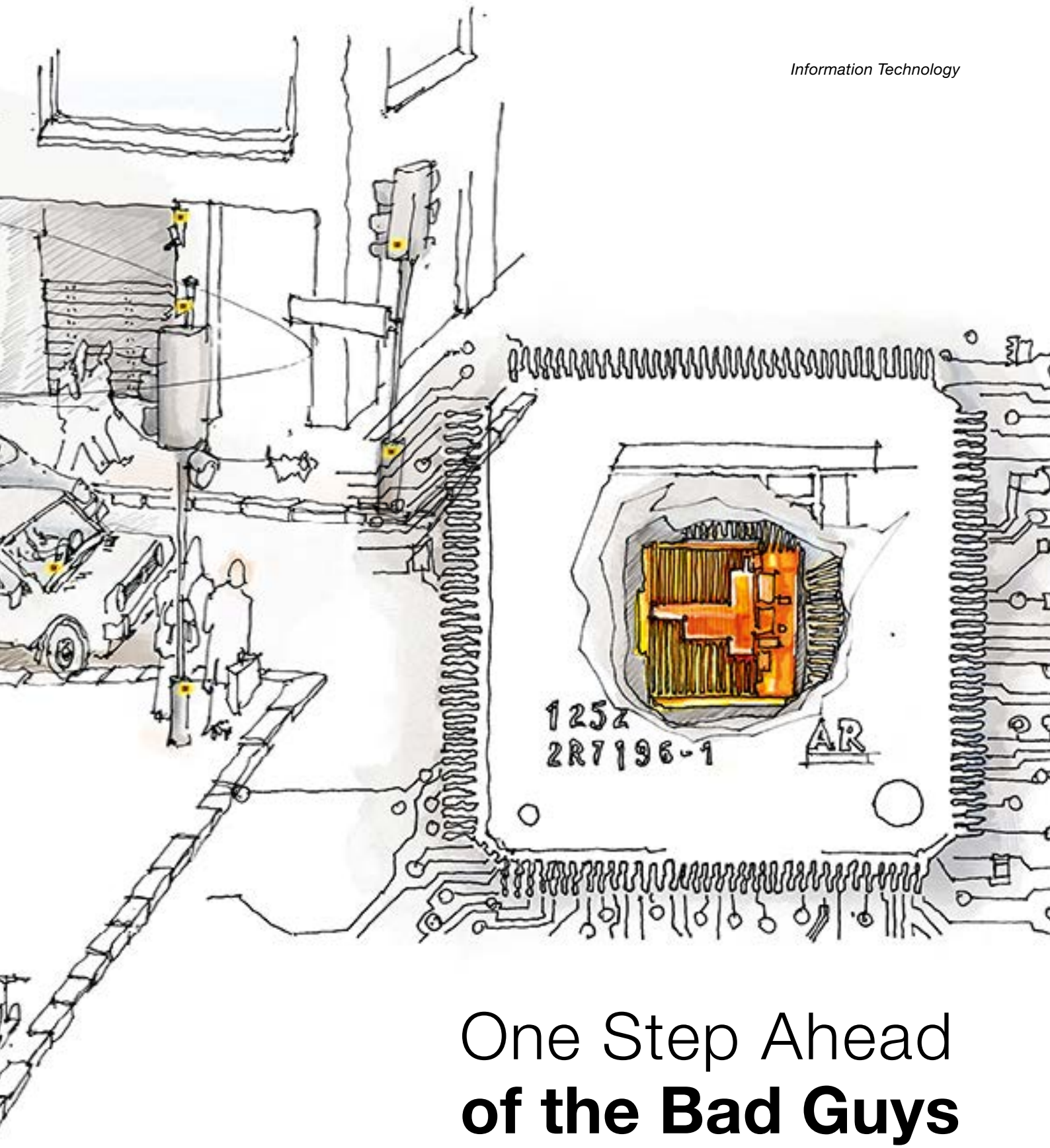
