Building Secure Automotive IoT Applications : Developing Robust IoT Solutions for Next-Gen Automotive Software /

Oka, Dennis Kengo,
author

Monografía

Enhance your automotive IoT design and development knowledge by learning vehicle architectures, cybersecurity best practices, cloud applications, and software development processes Key Features Explore modern vehicle architectures designed to support automotive IoT use cases Discover cybersecurity practices and processes to develop secure automotive IoT applications Gain insights into how cloud technologies and services power automotive IoT applications Purchase of the print or Kindle book includes a free PDF eBook Book Description Software-defined vehicles, equipped with extensive computing power and connectivity, are unlocking new possibilities in automotive Internet of Things (IoT) applications, creating a critical need for skilled software engineers to lead innovation in the automotive sector. This book equips you to thrive in this industry by learning automotive IoT software development. The book starts by examining the current trends in automotive technology, highlighting IoT applications and key vehicle architectures, including the AUTOSAR platform. It delves into both classic and service-oriented vehicle diagnostics before covering robust security practices for automotive IoT development. You'll learn how to adhere to industry standards such as ISO/SAE 21434, ASPICE for cybersecurity, and DevSecOps principles, with practical guidance on establishing a secure software development platform. Advancing to the system design of an automotive IoT application, you'll be guided through the development of a remote vehicle diagnostics application and progress through chapters step by step, addressing the critical aspects of deploying and maintaining IoT applications in production environments. By the end of the book, you'll be ready to integrate all the concepts you've learned to form a comprehensive framework of processes and best practices for embedded automotive development. What you will learn Explore the current automotive landscape and IoT tech trends Examine automotive IoT use cases such as phone-as-a-key, predictive maintenance, and V2X Grasp standard frameworks such as classic and adaptive AUTOSAR Get to grips with vehicle diagnostic protocols such as UDS, DoIP, and SOVD Establish a secure development process and mitigate software supply chain risks with CIAD, RASIC, and SBOM Leverage ASPICE and functional safety processes for industry standards compliance Understand how to design, develop, and deploy an automotive IoT application Who this book is for This book is for embedded developers and software engineers working in the automotive industry looking to learn IoT development, as well as IoT developers who want to learn automotive development. A fundamental grasp of software development will assist with understanding the concepts covered in the book

Título: Building Secure Automotive IoT Applications Developing Robust IoT Solutions for Next-Gen Automotive Software Dennis Kengo Oka [and four others]

Edición: First edition

Editorial: Birmingham, England Packt Publishing [2024] 2024

Descripción física: 1 online resource (358 pages)

Bibliografía: Includes bibliographical references and index

Contenido: Cover -- Copyright -- Foreword -- Contributors -- Table of Contents -- Preface -- Part 1: Introduction to Automotive IoT -- Chapter 1: Automotive Technology Trends -- Overview of current automotive trends -- CASE -- SDV and SOA -- Mobile apps and the cloud -- Modern software development -- Standards and regulations -- Introduction to automotive IoT -- Automotive IoT -- Automotive IoT use case examples -- Data management for automotive IoT use cases -- Summary -- References -- Chapter 2: Introducing Automotive IoT Use Cases -- Phone as a key -- Personalized in-car experience -- Connected car services -- Enhanced driver experience and safety -- Optimized fleet management -- Real-time vehicle tracking and telematics -- Driver performance monitoring -- Predictive maintenance -- Connected mobility revolution -- Smart parking solutions -- Vehicle-to-Everything (V2X) communication -- Connected supply chain and manufacturing -- Summary -- References -- Advanced driver-assistance systems -- Part 2: Vehicle Architectures -- Chapter 3: Vehicle Architecture and Frameworks -- The scale of vehicle architecture -- Distributed architecture -- Centralized zonal domain architecture -- A central computer with multiple domain-specific SoCs -- A central computer with a single SoC -- Standard frameworks to support vehicle architecture and IoT -- A high-level overview of the domain controller -- Summary -- References -- Chapter 4: Vehicle Diagnostics -- UDS -- UDS message structure -- DoIP -- DoIP message format -- DoIP example message flow -- Diagnostic communication workflow in Classic AUTOSAR -- Diagnostic service management in Adaptive AUTOSAR -- Reflecting on the application of remote diagnostics -- Summary -- References -- Chapter 5: Next Wave of Vehicle Diagnostics -- Technical requirements -- Needs beyond UDS -- SOVD -- REST SOVD example, demo, and details -- Example of a diagnostic message using UDS and SOVD -- Example of an SOVD interface as part of applications on the server side -- SOVD documentation and demo -- SOVD and UDS comparison -- Summary -- References -- Part 3: Secure Development for Automotive IoT -- Chapter 6: Exploring Secure Development Processes for Automotive IoT -- An overview of security threats and the need for security and secure development processes -- New cybersecurity threats -- Examples of recent attacks -- Simplified threat model of automotive IoT ecosystem -- ISO/SAE 21434 and ASPICE for Cybersecurity -- ISO/SAE 21434 Overview -- ISO/SAE 21434 organizational-level requirements -- ISO/SAE 21434 project-level requirements -- ASPICE for Cybersecurity overview -- ASPICE for Cybersecurity - security activities -- NIST Cybersecurity Framework, ISO 27001, SOC 2, and OWASP -- NIST Cybersecurity Framework -- ISO 27001 -- SOC 2 -- OWASP -- DevSecOps and agile development -- V-model -- Agile -- Scrum -- DevSecOps -- Summary -- References -- Chapter 7: Establishing a Secure Software Development Platform -- Activities in the SSDLC -- TARA/threat model -- Requirements review -- Design review -- Code review -- Static application security testing -- Vulnerability scanning -- Fuzz testing -- Dynamic application security testing -- Interactive application security testing -- Penetration testing -- Project inventory -- Project information and risk level -- Cybersecurity assurance level and activities -- Example project inventory -- Practical steps for establishing a secure software development platform -- Purpose and need -- Overview of the secure software development platform -- Requirements, policies, and compliance -- Vulnerability management -- AppSec tooling -- Common AppSec tooling and test approaches -- SAST -- SCA -- DAST -- Fuzz testing Penetration testing -- Summary -- References -- Chapter 8: Securing the Software Supply Chain -- Software supply chain and distributed development -- Overview of the software supply chain -- RASIC, vendor security assessments, and CIADs -- RASIC -- Vendor security assessments -- CIADs -- Managing risks with OSS -- Security vulnerabilities -- License compliance -- Operational risk -- SBOM -- SBOM formats -- Executive Order 14028 -- NTIA -- OpenChain -- Secure software supply chain risk management -- Identifying the risks -- Assessing the risks -- Mitigating the risks -- Summary -- References -- Part 4: Automotive IoT Application Life Cycle -- Chapter 9: System Design of an Automotive IoT Application -- System design process overview -- UXDD -- Use case - remote diagnostics -- System components -- Vehicle telematics gateway -- Vehicle cloud platform -- End-user mobile device -- Gateway design considerations -- GNSS receivers -- Wireless communication -- Wired communication -- CAN -- Sensors -- SIM/eSIM -- Gateway hardware -- Cloud design

