CEC Continuing Education Center

DesignNews

Secure MCUs and RTOSs

DAY 5 : Secure RTOSs

Sponsored by

Digi-Key ELECTRONICS

BENINGO EMBEDDED GROUP

informa markets

Webinar Logistics

- Turn on your system sound to hear the streaming presentation.
- If you have technical problems, click “Help” or submit a question asking for assistance.
- Participate in ‘Group Chat’ by maximizing the chat widget in your dock.

THE SPEAKER

Jacob Beningo

Visit ‘Lecturer Profile’

Beningo Embedded Group - President

Focus: Embedded Software Consulting

An independent consultant who specializes in the design of real-time, microcontroller based embedded software.
He has published two books:

- Reusable Firmware Development
- MicroPython Projects
- Embedded Software Design

Writes a weekly blog for DesignNews.com focused on embedded system design techniques and challenges.

Visit www.beningo.com to learn more …

Visit ‘Lecturer Profile’ in your console for more details.

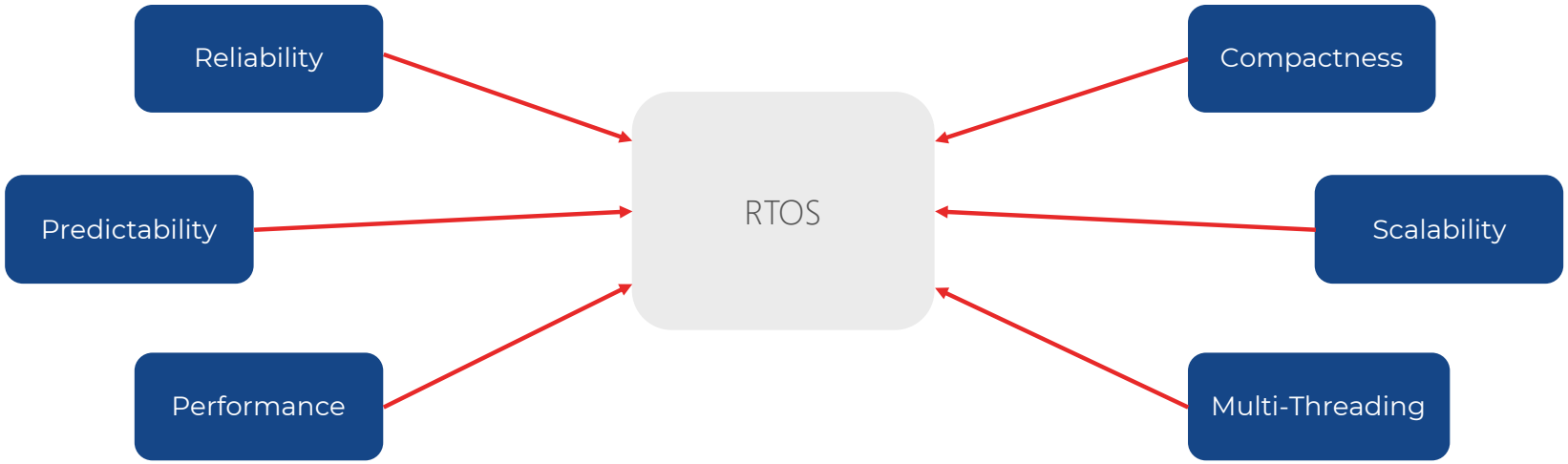
Course Sessions

- Threat Model Security Analysis (TMSA)
- Secure Microcontroller Solutions
- Arm TrustZone
- Secure Boot and Firmware Updates
- **Secure RTOSs**

