Synopsys Automotive Solution Seminar 2019

【Date/Place】

Feb. 27, 2019 (Wed)
Seminar : 10:45～17:55 (Registration 10:15～) Networking Party : 18:00～19:30

Tokyo Conference Center, Shinagawa 4F
https://www.tokyo-cc.co.jp/eng/shinagawa/index.html#access

【Agenda】

Time	【 Keynote 】
10:15	Registration starts
10:45-11:45	**【Keynote】 Shift left - Disrupting the Current Automotive Development Process** **Dr. Burkhard Huhnke** VP Automotive Corporate Marketing Group **Synopsys, Inc.** In the automotive world, recalls for electronics affects about five percent of the vehicles on the road. That means 5 out of every 100 vehicles today has a problem with their electronics. If we want to see more autonomous driving vehicles, there must be more robustness in the development process. Unlike a blue screen of death that may occur on a desktop or laptop computer, a chip or software failure within a vehicle traveling at highways speeds could result in significant injury or death to the driver, their passengers, or others. Preventing this possibility requires building in functional safety. Specifically, ISO 26262 sets out definition for various Automotive Safety Integrity (ASIL) levels with Level D (ASIL-D) being the highest automotive software integrity level, and often the hardest to achieve. To guarantee the safety of any vehicle, ASIL-D must be a part of even the smallest pieces of electronics. Robust design can and should begin at the SOC level by integrating functional safety from automotive industry. In other words, functional safety doesn't have to wait until later -- in the system world, in the ECU world – it can be built into the chip design itself. This can be done with a virtual prototype, a model of the hardware in development, which can allow software development on those SOCs to begin at a very early phase. This keynote talks about automotive SOCs including functional safety design/verification

	and tools to optimize the quality, security, and safety in the entire automotive development process. **Latest Bio** **Dr. Burkhard Huhnke** Dr. Burkhard Huhnke is the Vice President of Automotive at Synopsys. Prior to Synopsys, he was SVP of Product Innovation & E-Mobility at VW, based in Silicon Valley. He was responsible for synchronizing VW's innovation activities and alliances to identify new concept ideas, business models and partners in the US and had end-to-end ownership of the electric vehicle platform in North America. He also held several positions both in the US and Germany, including Senior GM, Electronics System Integration and Whole Vehicle Integration. Dr. Huhnke studied electrical engineering, at the University of Braunschweig. Dr. Huhnke serves as Research Fellow the Hult Business School in San Francisco, and is a member of the Board of Advisors at the College of Engineering at University of Tennessee Knoxville and at the College of Engineering.
11:45-12:45	**Lunch** Lunch Boxes will be served
12:45-	**Breakout sessions** **【 Track 1: Designing for Autonomous-Drive and ADAS 】** **【 Track 2: "Shift-Left" System Level SW Quality and Security 】** ↓ ↓ ↓ **See following pages for details of each Track.** ↓ ↓ ↓

Time	【Track 1:　Designing for Autonomous-Drive and ADAS】
12:45-13:30	**Designing SoCs for Autonomous-Drive and ADAS** **Ron DiGiuseppe** Sr. Product Marketing Manager Solutions Group **Synopsys, Inc.** As automakers plan for autonomous driving (AD), the systems and architectures used in modern automotive SoCs require increasing levels of functionality. Driven by new safety features and content; AD, ADAS and infotainment systems are evolving from distributed ECUs to integrated domain controllers with higher Automotive Safety Integrity Levels (ASILs). This session will review the increased requirements of leading edge SoCs and show how semiconductor suppliers including automotive IP suppliers are meeting the latest requirements. The session will highlight the IP required to implement automotive SoCs built on advanced FinFET processes, and how IP providers can help automotive SoC suppliers obtain a fast path to volume production.
13:30-14:15	**Deep Learning Requirements and Solutions for Processors in Autonomous Vehicles** **Pierre Paulin** Director, R&D Solutions Group **Synopsys, Inc.** Deep learning techniques for embedded vision processors are enabling cars to 'see' their surroundings and have become a critical component in the push toward fully autonomous vehicles. The early use of deep learning for object detection, e.g., pedestrian detection and collision avoidance, is evolving toward scene segmentation where every pixel of a high-resolution video stream must be instantaneously identified and judged. Embedded vision solutions will be a key enabler for making automobiles fully autonomous. Giving an automobile a set of eyes – in the form of multiple cameras and image sensors – is a first step, but processors within the automobile must quickly interpret content from those images and react. To accomplish this, embedded vision processors must be hardware-optimized for ADAS-levels of performance while achieving low power and small area, and have high-productivity tools to program the hardware efficiently. Those tools should be based on industry standards like OpenCV, OpenVX, OpenCL and C/C++ for classical vision functions. For deep learning-based parts of the application, support for leading AI frameworks like Tensorflow, Caffe and multiple others supported by the recent ONNX exchange format are required. This presentation will discuss the current and next-generation requirements for ADAS vision applications, and solutions for high-performance mapping of classical vision and deep

