Security and Safety Considerations of the DECOS Core OS

Andreas Wolf[1], Maximilian Rosenblattl[1], and Bernhard Leiner[1]

TTTech Computertechnik AG
Schoenbrunner Strasse 7, 1040 Vienna, Austria,
phone: +43 1 5853434 0, fax: +43 1 5853434 90,
bernhard.leiner@tttech.com

Abstract. This paper presents safety and security considerations of the Core Operating System (COS) of the Encapsulated Execution Environment (EEE) developed in DECOS (Dependable Embedded Components and Systems), an integrated project within the Sixth Framework Programme of the European Commission.
It is shown that security and safety is well considered in the COS and a high level of security and safety can be achieved when systems using the COS are designed properly.
Keywords: Embedded Systems, Security, Virtualization.

1 Introduction

Reliable embedded systems have high safety requirements, especially in the automotive, aerospace or industrial control domains. As embedded systems are getting more complex with each generation and more interactivity and network connectivity is proposed, security considerations must be taken. While traditional embedded systems work in a well-defined, separated network with its own communication links and predefined environment, modern systems shall be able to work in heterogeneous networks and shall be configured dynamically. Here, security becomes a big issue as hardware and software components of different vendors are mixed and standard communication systems are used.

In the DECOS project (Dependable Embedded Components and Systems), an integrated project within the Sixth Framework Programme of the European Commission, mixed criticality subsystems are integrated into the same embedded hardware node. While safety and reliability were covered by design requirements, security and protection of intellectual property were not explicitly covered.

This paper covers security considerations which also apply to the protection of intellectual property of the integrated subsystems by analyzing the design and implementation of the Core Operating System (COS) of the DECOS Encapsulated Execution Environment (EEE).

The security considerations cover bogus and malicious subsystems on the same node as well as robustness to security attacks from outside while still considering the safety of the whole system.

As a result of the analysis an overview of vulnerabilities is given and possible solutions as well as enhancements of the COS and the hardware platform are presented.