報告番号	※甲　　第　　号

主　論　文　の　要　旨

論文題目　ADVANCED INTEGRATION TECHNIQUES FOR HIGHLY RELIABLE DUAL-OS EMBEDDED SYSTEMS
(高信頼デュアル0S組込みシステムにおける統合技術)。

氏　　名　SANGORRIN LOPEZ, Daniel

論 文 内 容 の 要 旨

This thesis considers dual-OS virtualization for consolidating a trusted real-time operating system (RTOS) and an untrusted general-purpose operating system (GPOS) onto the same hardware platform. Research on dual-OS systems is motivated by their smaller hardware cost—due to the fact that hardware is shared—and their ability to address the increasing complexity of modern embedded systems—by leveraging the GPOS advanced functionality—without affecting the timely behavior of the RTOS. The most fundamental requirement of a dual-OS system is guaranteeing the reliability and real-time performance of the RTOS against any misbehavior or malicious attack coming from the untrusted GPOS. For that reason, we use a dual-OS system (SafeG) that supports complete isolation of the memory and devices assigned to the RTOS; and gives higher priority to the execution of the RTOS. The SafeG dual-OS system is based on ARM TrustZone Security extensions, and its main component is the SafeG monitor, which is used to context-switch between both OSs.

Although the mere execution of the RTOS and the GPOS in isolation may satisfy the requirements of some systems, increasing the integration of the dual-OS system can lead to performance improvements, new collaborative applications with higher sophistication, and a further decrease of the hardware cost. The main three novel contributions to the reliable integration of a dual-OS system proposed in this thesis are: an integrated scheduling framework; efficient dual-OS communications; and repartition-based device sharing.

The integrated scheduling framework supports the interleaving of the execution priority levels of both OSs with high granularity, and uses execution-time reserva-

tions for guaranteeing the timeliness of the RTOS. The evaluation results show that the framework is suitable for enhancing the responsiveness of the GPOS time-sensitive activities without compromising the reliability and real-time performance of the RTOS.

Dual-OS communications allow RTOS and GPOS applications to collaborate in complex distributed applications. Traditional approaches are usually implemented by extending the virtualization layer with new communication primitives. We present a more efficient approach that minimizes the communication overhead caused by unnecessary copies and context switches; and satisfies the strict reliability requirements of the RTOS.

Finally, we consider mechanisms for sharing devices reliably in dual-OS systems. We note that previous approaches based on paravirtualization are not well suited to device sharing patterns where the GPOS share greatly exceeds that of the RTOS. For that reason, we propose two new approaches that are based on dynamically re-partitioning devices between the RTOS and the GPOS at run time. The evaluation results show an interesting trade-off between overhead, functionality and device latency.

38 字×23 行

学位関係

38 字×23 行