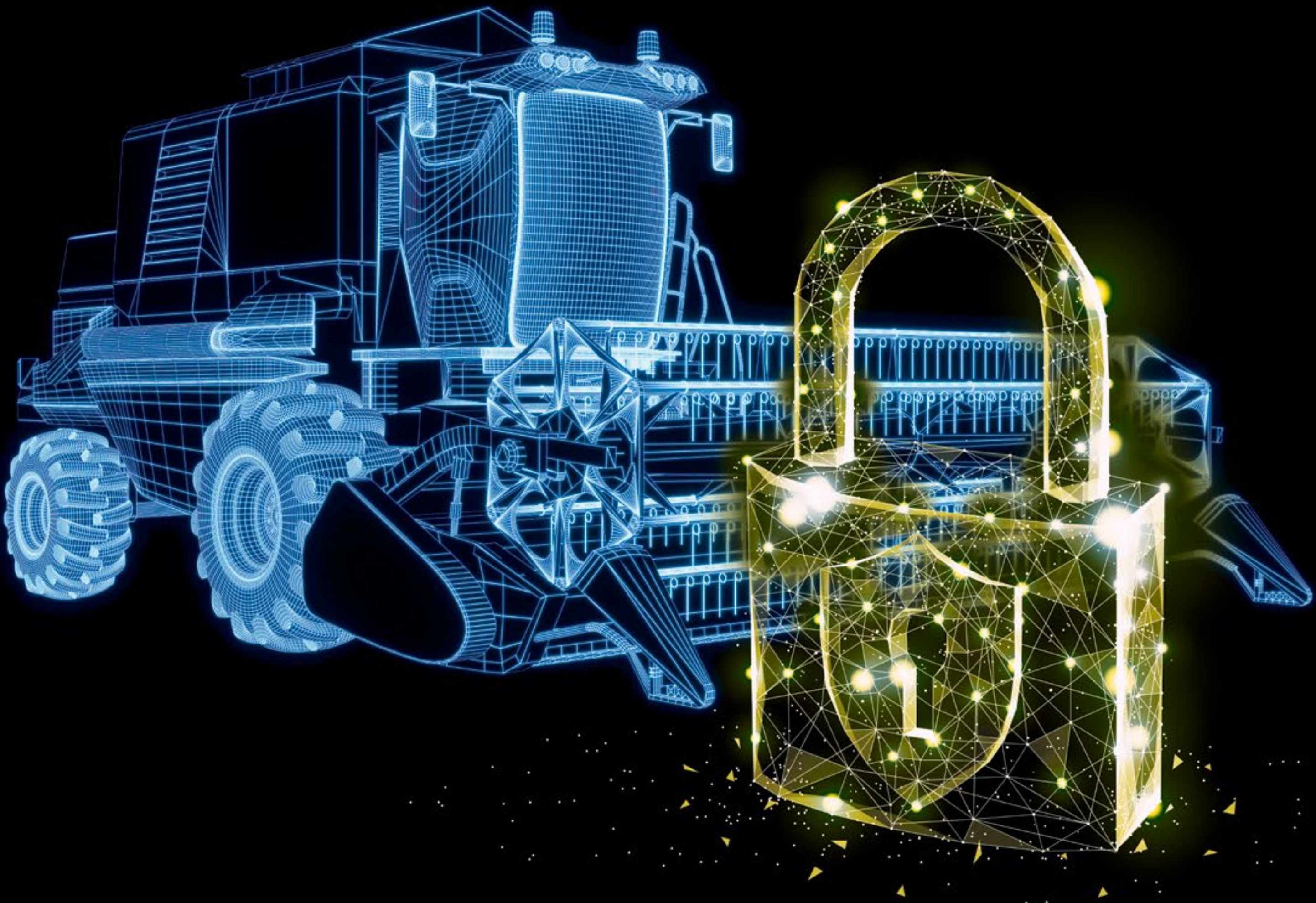
Springer Vieweg

ATZ extra



SECURITY

Facing Challenges Holistically

/// **INTERVIEW** Jens Köhler, Daniel Steinmetzer [ITK]

© ITK Engineering GmbH

"It is essential to protect complex attack paths holistically"

The high levels of cost pressure in the agricultural sector have made it necessary to ensure the optimum application of expensive machines and systems. This is the reason why digitalization and automation as well as autonomous driving in the agricultural sector are more advanced than in the automotive sector. In an interview with ATZelectronics, Dr. Jens Köhler and Dr. Daniel Steinmetzer explain the challenges developers at OEMs and suppliers face in terms of the subject of cybersecurity.