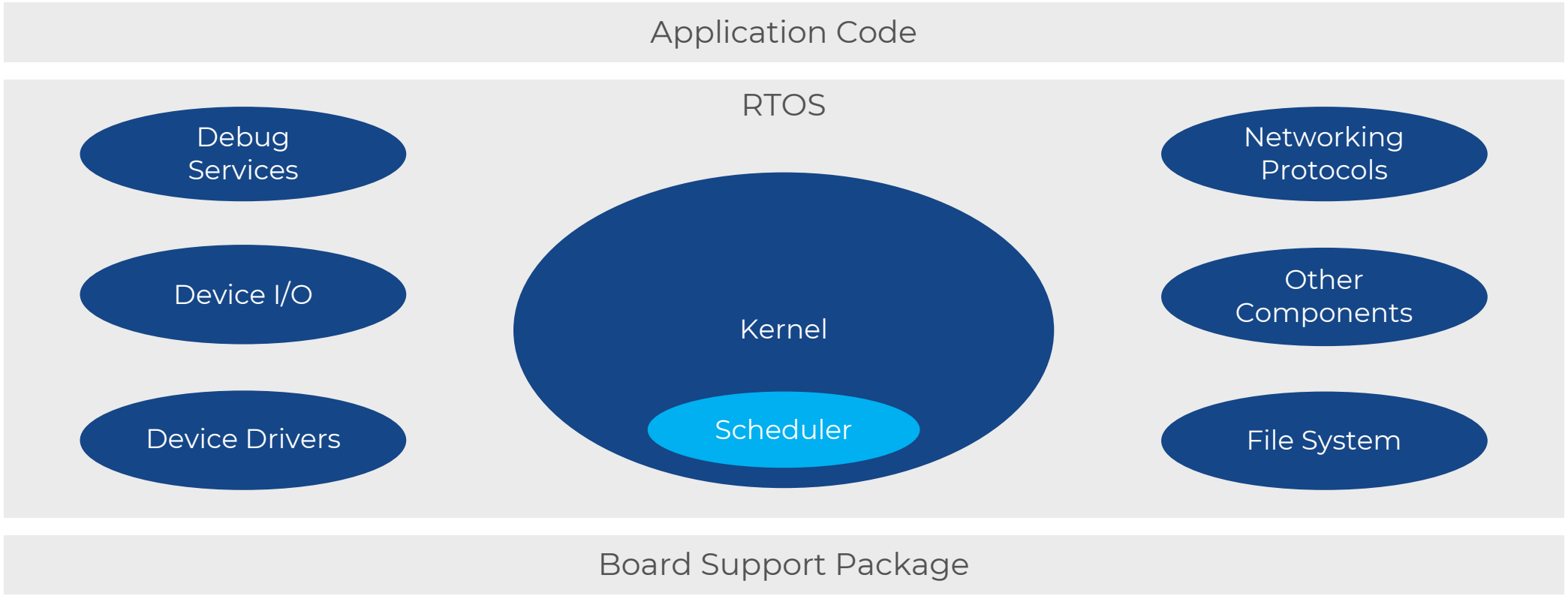
1 Real-Time Operating Systems (RTOSs)