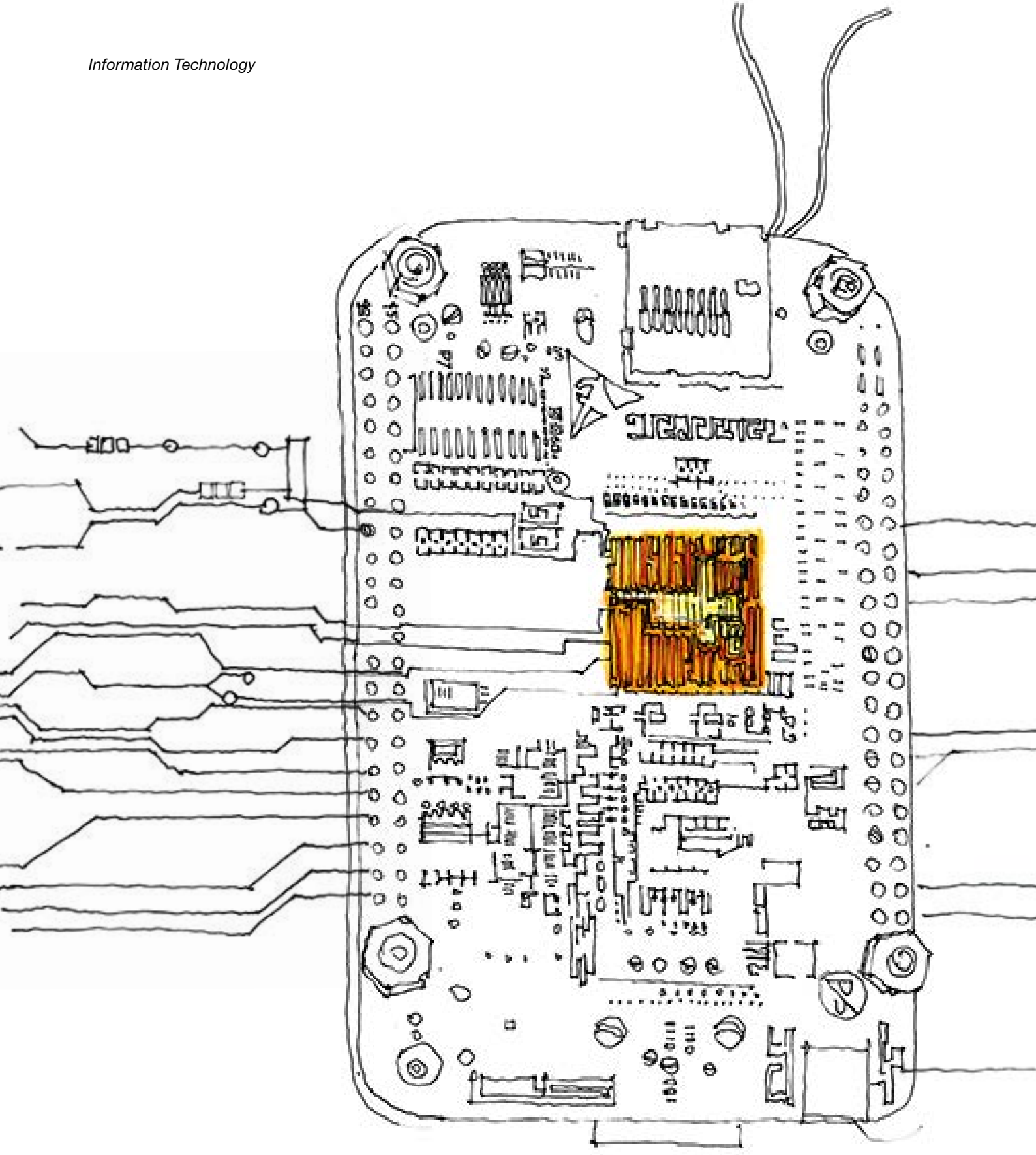

