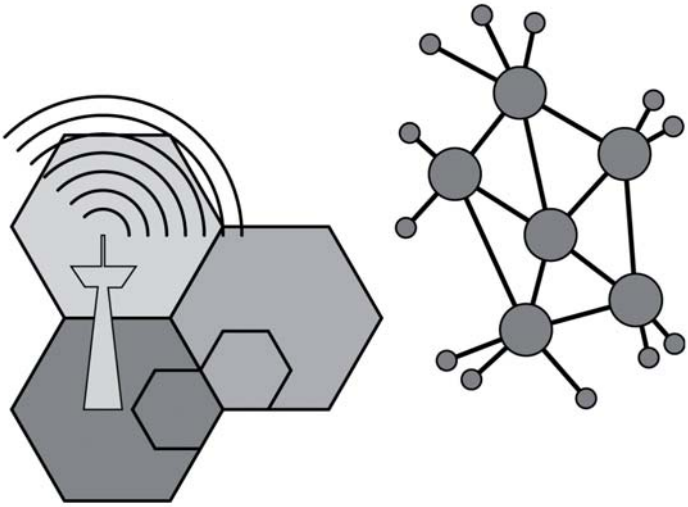
UNIVERSITÄT SIEGEN
Institut für Digitale Kommunikationssysteme

Forschungsberichte

Band 35 Herausgeber: Univ.-Prof. Dr. Christoph Ruland



Thomas Koller

Communication Security for Distributed Mixed-Criticality Systems

2018

SHAKER VERLAG

Communication Security for Distributed Mixed-Criticality Systems

DISSERTATION
zur Erlangung des Grades eines Doktors
der Ingenieurwissenschaften

vorgelegt von
Dipl.-Inform. Thomas Koller
geb. am 31.12.1988 in Kirchen (Sieg)

eingereicht bei der Naturwissenschaftlich-Technischen Fakultät
der Universität Siegen
Siegen 2017

1. Gutachter: Univ.-Prof. Dr. rer. nat. Christoph Ruland
2. Gutachter: Prof. Dipl.-Ing. Dr. Gerhard Fohler
Vorsitzender: Prof. Dr. rer. nat. habil. Frank Gronwald

Tag der mündlichen Prüfung: 01.12.2017

UNIVERSITÄT SIEGEN

Institut für
Digitale Kommunikationssysteme

Forschungsberichte

Herausgeber: Univ.-Prof. Dr. Christoph Ruland

Band 35

Thomas Koller

Communication Security for Distributed Mixed-Criticality Systems

SHAKER
VERLAG

Aachen 2018

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Siegen, Univ., Diss., 2017

Printed in Germany.

ISBN 978-3-8440-5693-8
ISSN 1614-0508

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • e-mail: info@shaker.de

Abstract

The increasing computational power of embedded systems allows the usage of various applications in one system. These applications may possess diverse safety requirements and have to be classified into different criticality levels. Systems that execute applications of different criticality levels are called Mixed-Criticality Systems (MCSs). In addition to the increasing computational power of embedded systems, there is the trend to interconnect the individual MCSs to distributed MCS. Assuring the safety of a system protects against unintended faults. Intentional faults are often not covered by safety. They may also lead to a failure of the system. To protect the system against intentional faults, security services have to be used. Hence, there is no safety without security. The dependability of the communication is important in safety critical systems. The usage of secure communication services can prevent attacks that lead to a fault. Security in distributed MCSs was barely addressed by now. This work proposes the extension of the core services of a distributed MCSs by secure communication services.

First, the architecture of a distributed MCS is introduced and its core services are explained. The architecture and the core services are analyzed regarding threats, followed by a discussion on attack scenarios. The attacks are divided into internal and external attackers. The analysis of the architecture allows the classification of the system into different security domains. These security domains are the cluster level and the application level. Security services for these domains are defined and grouped into security levels. Security services on the cluster level protects the communication between the subsystems. The core service time synchronization is an example for a service using the secure cluster-level communication. Security services on the application level provide a secure end-to-end channel between applications. The usage of the application-level security is illustrated by the core service resource management. For both the application level and the cluster level, the necessary key management is

presented. Both possess individual methods for key generation and distribution, adjusted for the respective level.

The security solution for distributed MCS presented in this thesis hardens the systems against attacks and protects the system from faults that may impair the dependability of the system.

