idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

fortiss - Landesforschungsinstitut des Freistaats Bayern für softwareintensive Systeme
Silvia Hervé

06/30/2021
http://idw-online.de/en/news771826

Research results, Transfer of Science or Research
Electrical engineering, Information technology, Traffic / transport
transregional, national

Thinking about security from the start

The vision of autonomous driving is constantly drawing ever nearer and apart from major economic success, it promises improved traffic safety. But with the development and implementation of self-driving vehicles at the latest, manufacturers now have to deal with a new challenge that the traditional IT industry has long had to deal with: cyber attacks. The ISO 21434 standard defines the path to more security in the future. With its white paper "Security Engineering for ISO 21434", fortiss is for the first time providing a practical implementation guideline for engineers in the automobile industry.

The ISO 21434 standard is a key step towards increased vehicle security since it addresses one of the most important challenges arising from the increased utilization of information and communications technologies in vehicles. With a view toward automobile manufacturers, this now calls for implementing these requirements and making the associated complexities tangible. In the future, vehicle-specific cybersecurity management systems must be implemented in vehicles. What does this mean today for developers and engineers? Automobile manufacturers are not the only ones affected. Development departments at original equipment manufacturers (OEMs), suppliers and numerous development service providers are impacted as well. Cybersecurity in connected vehicles is a "must" issue for all of these target groups and will one day become a permanent task that will not end when the customer takes possession of the vehicle.

The implementation guideline "Security Engineering for ISO 21434" from fortiss addresses precisely this issue, explains the standard and its components, and supports engineers to carry out the most efficient implementation.

Safety and security during the entire vehicle life cycle

The ISO 21434 industry standard is based on the requirements for the approaches and methods for assessing the security risks. This foundation is used to create arguments that the vehicle security should guarantee. Given the complexity of connected vehicles and tight production deadlines, it's simply not possible to execute all of the predefined activities and understand all artifacts without automation. Furthermore, cybersecurity is a continuous task since many new vulnerabilities and attacks are discovered after production, which then requires new measures and analyses again.

Scientists at fortiss are recommending a security engineering approach in order to extensively satisfy the cybersecurity requirements at the start of vehicle development. This approach contains appropriate automated methods to help ensure that (implicit) assumptions are not overlooked or that necessary risks between cybersecurity and functional safety are taken into account. Using practical application examples, the white paper illustrates that the recommended approach significantly improves efficiency when creating artifacts and can enable continuous security analyses. The paper then shows other important research approaches for realizing the recommended approach with as much automation as possible.

Challenge: implementing ISO 21434 in concrete development projects

The white paper is targeted toward all cybersecurity engineers in the automobile industry who currently face the challenge of implementing ISO 21434 in concrete development projects. Engineers should be put in the position of being able to develop a clear picture of ISO 21434, especially in terms of the risk assessment activities. And they will understand that parts of ISO 21434 can be automated with suitable methods. As a result they will gain a clear perspective on how a continuous vehicle security analysis can be implemented through an incremental approach.

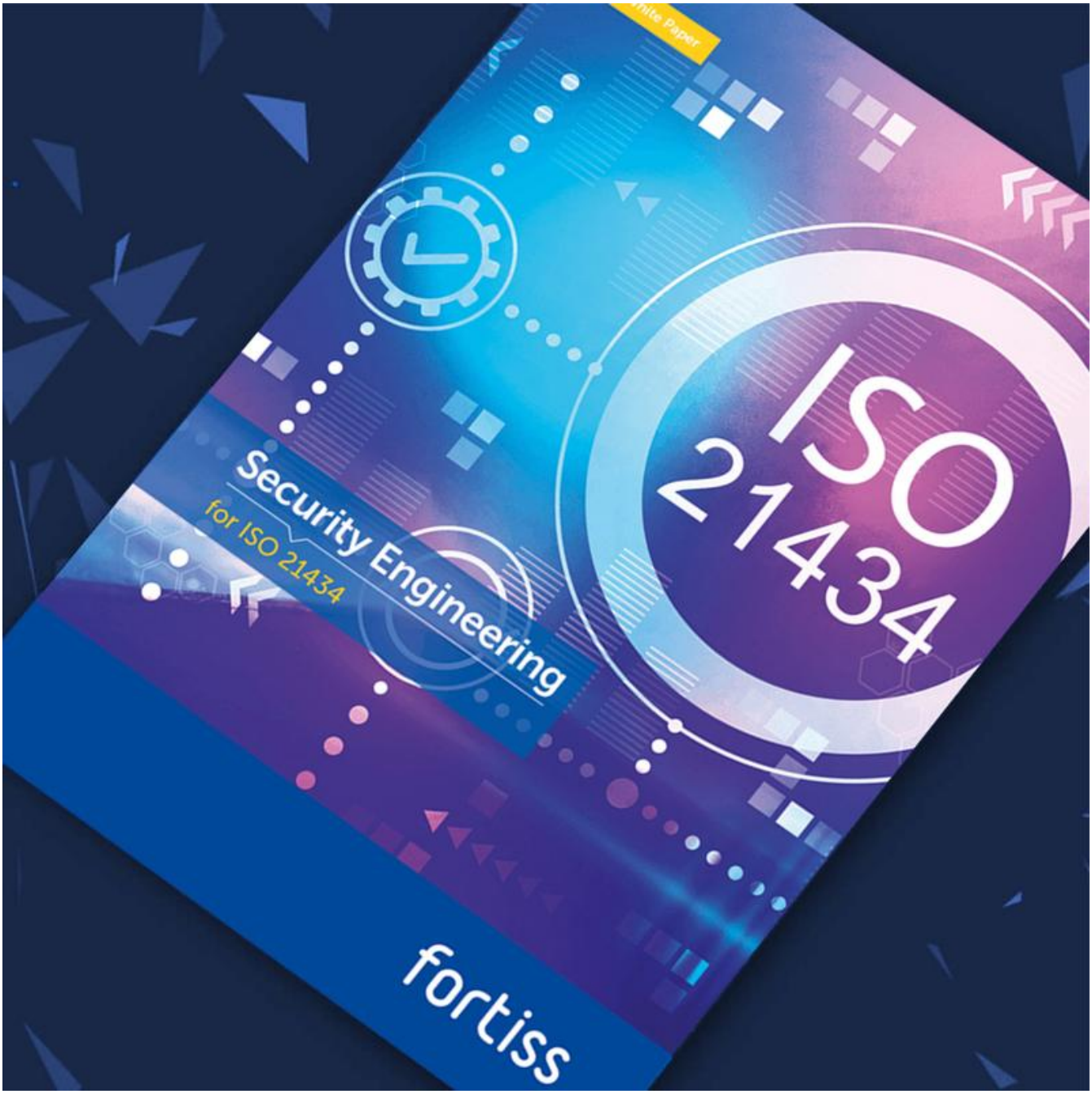
contact for scientific information:

Dr. Harald Rueß
Scientific Managing Director
fortiss GmbH
Research Institute of the Free State of Bavaria
for software-intensive systems
Phone: +49 89 3603522 0
Email: ruess@fortiss.org

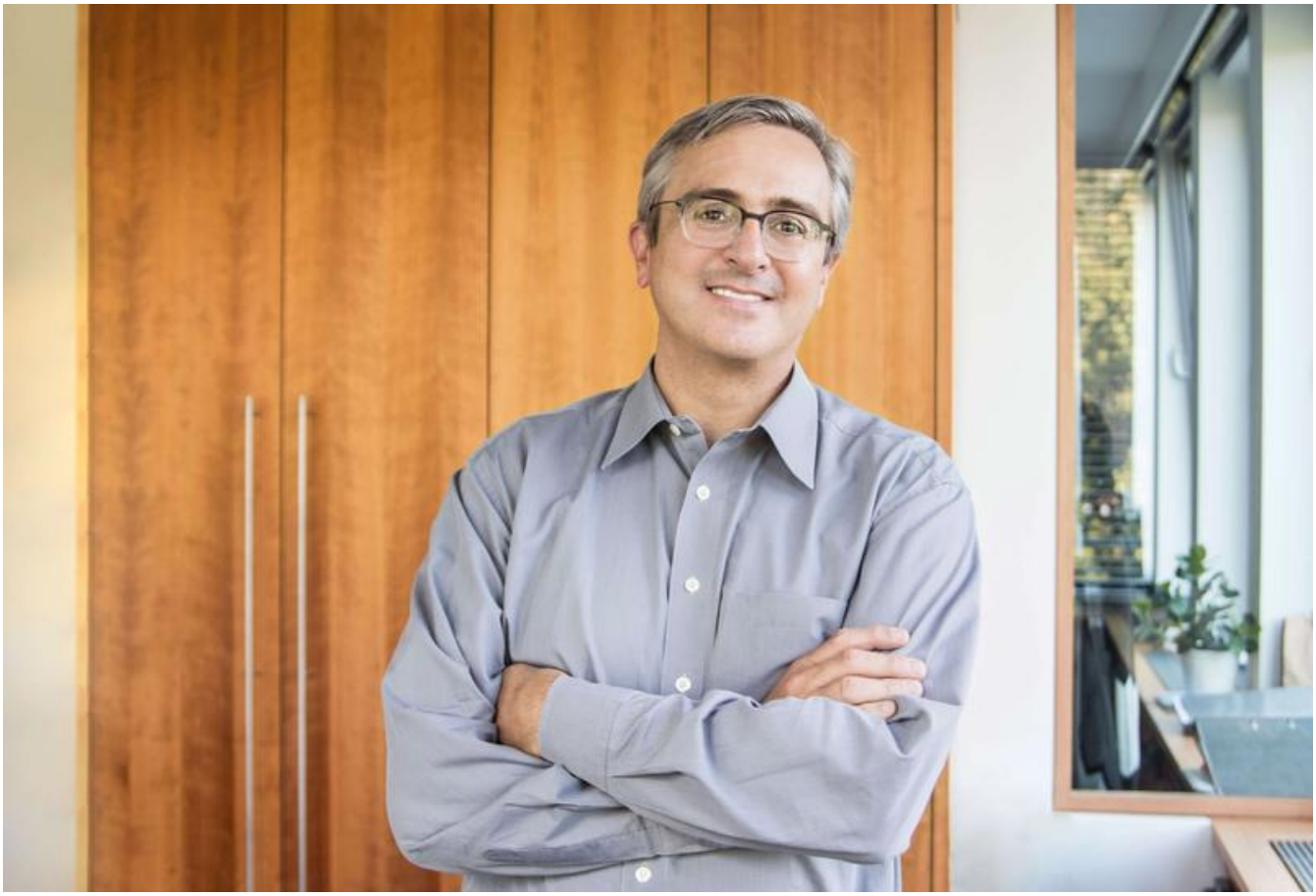
Original publication:

ISSN Print 2699-1217
ISSN Online 2700-2977

Attachment fortiss whitepaper Security Engineering for ISO 21434 http://idw-online.de/en/attachment86947



fortiss whitepaper Security Engineering for ISO 21434



Dr. Harald Rueß, Scientific Managing Director fortiss GmbH