Real-Time Operating Systems - Characteristics

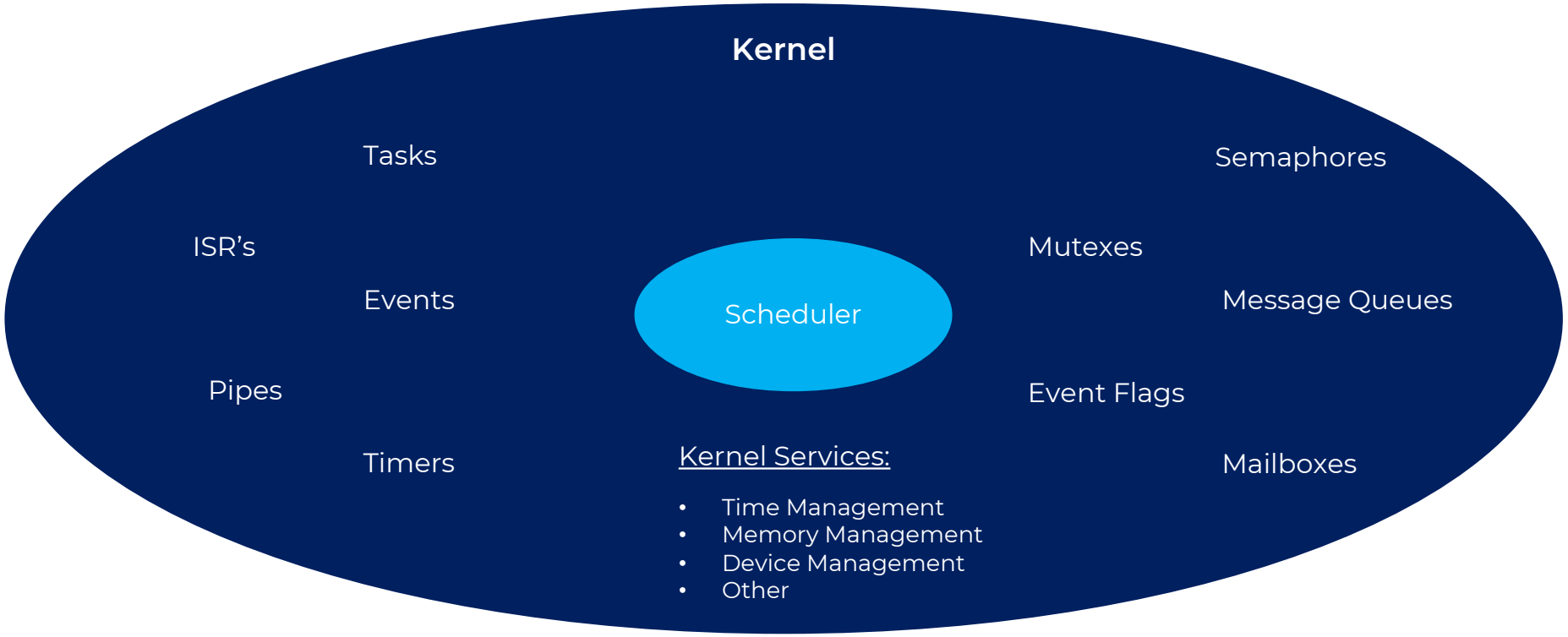
A **Real-Time Operating System (RTOS)** is an operating system designed to manage hardware resources of an embedded system with very precise timing and a high degree of reliability.



Real-Time Operating Systems – The Kernel



Real-Time Operating Systems – The Kernel



Which of the following is NOT part of an RTOS kernel?

- The scheduler
- Mutexes
- File system
- Semaphores
- Message Queues

2 Secure RTOS

Secure RTOS - Definition

A **secure Real-Time Operating System (RTOS)** is an operating system designed and implemented with a strong focus on protecting the system, its data, and its communication channels from unauthorized access, misuse, and exploitation.

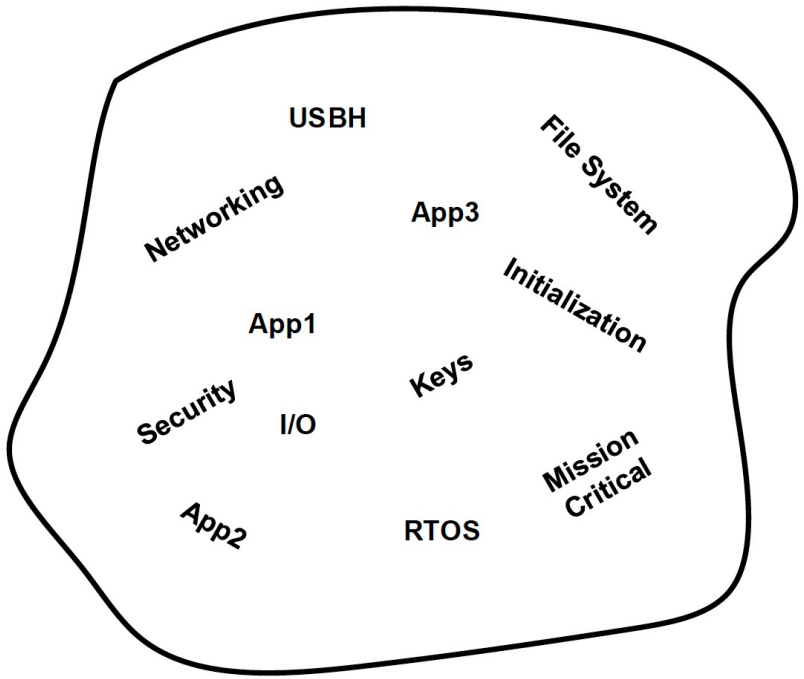
It encompasses a range of features, techniques, and best practices that collectively aim to establish a high level of security for real-time systems.