BANK



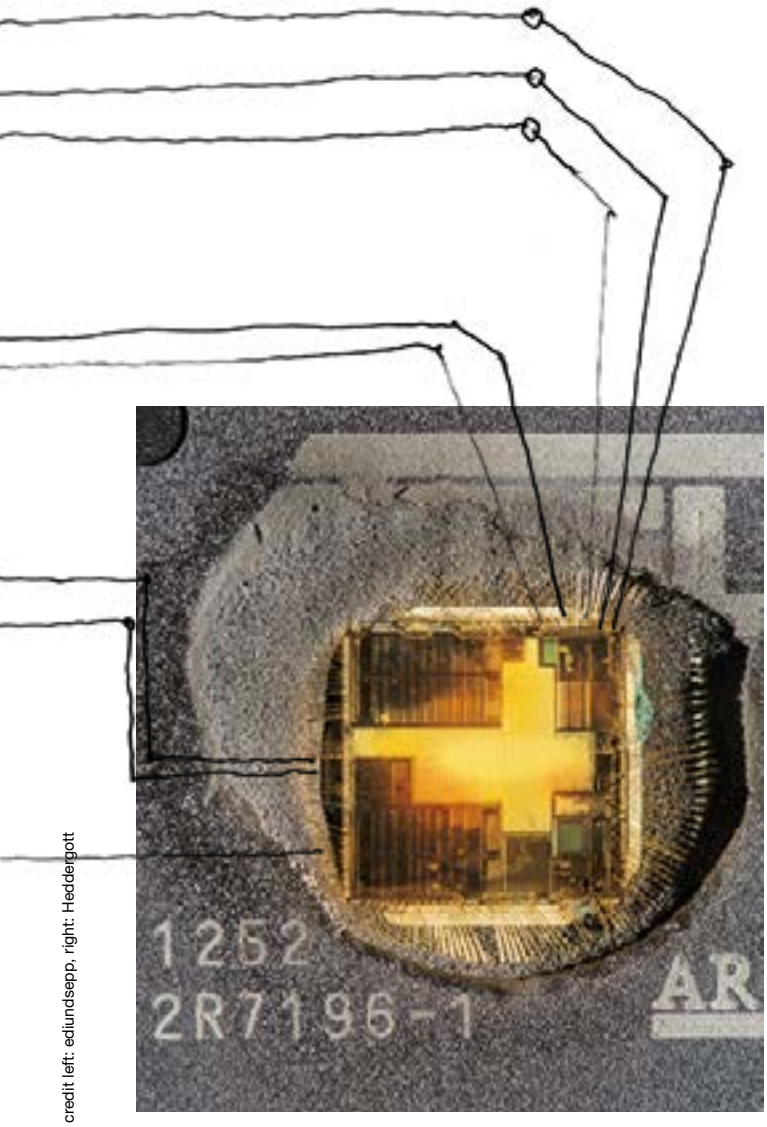
One Step Ahead **of the Bad Guys**

Georg Sigl is a professor of IT security. His job is to uncover security gaps in technical systems, particularly, control systems embedded in machines and production units. These embedded systems are increasingly being targeted by hackers, and Sigl leaves no stone unturned to identify weak spots, whether it's listening in on how cell phones compute or dropping acid on processors.

Picture credit: ediundsepp



Link
www.sec.ei.tum.de



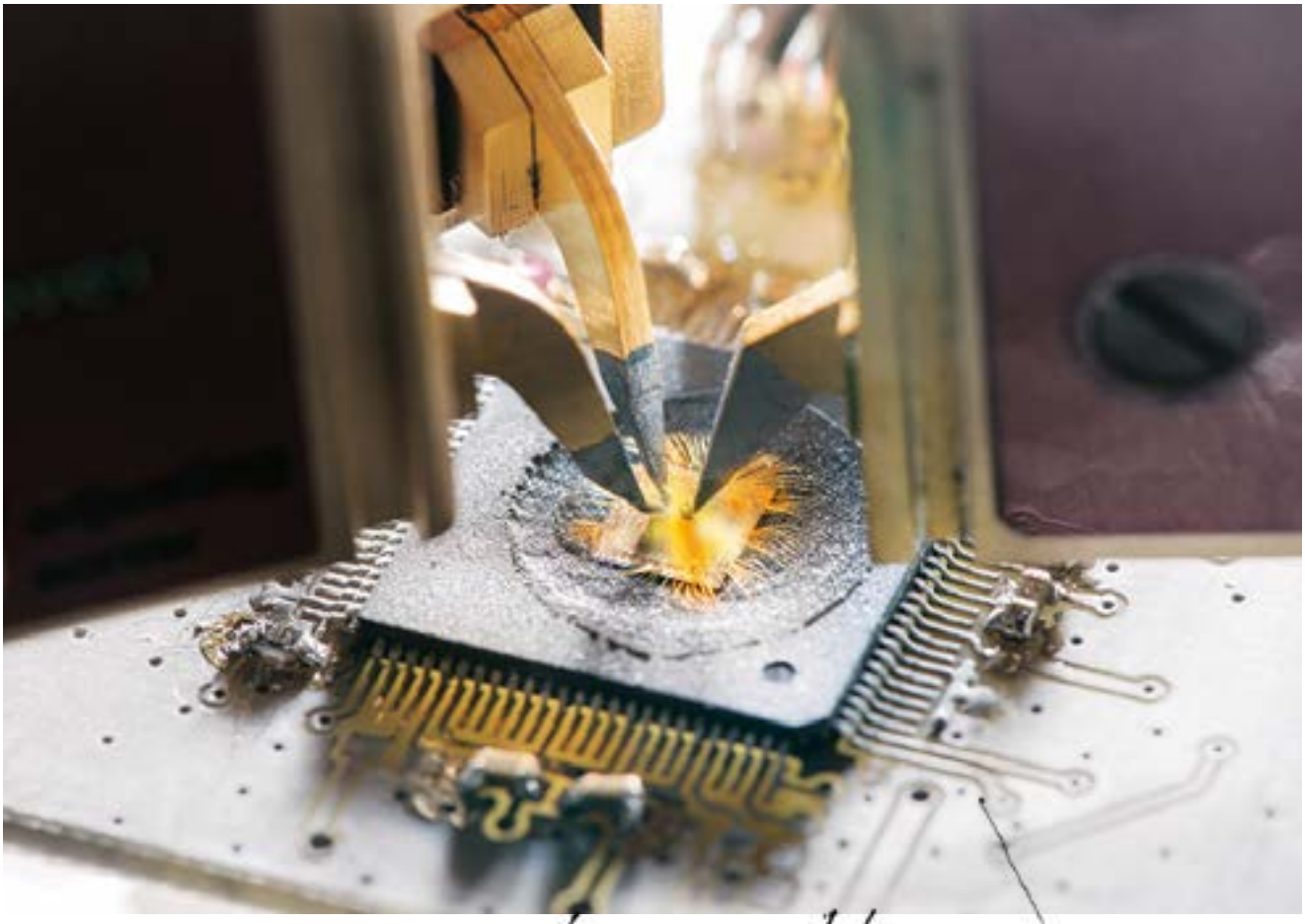
Picture credit left: ediundsepp, right: Heddergott