	learning-based applications onto a low-power, embedded processing platform with scalable performance. It will also discuss low-cost solutions for ASIL B and D functional safety which are essential in automotive applications.
14:15-14:40	**Coffee Break**
14:40-15:40	**Accelerating the Path to a Safe and Secure SoC** **Rich Collins** Sr. Product Marketing Manager Solutions Group **Synopsys, Inc.** As more SoC designs are used in electronic systems deployed in safety-critical applications, functional safety is an important consideration in system architecture. This session will outline the key requirements for ISO 26262 as they relate to processor IP and demonstrate how leveraging an SoC safety management architecture for SoC safety bring-up, functional safety testing, MBIST/LBIST control, and overall monitoring and executing safety escalations provides an ideal solution for deterministic safety decisions across complex SoCs.
15:40-16:10	**BIST for Safety Critical Designs** **Steve Pateras** Sr. Marketing Director Design Group **Synopsys, Inc.** Safety-critical circuits must check for errors during operation to comply with the ISO 26262 standard. Logic BIST is an increasingly popular approach for testing logic portions of automotive devices both at power-up as well as periodically during functional operation. Advanced LBIST solutions adapt to design styles and constraints and have minimal impact on design performance and area.
16:10-16:20	**Break**
16:20-16:50	**Accelerating IP and SoC Functional Safety Verification** **Marc Serughetti** Sr. Product Marketing Director Verification Group **Synopsys, Inc.**

	Semiconductor companies targeting automotive application need to address the ISO 26262 functional safety verification requirements. These requirements are expected to increase effort and cost by 30% with because of more complex design over existing MCU or because functional safety is a new requirement not addressed previously. Meeting ISO 26262 certification timeline while managing efforts and costs requires an integrated automation solution from FMEA to functional safety verification and generation of work products. Do you have what is required?
16:50-17:20	**Soft Error Analysis for Functional Safety Design** **Steve Pateras** Sr. Marketing Director Design Group **Synopsys, Inc.** Soft errors are hardware disturbances caused by external factors such as radiation that lead to bit-flip in registers which can cause catastrophic failures. This tutorial shows how static analysis of soft error propagation can be used either at RTL or gates to calculate the probability of avoiding a failure as reflected in the Single Point Fault Metric (SPFM). The analysis also provides the ability to identify and address hotspots to improve design functional safety.
17:20-17:50	**Are Your Engines Fast Enough?** **Yukio Mogi** Verification Group **Nihon Synopsys** Fault campaign is a significant part of the ISO 26262 functional safety verification task for semiconductor companies. With increased SoC complexity, achieving the expected results will require both fast and integrated engines delivering comprehensive and aggregated results. Using concurrent fault simulation engines, applying formal methods and leverage fast emulation platforms, we will discuss how to optimally use each engine in your functional safety verification flow.
17:50-17:55	**Wrap Up**
18:00-19:30	**Networking Party**

Time	【Track 2: "Shift-Left" System Level SW Quality and Security】
12:45-13:30	**Assuring software quality, security, and safety in automotive** **Andreas Kuehlmann** Co-GM, Corporate Staff Software Integrity Group **Synopsys, Inc.** The emergence of advanced driving assistance system is an example of the rapidly increasing importance of software in modern automobiles. Yet, faulty software would not only impact the proper functioning of a vehicle but can also have catastrophic consequences on the safety of its passengers. In this talk, we will discuss how quality, security, and safety can be addresses during the software development process by using modern tools and methodologies.
13:30-14:15	**The present and future of automotive security: a hacker's perspective** **Naohide Waguri** Manager Automotive Security **FFRI, Inc.** In the overall of history of the battle of cybersecurity, the history of embedded and automotive security is relatively new. Until now, automotive technology has succeeded in providing a more comfortable user experience by incorporating various technologies, but at the same time many engineers, especially researchers and white hackers, alarmed about automotive security, so we realized that we must seriously think about automotive cyber security. In near future (or already), it seems that vehicles will need to be connected more for higher-level autonomous driving and mobility. Along with that, diversification of services such as ride-hailing services will progress. In that world, what do security engineers and malicious hackers focus their attention on regarding automotive security? In this session, I will explain the importance of security measures and discuss the "Now" and the "Future" of automotive security based on actual hacking examples and examples from our projects.