Zusammenfassung

Eingebettete Systeme werden immer leistungsfähiger und ermöglichen die Nutzung unterschiedlicher Anwendungen mit verschiedenen sicherheitskritischen Anforderungen. Systeme, deren Anwendungen unterschiedliche Kritikalitätsanforderungen haben, werden Mixed-Criticality Systems (MCSs) genannt. Gleichzeitig werden diese Systeme zunehmend vernetzt, was die Kommunikation der Komponenten und Anwendungen verschiedener verteilter Subsysteme untereinander erlaubt. In sicherheitskritischen Systemen ist die Zuverlässigkeit dieser Kommunikation von besonderer Bedeutung. Nicht nur zufällige Fehler, sondern auch aktiv herbeigeführte Fehler beeinträchtigen die Zuverlässigkeit. Um das System vor aktiv herbeigeführten Fehlern zu schützen, können Kommunikationssicherheitsdienste eingesetzt werden. Diese Arbeit befasst sich mit der Kommunikationssicherheit in verteilten MCSs.

Zunächst wird die Architektur eines verteilten MCS vorgestellt und ihre Basisdienste erläutert. Anschließend wird die Architektur und deren Basisdienste im Hinblick auf potenzielle Bedrohungen analysiert und Angriffsszenarien erläutert, die in interne und externe Angriffe unterteilt sind. Die Analyse der Architektur erlaubt die Einteilung des Systems in verschiedene Sicherheitsbereiche und -ebenen, sowie die Definition der für die Architektur erforderlichen Sicherheitsdienste. Diese Dienste müssen sowohl auf Cluster- als auch auf Applikationsebene bereitgestellt werden, da die Clusterebene zwar die Sicherheit auf den Verbindungen zwischen den Subsystemen bereitstellt, allerdings keine Ende-zu-Ende Sicherheit gewährleisten kann. Für beide Ebenen werden Sicherheitsarchitekturen mit den entsprechenden Anforderungen entwickelt. Ein Beispiel für diese Anforderungen auf Clusterebene ist der Basisdienst Zeitsynchronisation, der die Uhren der verschiedenen Systemkomponenten synchronisiert. Die Sicherheitsmechanismen der Clusterebene bauen auf bestehende Protokolle auf. Für die Applikationsebene ist ein eigenes Protokoll entwickelt worden. Die Anwendung der Sicherheitsdienste auf Applikationsebene wird am Beispiel des Basis-

dienstes Resource Management verdeutlicht. Beide Ebenen verfügen über eigene Methoden des Schlüsselmanagements. Schlüsselverteilung und -vereinbarung sind angepasst an die jeweilige Ebene.

Die in dieser Arbeit entwickelte Sicherheitsarchitektur für verteilte MCSs sichert das System gegen Angriffe ab und schützt das System vor Fehlern, welche die Zuverlässigkeit des Systems beeinträchtigen können.

Acknowledgements

This thesis was created during my employment at the Chair for Data Communication Systems at the University of Siegen and has been supported by the research project Distributed Real-time Architecture for Mixed Criticality System (DREAMS) of the European Union.

First and foremost, I would like to express my sincere gratitude to the chairholder of the Chair for Data Communication Systems and my adviser Univ.-Prof. Dr. rer. nat. Christoph Ruland, who provided me with the necessary means for my research, my work in the project and my regular tasks at the chair. Further, I would also like to to express my gratitude to Prof. Dipl.-Ing. Dr. Gerhard Fohler, who without hesitation agreed to act as the second reviewer for this thesis. Special thanks to Prof. Dr. rer. nat. habil. Frank Gronwald for chairing the examination commission and to Prof. Dr.-Ing. Roman Obermaisser for his participation in the commission.

I would also like to thank all of my colleagues and former colleagues Donatus Weber, Romeo Ayemele Djeujo, Robin Fay, Wilfried Kahle, Martin Kramer, Stephan Meyer, Obaid Ur-Rehman, Jochen Saßmannshausen, Andreas Schantin, Matthias Schneider, Jinsuh Shin, Amir Tabatabaei, Birgit Wichmann, Tao Wu, Sadia Zeb, Natasa Zivic, and my colleagues from the Chair for Embedded Systems, for the continuous support and the valuable discussions.

Finally, I would like to thank my family for the great and never-ending support throughout my life.

Contents