A microcontroller opened with the help of chemicals in order to find out about the composition of the processor.

Den Bösen einen Schritt voraus

Georg Sigl, Professor für Sicherheit in der Informationstechnik an der TUM, entwickelt Sicherheitstechnologien, um Steuerungs-Hardware für die Industrie, sogenannte Embedded Systems, zu schützen. In Deutschland wird derzeit unter dem Schlagwort „Industrie 4.0“ die Vernetzung von Maschinen vorangetrieben. Maschinen und andere Komponenten einer Produktionsanlage werden zunehmend mit Steuergeräten, sogenannten Embedded Systems, ausgestattet und an das Internet angebunden. So ist es möglich, alle Maschinen miteinander intelligent zu vernetzen. Mit der Vernetzung steigt aber auch das Risiko, dass Hacker über das Internet in Fabriken eindringen, Produktionsdaten aus Maschinen stehlen und Fertigungsstraßen zum Stillstand bringen. Um das zu verhindern, entwickelt Georg Sigl Sicherheitstechnologien, die die Embedded Systems vor Angriffen schützen.
Sigl gehört auch der Leitung des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit (AISEC) in München an. Er simuliert in seinen Labors unter anderem Hackerangriffe auf Hardware, mit denen er die Sicherheitscodes, sogenannte Schlüssel, von Computerprozessoren knackt. Dafür nutzt er unter anderem sehr empfindliche Messverfahren, mit denen er den Stromverbrauch oder die elektromagnetischen Abstrahlungen der Prozessoren analysiert. Ein Schwerpunkt der Arbeit liegt derzeit auf der Entwicklung robusterer Verfahren für die Verschlüsselung von Hardwarekomponenten. Dazu gehören sogenannte PUFs, Physical Unclonable Functions, nicht kopierbare, physische Eigenschaften. Dabei verwendet man äußere, physische Merkmale von Prozessoren oder anderen elektronischen Bauteilen, um sie fälschungssicher zu machen. So lässt sich beispielsweise der individuelle Ladungszustand, den ein Prozessor mitsamt seiner Tausenden von Transistoren beim Einschalten des Computers hat, als fälschungssicheres individuelles Merkmal des Prozessors nutzen. Sigls Arbeit zeichnet sich dadurch aus, dass sie informatische, mathematische und elektrotechnische Expertise vereint und damit umfassende Schutzkonzepte liefert. *Tim Schröder*

There are many theories regarding the origins of Stuxnet. Some experts believe that hackers developed the computer worm for industrial espionage. Others think it was created by the Israeli secret service to disable Iran’s nuclear capabilities. Whatever the reason, the developers behind Stuxnet had one clear target in mind: a Siemens controller used to regulate electronic components in industrial systems. Stuxnet was designed to sabotage these facilities, or at least significantly disrupt production. Numerous companies across the globe reported that they had come under attack from Stuxnet. Even today, the extent of damage to systems in Iran and elsewhere in the world is unclear. What we do know, however, is that this computer worm – which was discovered roaming the globe four years ago – is one of the most high-profile examples of professional malware designed to attack industrial facilities. It revealed just how vulnerable sophisticated technology can be if manufacturers do not implement sufficient protective measures.
There are a lot of computer controllers in the world today. Just one car alone can contain several dozen minicomputers used to control engine valves or power windows. The number of these embedded systems is set to rise by billions in the near future. The German government, for example, is currently promoting the transition to smart factories ▷