Naohide Waguri - Bio :

After he was working as quality assurance and developer for network switches for 8 years, he joined FFRI as a researcher. He was writing research papers, speaking at Code Blue, and writing for SCIS from 2015 to 2016. He took on his current position as division chief of automotive security in 2017. His specialty is embedded and network security though, he is full of curiosity and his motto is “try anything interesting”.

14:15-14:40	**Coffee Break**
14:40-15:25	**Virtualize your SW development or be left behind!** **Marc Serughetti** Sr. Product Marketing Director Verification Group **Synopsys, Inc.** Reducing your development from 5 to 2 years? Increasing you testing throughput? Vehicles electronic content is increasing and becoming more complex. Physical systems availability is a bottleneck to an earlier and more agile software development, integration and test process. Virtual environment have been a proven approach to eliminate such bottleneck and accelerate development. Automotive Tier 1 and OEM focusing on accelerating system development for the next generation domain controller unit must move from physical to virtual test platform or be left behind.
15:25-16:10	**CI/CD as your Accelerator Pedal** - ***Driving DevOps and CI/CD Practices into Automotive Production Methodologies*** **Ofer Maor** Product Marketing Director Software Integrity Group **Synopsys, Inc.** Over the past few years, software development has taken the front seat in Automotive production; yet, a strong reliance on legacy software development methodologies remains strongly coupled with legacy hardware development methodologies and its constraints. Be that, with this increasingly rising volume of software development and the changing competitive landscape demanding faster time-to-market, the adoption of faster software development methodologies, including CI/CD (Continuous

	Integration/Continuous Delivery) and DevOps, into the Automotive world is inevitable. This talk will feature an overview of the challenges faced in adopting these methodologies in the Automotive space as they pertain to software quality and security, and what can organizations do in order to mitigate such risks and move towards rapid development, both on the backend and on the system side.
16:10-16:20	**Break**
16:20-17:05	**Crossing the Chasm: From defining the cyber-risk to monitoring its realization** **Yuval Weisglass** Vice Prresident Automotive Cybersecurity Business Unit **HARMAN** As the automotive industry generates a growing number of connected, computer-controlled, vehicles it is also expected to invest in securing cars against cybersecurity threats. Significant attention has been given in the recent years on maturing a security-by-design approach where the risk is properly identified in advance so proper security measures could be put in place to mitigate or lower such risk. While putting security in place is a necessity, how do we measure its effectiveness? Can we prove return on investment? How can we better define the strategy moving forward without first answering some of these fundamental questions? In his talk, Yuval will present some real-world examples where proper security monitoring enabled car manufacturers to identify security shortcomings, unveil ineffective protection measures and create added-value using data-driven security analytics. **Yuval Weisglass - Bio :** Yuval Weisglass is Vice President for R&D, Automotive Cyber Security at HARMAN, a wholly-owned subsidiary of Samsung Electronics Co., Ltd. HARMAN designs and engineers connected products and solutions for automakers, consumers, and enterprises worldwide, including connected car systems, cyber security solutions, audio and visual products, enterprise automation solutions and services supporting the Internet of Things. Yuval joined HARMAN with the acquisition of TowerSec in January 2016 where he served as Co-Founder & CTO.

	Yuval has over 15 years of experience in cyber security both as a security researcher and as a leader of R&D groups specializing in security-related innovation projects. Among Yuval's unique expertise are: security research and security design of embedded systems, research of side-channel attacks on secured elements, security for cellular technology and long-time hobby of reverse engineering vehicle's systems. Before founding TowerSec in 2013, Yuval spent 11 years at the Israeli Security Agency where he held senior R&D management roles in the field of Cyber Security. Yuval is an alumni of the elite intelligence 8200 Unit of the Israel Defense Forces, where he served as an officer in the field of advanced technology research.
17:05-17:50	**The Future of Automotive Cybersecurity** **Matan Scharf** Sr. Product Marketing Manager Software Integrity Group **Synopsys, Inc.** The changing of the traditional OEM role, the emerging hyper-connectivity of 5G, and the imminent vision of autonomous/driverless vehicles, is reshaping the threat landscape for automotive cybersecurity. What are the challenges that the industry will face and what should be the strategy that will mitigate the risks and support the business growth into the mobility digital era.
17:50-17:55	**Wrap Up**
18:00-19:30	**Networking Party**

※ Please note that the program may change.