considerations -- Device management -- Connectivity management -- Remote diagnostics applications -- Classic vehicle ECU diagnostics -- Service-oriented vehicle diagnostics -- Regulatory compliance -- Build versus buy -- Summary -- References -- Chapter 10: Developing an Automotive IoT Application -- Cloud backend deployment and service models -- Deployment models -- Service models -- Server-based and serverless computing -- IoT application architecture -- Cloud device gateway -- Edge computing -- Stream processing -- Device management -- OTA solutions -- Telemetry datastore -- Rule engine -- Application Programming Interface (API) gateway -- Connectivity management -- IAM -- Vehicle telematics gateway -- Remote diagnostics application -- Predictive maintenance -- Development process -- Summary -- References Chapter 11: Deploying and Maintaining an Automotive IoT Application -- The DevSecOps life cycle -- The plan stage -- CI -- The code stage -- The build stage -- The test stage -- CD -- The release stage -- The deploy stage -- The operate stage -- The monitor stage -- Summary -- References -- Part 5: Putting It All Together -- Chapter 12: Processes and Practices -- Introduction to processes and practices -- ASPICE -- SWE.1 - Software Requirements Analysis -- SWE.2 - Software Architectural Design -- SWE.3 - Software Detailed Design and Unit Construction -- SWE.4 - Software Unit Verification -- SWE.5 - Software Integration and Integration Test -- SWE.6 - Software Qualification Test -- Functional safety -- Vocabulary -- Risk classification system -- Development process -- Additional automotive processes and practices -- DFMEA -- 5 Whys root cause analysis -- Fishbone -- A-B-A testing -- Summary -- Reference -- Chapter 13: Embedded Automotive IoT Development -- Embedded software development -- Electrical engineering -- Schematics/block diagrams -- Datasheets, errata, and application notes -- Device drivers -- Hardware Abstraction Layer (HAL) -- Additional aspects of embedded development -- Automotive-focused aspects -- Power state management -- Operating systems -- Hypervisors -- Development tools -- Life cycle management tools -- Software development ecosystem -- You and your customers -- You and your co-suppliers -- You and your suppliers -- Summary -- References -- Chapter 14: Final Thoughts -- Agile -- Agile+ASPICE -- Automotive embedded testing -- Types of testing -- Security -- Summary -- References -- Index -- Other Books You May Enjoy

ISBN: 1-83546-284-7

Materia: Automotive computers Software engineering Software architecture Internet of things Application software- Development Embedded computer systems Automobiles- Design and construction

Enlace a formato físico adicional: 1-83546-550-1

Baratz Innovación Documental

- Gran Vía, 59 28013 Madrid
- (+34) 91 456 03 60
- informa@baratz.es