Chips under attack in Georg Sigl's laboratory: Measuring electromagnetic radiation to prepare for side channel attacks (top left); fault injection with power glitches in order to perform fault attacks (top center); firing laser beams at an open processor chip while it carries out calculations. The laser causes calculation failures, which can be used to extract secret information (top right). Side channel attack by means of three highly sensitive measuring probes (bottom).

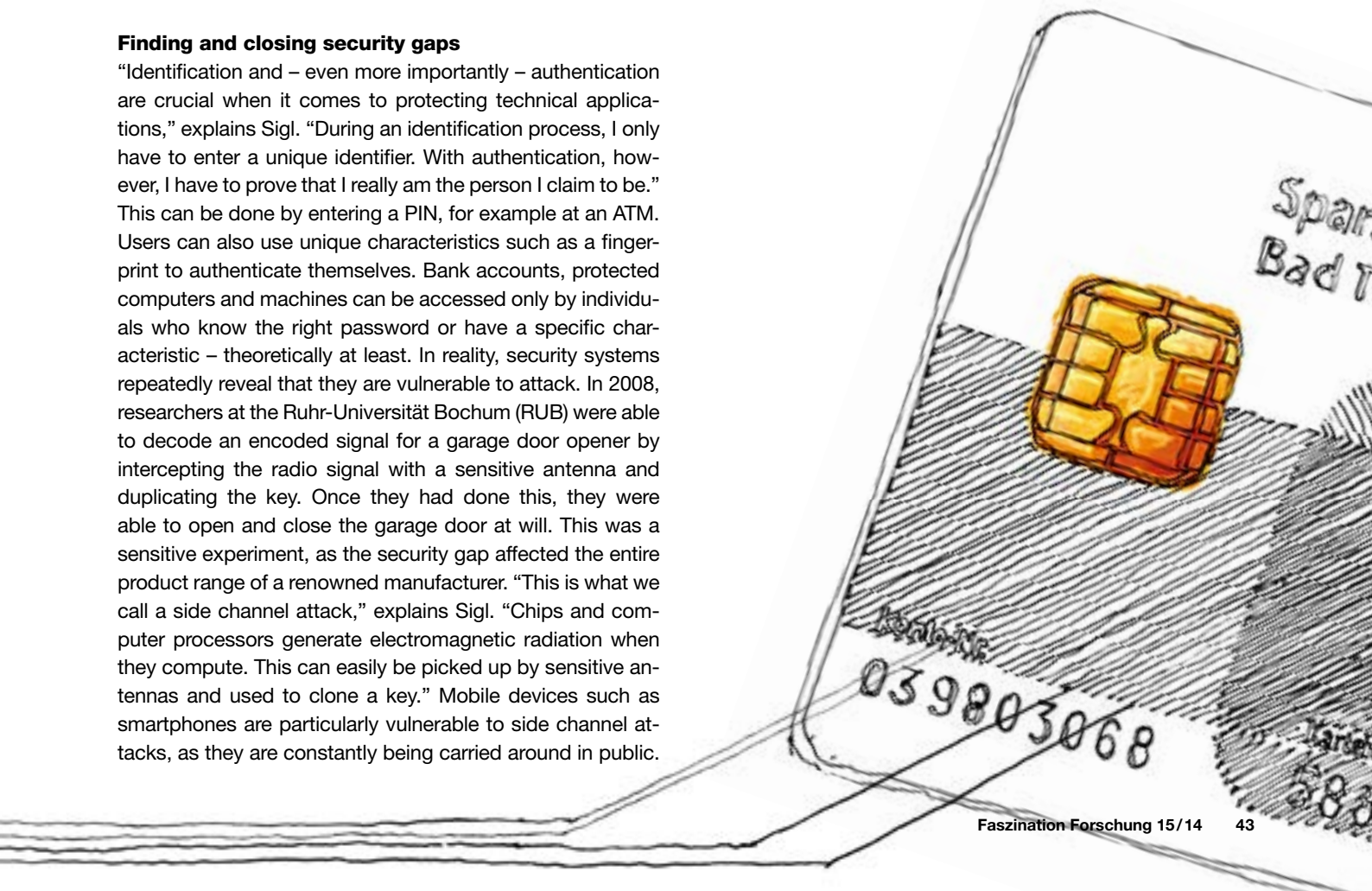
Picture credit left: Heddergott, right: ediundsepp

under the banner of its “Industry 4.0” initiative. More and more machines and components in production facilities are being equipped with embedded systems and linked to the Internet. In other words, all machines are being connected in smart networks. When a company receives an order, it can then use this intelligent network to send commands to its different production sites via the Internet. Embedded systems enable machines to activate themselves and components to organize their own transport. A malware attack could therefore have devastating consequences, allowing criminals to steal blueprints from machines or bring entire production lines to a halt. Yet these systems harbor an alarming number of security gaps.

It is Georg Sigl‘s job to close these gaps before they can be exploited by criminals. Sigl is a professor of IT security at TUM and one of the heads of the Fraunhofer Institute for Applied and Integrated Security (AISEC) in Munich. In his labs, he fires laser beams at computer processors and measures electromagnetic radiation from smartphone chips in a bid to decode the secrets of computers, chip cards and embedded systems, crack codes and break into secure systems. He does this to discover and close security gaps before hackers strike. Sigl spent many years at Siemens and later Infineon, working on secure chip cards and developing a number of groundbreaking security technologies. Today, he applies this expertise to a number of tasks, including the protection of embedded systems.

Finding and closing security gaps

“Identification and – even more importantly – authentication are crucial when it comes to protecting technical applications,” explains Sigl. “During an identification process, I only have to enter a unique identifier. With authentication, however, I have to prove that I really am the person I claim to be.” This can be done by entering a PIN, for example at an ATM. Users can also use unique characteristics such as a fingerprint to authenticate themselves. Bank accounts, protected computers and machines can be accessed only by individuals who know the right password or have a specific characteristic – theoretically at least. In reality, security systems repeatedly reveal that they are vulnerable to attack. In 2008, researchers at the Ruhr-Universität Bochum (RUB) were able to decode an encoded signal for a garage door opener by intercepting the radio signal with a sensitive antenna and duplicating the key. Once they had done this, they were able to open and close the garage door at will. This was a sensitive experiment, as the security gap affected the entire product range of a renowned manufacturer. “This is what we call a side channel attack,” explains Sigl. “Chips and computer processors generate electromagnetic radiation when they compute. This can easily be picked up by sensitive antennas and used to clone a key.” Mobile devices such as smartphones are particularly vulnerable to side channel attacks, as they are constantly being carried around in public. Cloning keys in this way requires sensitive equipment. And Sigl has it all in his labs. In fact, Sigl and his team even go so far as to burn away processor casing with nitric acid to uncover the circuit paths inside. After all, this is something that could well happen in real life if industrial spies were to steal hardware. Once the processor is exposed, Sigl and his employees use a probe measuring just one tenth of a millimeter in size to eavesdrop on the faint electromagnetic signals – in much the same way as a doctor uses a stethoscope to listen to the human body. The researchers are listening for the security key. Almost every secure technology system has a key of this kind. Experts differentiate between symmetric and asymmetric encryption. In the case of symmetric encryption, the transmitter and receiver use the same key. When children create a secret language, for example, they are using symmetric encryption and use the same key to encrypt and decrypt messages. In contrast, asymmetric encryption uses a public and a private key. Here, users can encrypt (or sign) a message using a private key. This happens automatically when you transfer money, for example, during online banking. The bank then uses a public key to check whether the signature is correct. With this method, the sender and the receiver do not need to send the key to each other – a clear benefit over a secret language, as the act of exchanging the key is a potential threat to security. ▷