Secure RTOS - Characteristics

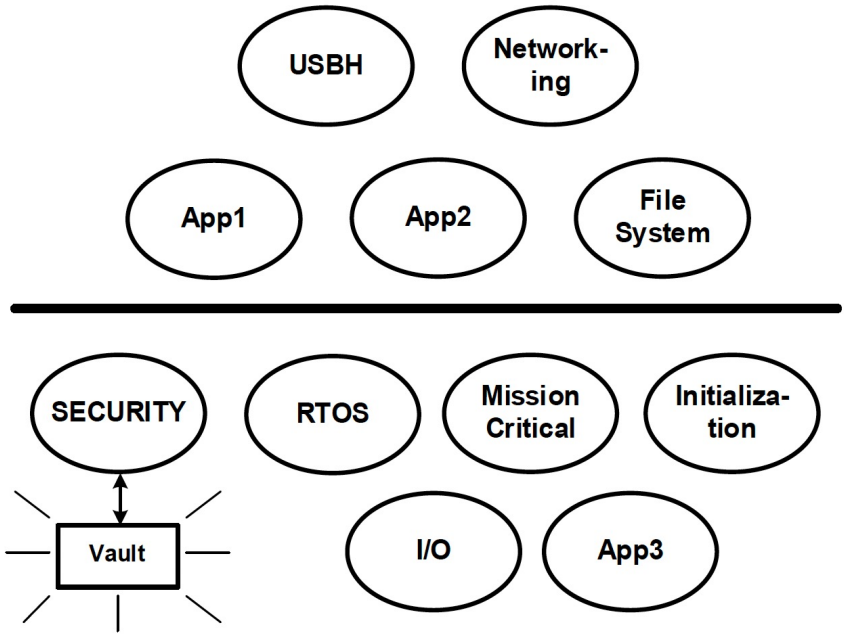
- Memory Protection
- Authentication and Authorization
- Secure Communication
- Access Control
- Security Updates and Patching
- Secure Boot
- Auditability and Logging
- Secure Configuration
- Compliance with Security Standards

Secure RTOS - Partitioning

Most RTOS Applications



Secure RTOS Applications



https://www.smxrtos.com/doc/ssmxug_peek.pdf

Which best describes your software?
- Not-partitioned
- Partitioned?

3

SecureSMX®

User Guide:
https://www.smxrtos.com/doc/ssmxug_peek.pdf

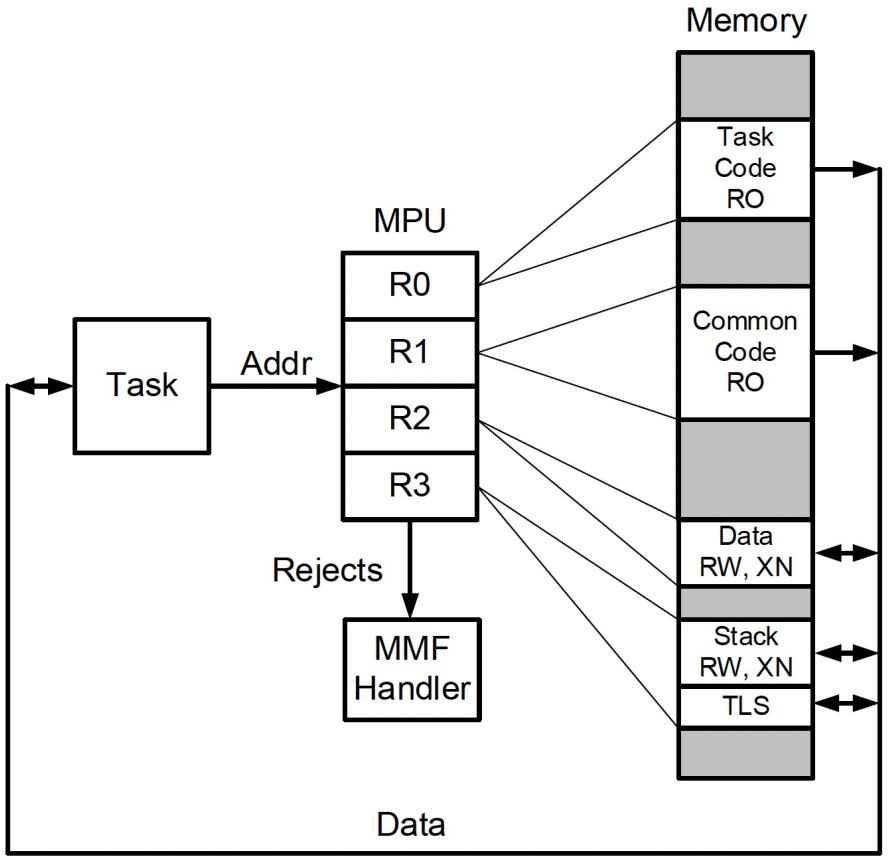
SecureSMX® - Hardware / Software Integration