ATZelektronik _ Digitalization in farming is becoming increasingly more important. This is reflected in the increased relevance of cybersecurity. What threats are there in the agricultural sector and are the hacker attacks focused more on ransomware or directed toward sabotage?

KÖHLER _ In fact, there is actually no one type of attacker, but a whole range of types of attackers. One possible attacker that would not immediately come to mind is the user themselves: particularly in business models where additional features need to be paid for and then activated, the user has a certain motivation to attempt to circumvent this. These customer options need to be checked properly to see whether they could represent ports of entry for a hacker or for manipulation. The motivation of an external attacker is very different: white-hat hackers want to establish their image in the scene and the aim of terrorist attackers is to paralyze important infrastructure such as a fleet of harvesting machines. Commercially motivated hackers just want profit. The latter group is currently gaining in prominence via ransomware attacks. To get an idea of the size of this, market researcher Vansom Bourne estimates the global turnover of cybercriminals to be almost 600 billion dollars.

What have manufacturers of agricultural machines to lose as a result of the attacks you mentioned?

KÖHLER _ This varies a lot. We often employ five damage categories in our risk analyses: damage to reputation, since no one would want to drive a tractor that can be driven remotely by unknown parties or even immobilzed. Intellectual property, since information about the target equipment should not fall into the hands of the competition. Safety, so that protection life and limb of people interacting with the system are safeguarded. There are also other aspects to be considered such as legal damages for example, claims for damages, due to unsafe products and financial damage caused by recall actions, or the downloading of required updates to correct weaknesses, or lost profit due to the piracy of products.

Where are the weak spots that can be attacked?

KÖHLER _ The most obvious are system interfaces such as Wi-Fi, Bluetooth, CAN, NFC, USB, GPS, or the Cloud connection. Physical interfaces are particularly relevant for protection against the users themselves. With systems connected to a backend, the backend itself is a popular port of attack. This was displayed by hacks on numerous automotive OEMs at the beginning of 2023. But there are also dangers that are not connected to the system. These include supply chain attacks, which are attacks against the target system even while it is under development, either by the developer planting damaging code or indirectly via compromised suppliers.

“The agricultural machinery sector is in the favorable position of being a fast follower”

Which security-based norms, standards, and processes have already been established and what will manufacturers and suppliers of agricultural machines have to expect?

KÖHLER _ Now that is a very good question. The scope of the UNECE R155 regulation for type approval is valid for road vehicles. Agricultural machines were included in a previous version but were then excluded again. The UNECE R156 regulates the handling of software updates and is used for agricultural machines today. The EU Cyber Resilience Act (CRA) is focused on “products with digital elements”. This includes tractors and other mobile machines (e.g., harvesters). The CRA regulation has not yet been finalized. If the current proposal of the legislation is passed, then we can assume that the consideration of cybersecurity will have to be proven in the development process and system’s or subsystem’s life cycle. If this isn’t the case, then fines can be imposed of up to 15 million euros, or 2.5 % of the global annual turnover. As soon as the CRA is passed, manufacturers and suppliers have 24 months to implement the directives. This time period is extremely ambitious, particularly for products that go beyond pure software. CEMA has already expressed concerns and is pushing for an extension of the deadline to 2030. In terms of standardization, the most fitting existing standard is currently ISO/SAE 21434, which influences the prevailing state-of-the-art technol-

© ITK Engineering GmbH

Dr.-Ing. Jens Köhler is a senior specialist for cybersecurity at ITK Engineering GmbH. For over seven years, he has been supporting customers in a range of fields determining, implementing, and testing appropriate cybersecurity measures and establishment of cybersecurity engineering processes and methods in companies. He completed his PhD at the Department of Informatics at the Karlsruhe Institute of Technology (KIT) in the field of Cloud Security.