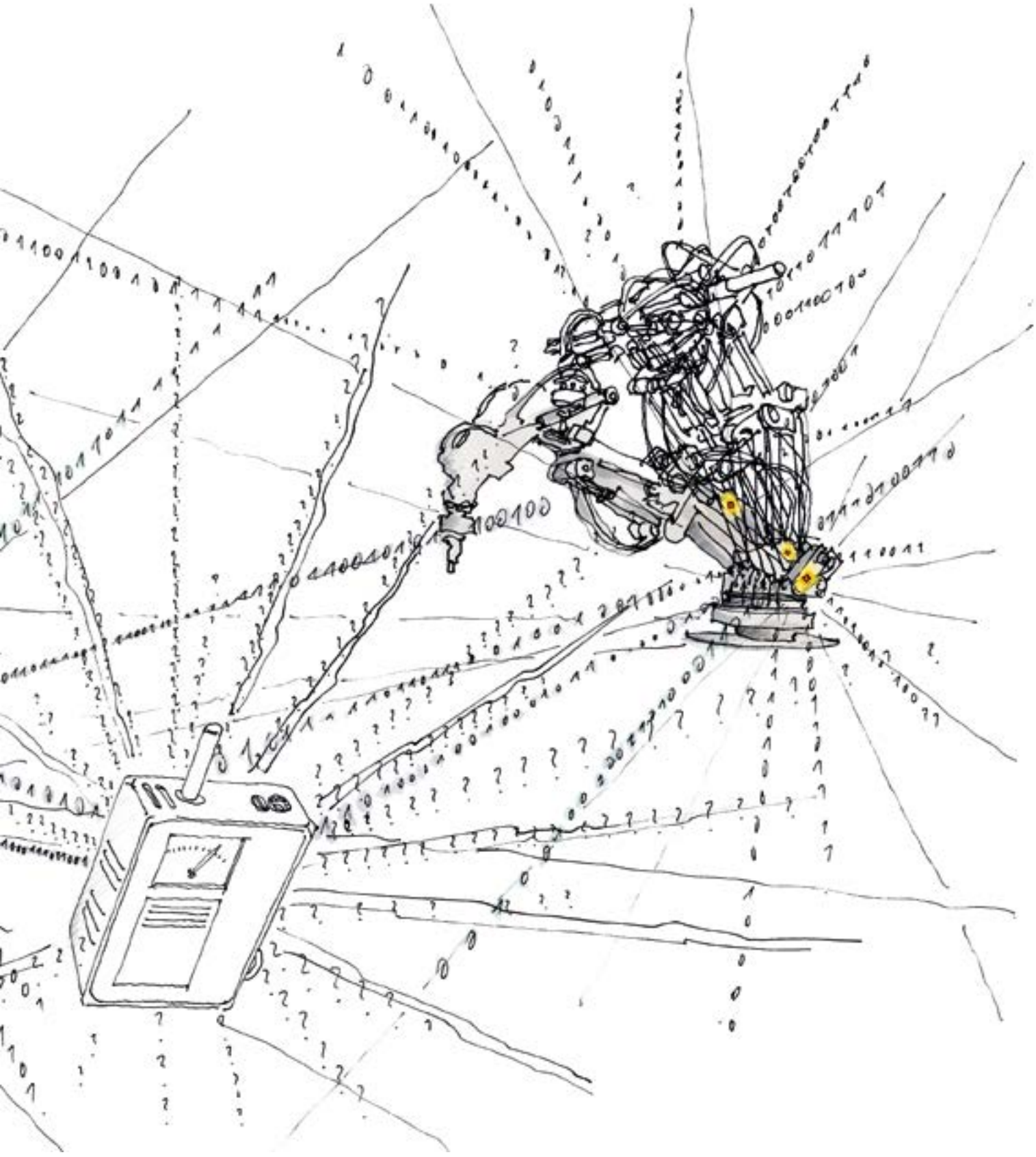
Protecting keys

In cryptography, a secret number is used to encrypt the data to be sent. This private key protects the message from outside attack. Hacking is all about decoding this key. And there are different ways of doing this for different applications. Sigl is familiar with these methods from his time in the chip card industry. One way is to measure the duration of a computing operation. If the process takes a long time, for example, this could indicate that the key is using more ones than zeros. Measuring a chip's power consumption can also be used to capture security keys, as complex computational operations require more power. Sigl uses the differential power analysis (DPA) principle to outline how this method works. In this case, a hacker feeds random data many thousands of times into a chip that uses an unknown key to encrypt it and measures the power consumption during these cryptographic operations. This consumption depends on every single key bit. The hacker then guesses one bit of the key and calculates an internal bit, which depends on the data and the guessed key bit. Then he assigns the thousands of power consumption measurement values into two groups, using the internal bit for the decision. If the statistical distribution of these values can be separated into two groups of high and low power, he has guessed the key bit correctly. If no statistically relevant distinction of the power values is possible, the guessed bit is wrong. In this way, a long key with many bits can be determined bit by bit.

Yet there is a way of countering this. "Engineers can incorporate random numbers that change the computing operation and make it impossible for an attacker to map regularities during DPA," explains Sigl. "However, you have to be very careful when doing this to ensure that you do not incorporate any leaks that allow information to be captured via a side channel attack."

For Georg Sigl, the move to security came very much by chance in the 1990s, when he switched departments while working at Siemens. "I was an experienced microprocessor designer, but cryptography was a completely new area for me," he says. "It was a secretive world that I knew nothing about, and it wasn't until I moved departments that I found out how fascinating it is." Today, the electrical engineer is primarily interested in fostering an interdisciplinary approach to cryptography that incorporates mathematics, IT and electrical engineering. "Electrical engineers are, above all, hardware specialists, whereas mathematicians and IT engineers have in-depth insights into the mathematics of cryptography. We bring these areas of expertise together to provide a multi-disciplinary approach to study." This integrated approach is crucial, as today's hackers are already combining mathematical, physical and engineering methods to uncover new channels of attack. "The challenge for researchers in our field is to become so proficient in these areas that we can cross-link them and come up with new ideas for counteractive measures." ▷

Picture credit: ediundsepp

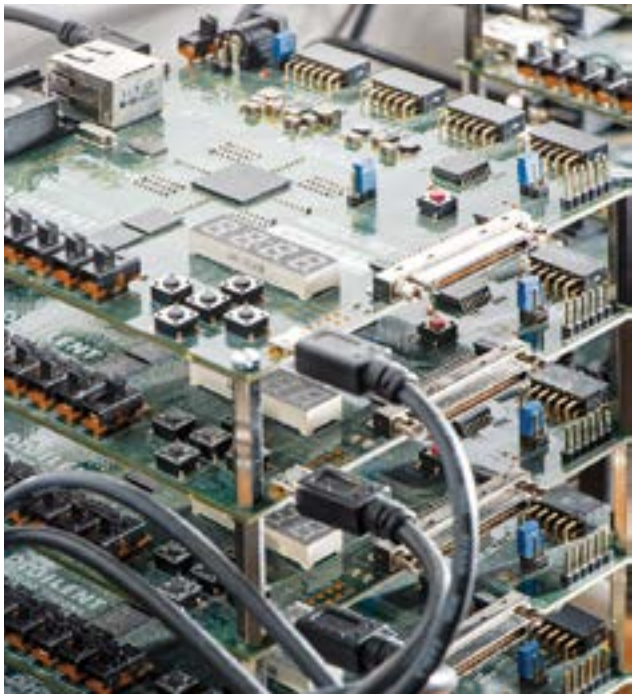


In the future, smart factories, machines and other components will be equipped with embedded systems to be controlled via the Internet. These systems are prone to security gaps. Georg Sigl and his group continuously develop new technologies to protect the industry's control hardware from any such attack.

Georg Sigl is a professor of IT security at TUM and one of the heads of the Fraunhofer Institute for Applied and Integrated Security (AISEC). Before that he spent ten years at Infineon developing technologies for secure chip cards. "Germany has a world wide leading position in this high-end hardware security technology," he says, "The two leading chip card companies have their main R&D sites here, and we build the bridge between this industry and university research in order to win the unending race against hackers."

Unclonable chip functions

A relatively recent technology known as the physical unclonable function (PUF) underscores the importance of this approach. PUF uses the external, physical properties of processors and other electronic components to make them uncopiable or incapable of generating security keys. Georg Sigl and his team are working intensively in this field. PUFs can also be used to protect embedded systems. The risk of malware being introduced to technical systems via counterfeit hardware is a major concern for manufacturers. Being able to uniquely identify security-relevant hardware would help close this security gap. PUFs can be used to do this. The technology usually harnesses the unique properties that a hardware component is given during production. Every computer processor, for example, differs slightly from all other seemingly identical microprocessors – even if they are produced in the same series. When a device is switched on, the many thousands of transistors in a processor's memory often have different states. Some are switched to represent 1, and others 0. This state pattern is almost exactly the same every time a chip is switched on. It can therefore be used as a kind of individual key to encrypt data on the component or to make it uniquely identifiable. Another type of PUF uses properties that are created during production and stored for the customer in much the same way as a TAN list. This can include specific electronic properties. To identify a processor or other component at a later date, the chip is fed predefined computing operations saved on the PUF list. If the chip responds with a characteristic PUF pattern, the customer can be sure that it is an original component. The real challenge for Sigl is to always be one step ahead of the attackers. "Staying ahead of the curve is not just a question of carrying out research in secret in companies. We also need to develop and implement new ideas at universities and research institutes." This was one of the main reasons why Georg Sigl moved into research in 2010. And with the two working groups at the TUM and the Fraunhofer Institute AISEC, he is certainly in the best possible position to make life difficult for hackers, even in this increasingly networked world. *Tim Schröder*



Connected evaluation boards with field programmable gate arrays are used to test out ideas for new PUFs.

Picture credits: Heddergott