SecureSMX utilizes the following security features of the Cortex v7M and v8M architectures:
1. Memory Protection Unit (MPU).
2. Privileged and Non-privileged processor levels.
3. SVC Exception.

Full partition isolation requires the following:
1. Limiting code, data, and I/O region access via the MPU.
2. Restricting access to system services via the SVC exception.
3. Dedicated heap for each partition that requires a heap.
4. Portals for communication between partitions.
5. Runtime and service limitations.

SecureSMX® - MPU Operation

The MPU provides N *slots* for N *regions*. Each region has a starting address, a size, and access parameters, such as Read-Only (RO), Read/Write (RW), eXecute Never (XN), etc. If a memory access is not permitted by a region in the MPU, a Memory Manage Fault (MMF) is generated. The MMF is an exception that causes the MMF Handler to run. It normally stops the faulting task and initiates recovery.

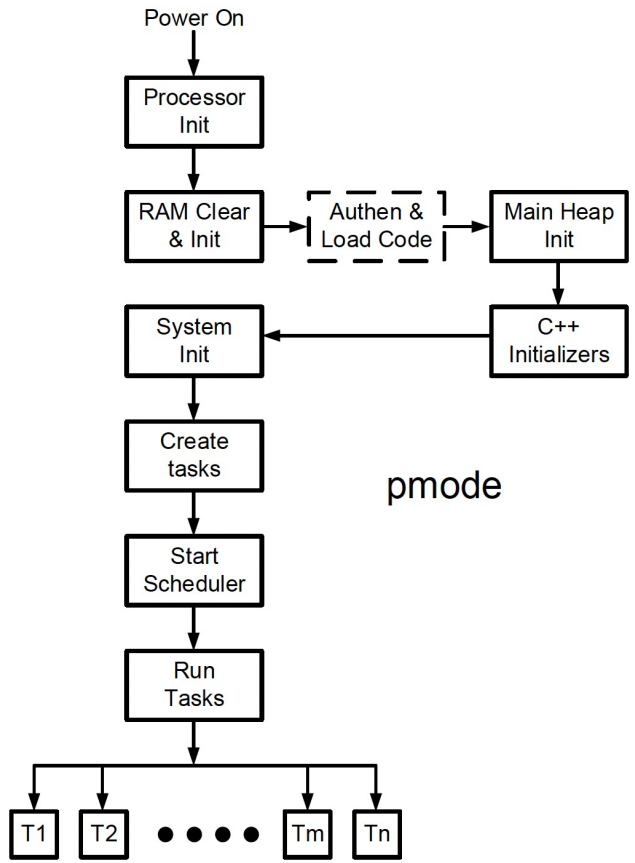


https://www.smxrtos.com/doc/ssmxug_peek.pdf

SecureSMX® - Startup

The secure RTOS does NOT manage secure boot. It performs the following:

- Kernel initialization
- Heap initialization
- Task start-up
- Scheduler bring up



How important is it for you to use a secure RTOS in your application?
- There is no need
- It would be nice
- Must have one
- A necessity

4 Going Further

Security and RTOS Resources

- Jacob's RTOS Blogs
- Jacob's RTOS courses
- Jacob's Security Blogs
- TrustZone for Cortex-M

- Embedded Bytes Newsletter
  - http://bit.ly/1BAHYXm

BENINGO EMBEDDED GROUP

www.beningo.com

CEC Continuing Education Center

DesignNews

Thank You

Sponsored by

Digi-Key ELECTRONICS

BENINGO EMBEDDED GROUP

informa markets