© ITK Engineering GmbH

Dr.-Ing. Daniel Steinmetzer is lead expert for cybersecurity at ITK Engineering GmbH. He has been active as project manager, trainer, and consultant and supports a variety of customers in introducing and implementing cybersecurity engineering measures and processes. He completed his PhD at the Department of Computer Science at the Technical University of Darmstadt in the field of Secure Wireless Communications.

ogy. ISO/TC23/SC19 is a specific agricultural standard planned for 2026; however, it cannot be finalized before the CRA comes into force.

Do the comparably low production volumes in the agricultural sector make the topic of digitalization/cybersecurity more difficult to implement than in the automotive sector, for example?
KÖHLER _ Yes, definitely. The lower production volumes are largely reflected in the unit price. Since customers of agricultural machines are also price-sensitive, this means that there is less money available for the development of software and nonfunctional aspects such as cybersecurity than in other sectors. But what is very different is that, very often, much more pragmatic ways have to be found than in the automotive sector where a lot has to be validated via processes, quality assurance procedures for development artefacts such as security risk analyses and concepts, and complex supplier structures.

In software development projects, time and resources are normally limited. Can the agricultural technology sector profit from other sectors which faced the same challenges?
KÖHLER _ The agricultural sector is in the favorable position of being a fast follower. In the automotive sector, similar restructuring had to take place over the past few years. Of course, not everything can be adopted 1:1, but there are definitely comparable challenges. Basic concepts from the commercial vehicle sector can be easily integrated in agricultural products, such as validation of updates, secure boot, secure onboard communication, validation processes for diagnostics, and debugging interfaces. Even existing products needed to implement these concepts, such as software solutions or hardware security modules, can be adopted.

In your opinion, where should one start?
KÖHLER _ Our experience from the automotive sector shows that pragmatic approaches to cybersecurity lead to the best results: start small and early and build up the topic iteratively. Since product-related risk analyses are required anyway, it would make a lot of sense to start there. The results of risk analyses are the basis for further decisions on measures to take and promote the understanding and acceptance of employees and managers for the expansion of development processes with the topic of security.

> **“Compared to the automotive sector, very often, a more pragmatic path has to be found”**

© ITK Engineering GmbH

The later cybersecurity is considered in engineering processes, the more expensive and difficult it is to implement any required changes, Köhler says

What technical measures can be taken to protect agricultural machines against manipulation?
STEINMETZER _ Efforts need to be made to protect against manipulated firmware in the internal memory or a manipulated update. Cryptographic protocols can be implemented to protect wireless communication with other machines or the onboard communication between control units in the vehicle. An intrusion detection and prevention system can make sense in certain scenarios in order to recognize attacks and malicious code at runtime, and ideally to even block them entirely. In addition, care should be taken during development and production that all non-essential connections and debugging interfaces such as the JTAG interface are closed or deactivated. They often act as backdoors to circumvent security measures. Since these mechanisms are normally associated with development, integration, or operational effort, it makes sense to check first whether these are really essential. Effective protection is ultimately possible with a device-specific, individual combination of security measures.

© ITK Engineering GmbH

Effective protection is possible with a device-specific, individual combination of security measures, Köhler and Steinmetzer agree

What is done regarding development and test of the systems and software to ensure it is secure?
STEINMETZER _ Basically, the entire development of the system or the software should be subject to a standardized security engineering process. This starts with a risk analysis to identify weaknesses and risks. Based on this, measures can be defined within the scope of a security concept that make potential attacks more difficult and reduce risks. When selecting measures, it is important to employ established measures and algorithms. This helps to minimize the risk of creating new weak points. During implementation, the focus alongside code quality should be on secure coding guidelines to avoid weaknesses in software development. During subsequent testing, checks are made to determine whether the measures are suitable and have been correctly implemented, ideally via functional testing of the security features and via nonfunctional penetration tests. The latter check the finished system using methods and tools that an external attacker would have available to them.

Other issues are remote maintenance and over-the-air updates. How can these be protected?
STEINMETZER _ All updates should be validated with a digital signature. The creation of an update then requires the digital key, which only the publisher has. Particularly with remote maintenance, emphasis should be placed on strong, mutual authentication to guarantee that only authorized service providers have access.

AI is being increasingly used in agricultural machines. How can they be protected?
STEINMETZER _ A current particularity with AI is the question of how the AI algorithm was trained and with which data in order to avoid possible adversarial attacks. Such adversarial attacks present the AI with constructed input data that would lead to false classifications. Such attacks can lead to serious problems, depending on the application. This can be demonstrated with slightly modified street signs. A human could recognize a stop sign, the AI could recognize a sign with a speed limit of 130 km/h. Since AI by very definition is not expressly shown how to make decisions, it is not a trivial matter when deciding how to protect against such attacks. This is indeed still a focus area of current research. For example, AI-based sign recognition could be made plausible by using map material. A security operations center can also be used reactively to observe and evaluate possible AI weak points over a device's entire lifetime and, if required, build up the AI algorithm against new attacks.

The combination of external data and internal sensors, can it be a point of attack?
STEINMETZER _ Yes, that is correct. This is why protection against external and internal sensors as well as the communication link is important. External data is often accessed via Cloud services, which offer a large area of attack. In the event of manipulation or failure, internal data should serve as a basis for plausibility checks or as a fallback option. In most application cases, this is why internal sensor data is normally assigned a higher priority so that the local consequences of an attack on external data sources remain limited. It is important that the device is enabled to ensure safe, and under certain circumstances limited, operation even if the external data source has been compromised.

In summary then, what are the most important things to consider when anchoring the topic of security in agricultural technology?
KÖHLER _ In summary, you can say that lower production volumes mean that there is a lower budget for cybersecutity in agricultural applications compared with the passenger car sector. This means that a pragmatic approach is important. Several approaches can be adopted from the automotive sector and other sectors. The basis is always risk analysis; this is the only way to systematically identify all potential risks. Particularly in the expert field of cybersecurity, the devil is often in the detail. Expertise is therefore essential: it is essential to protect complex attack paths holistically. Implementing cybersecurity in companies is a long process that cannot be rolled out overnight. This is why security approaches such as risk analysis and design should be piloted early on in selected projects. The later cybersecurity is considered in engineering processes, the more effort necessary changes will require.

Dr. Steinmetzer, Dr. Köhler, thank you for the interesting interview.

INTERVIEW: Robert Unseld

© ITK Engineering GmbH

Increasingly networked systems harbor dangers and offer areas of attack. A clever security concept is therefore essential, Steinmetzer explains

IMPRINT:
Special Edition 2023 in cooperation with ITK Engineering GmbH,
Bergfeldstraße 2, 83607 Holzkirchen; Springer Fachmedien Wiesbaden
GmbH, Postfach 1546, 65173 Wiesbaden,
Amtsgericht Wiesbaden, HRB 9754, USt-IdNr. DE81148419

MANAGING DIRECTORS:
Stefanie Burgmaier | Andreas Funk | Joachim Krieger
PROJECT MANAGEMENT: Anja Trabusch

COVER PHOTO: © [M] KengVit14 |CoreDESIGN | Stock.adobe.com

ITK Engineering

Stability, reliability and methodological expertise – this is what we have stood for since our founding in 1994. At all times, our customers have benefitted from our dedicated multi-industry know-how, especially in the fields of control systems design and model-based design. Customers can count on us – from conception through to deployment, we cover the entire development process.

Our areas of expertise include:

- Software development
- Hardware development
- Electrical & electronic systems
- System integration
- Software as a product
- Turnkey systems
- Customer specific development
- Technical consulting
- Seminars
- Quality assurance

The satisfaction of each of our partners and mutually respectful cooperation shape our corporate philosophy, in which four values are firmly anchored: Read more about this on the web.

V.1.0.0_e_2021

ITK Engineering GmbH
Headquarters: Ruelzheim
Im Speyerer Tal 6
76761 Ruelzheim, Germany
T: + 49 (0)7272 7703-0
F: + 49 (0)7272 7703-100
info@itk-engineering.com

www.itk-engineering.com
www.itk-career.com

Founded in 1994
Branch offices throughout Germany – ITK companies worldwide.

Follow us on: