

# Secure Real-Time Operating System (SRTOS) Research and Development Directions

Beyond SCADA: Networked Embedded Control for  
Cyber Physical Systems

Brian Isle  
Todd Carpenter  
Charles Payne  
Kyle Nelson

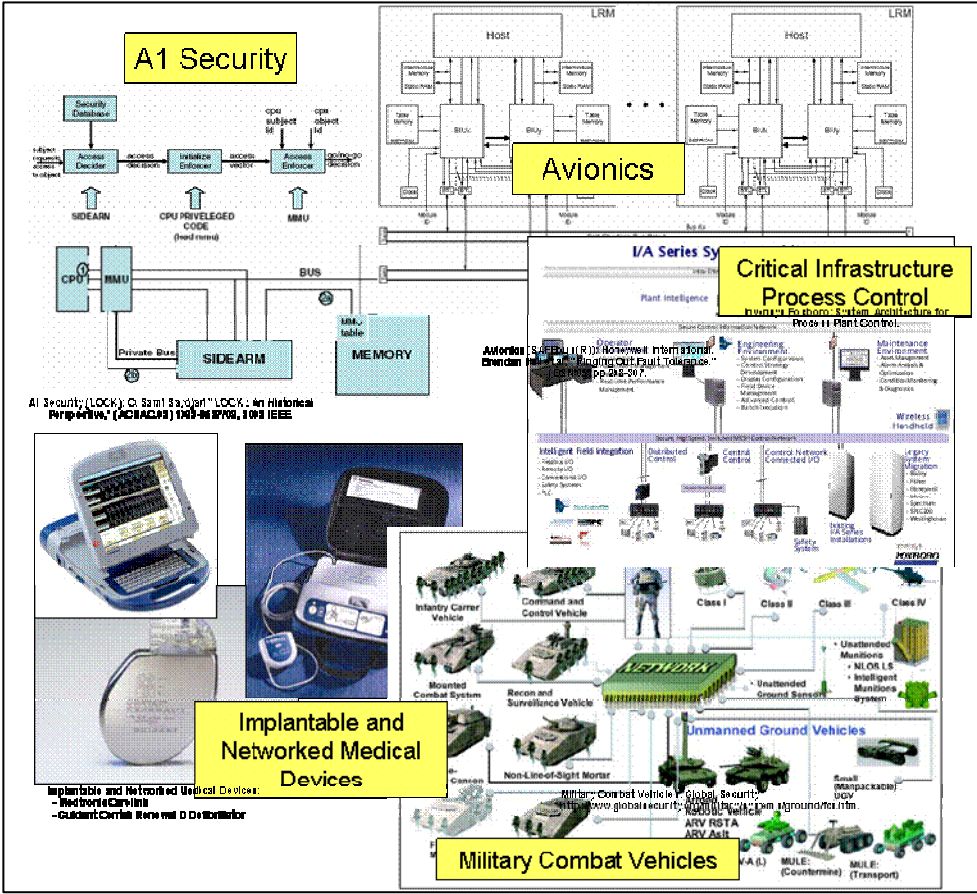
[www.adventiumlabs.org](http://www.adventiumlabs.org)

# Motivation for SRTOS Grand Challenge

Today's systems are far more networked than those considered when the core science was developed

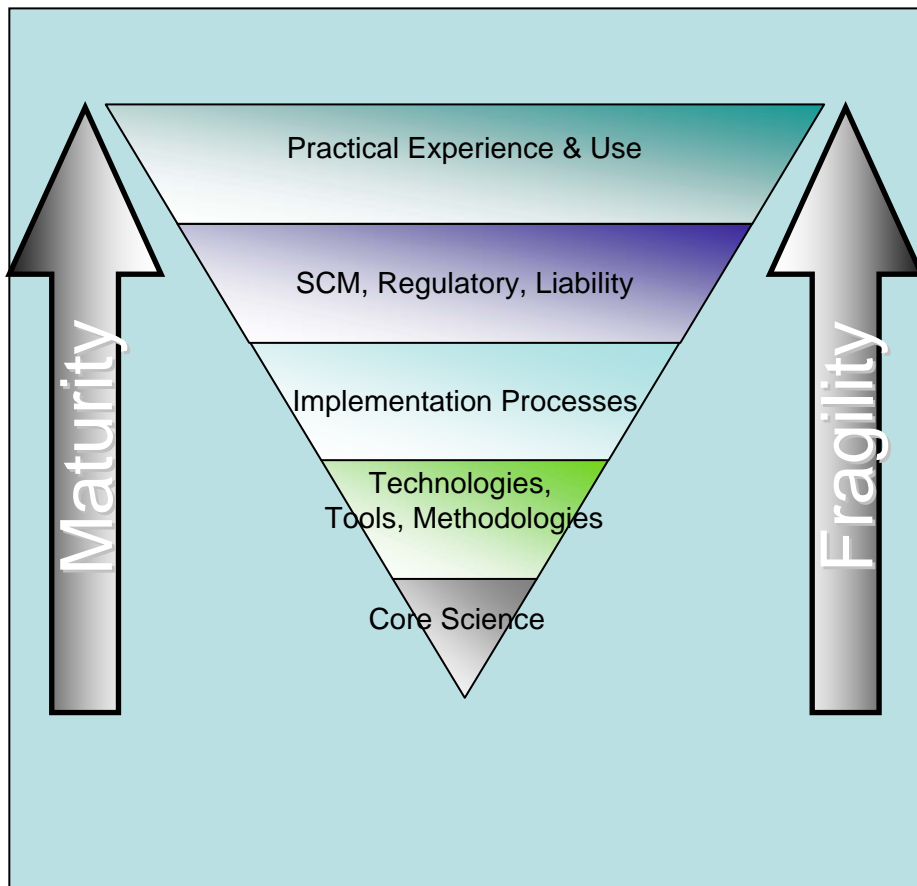
Major embedded system issues persist & challenge the traditional way of thinking about computer systems:

- Trade-off security with safety and foundational requirements, (e.g. real-time)
- Distributed functionality enabled by ubiquitous computing
- Impact of wireless access, & mobile ad-hoc networks



**Goal:** Enable future distributed, real-time, embedded systems that have security and assurance

# Invest in Fundamental Security Science

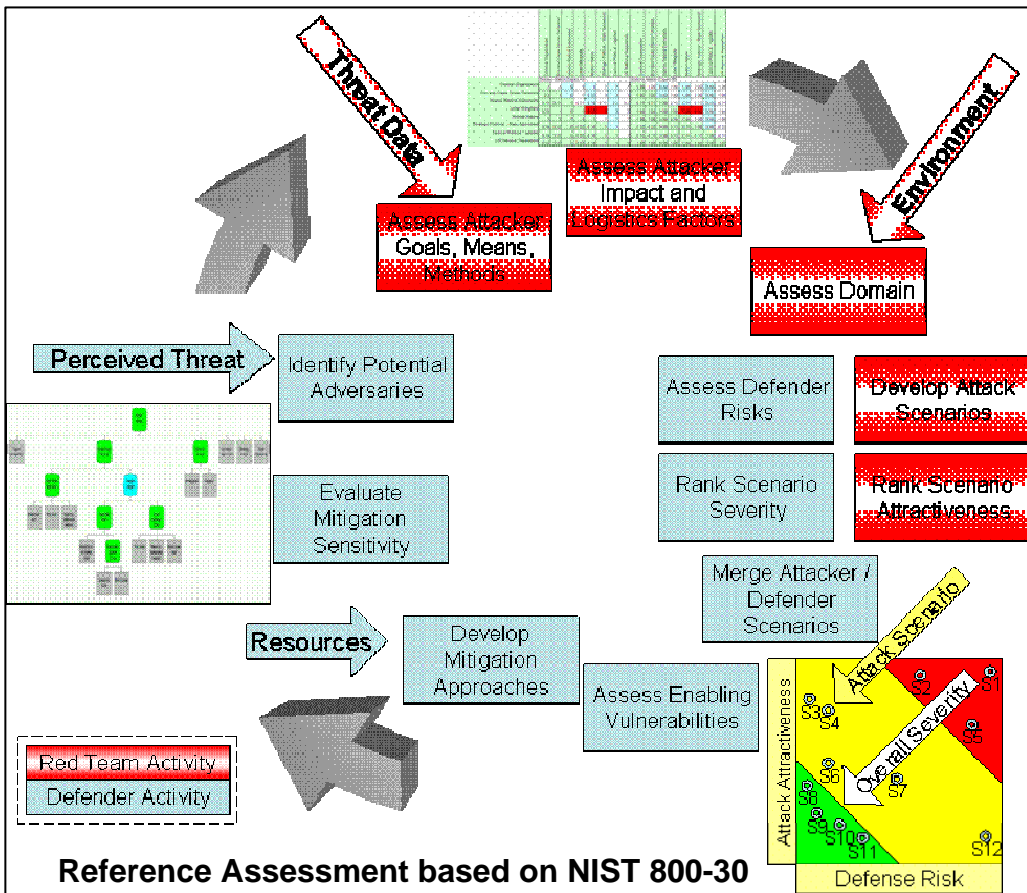


Industry needs investments in core science

- Clear and precise language for security requirements
- Address the physical, hardware, software, social domains (an SRTOS does not exist in a vacuum)
- Tools and methods for secure, real-time, fault-tolerant, mixed criticality and multi-level security development and analysis

A combination of needs, significant resources, and great talent have not been enough: we still are using old technology to thwart ancient threats.

# Define Threat & Failure Models

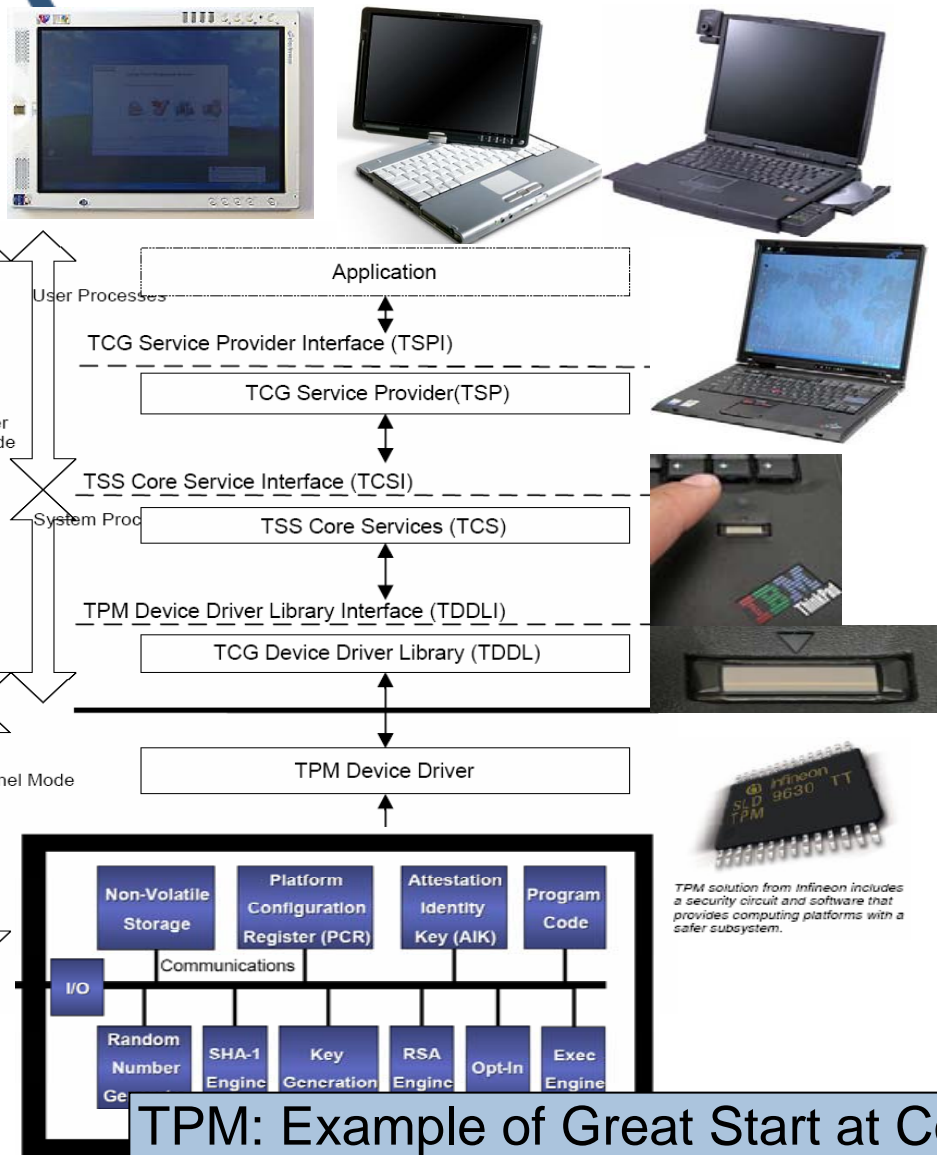


Need tools & methods to identify and quantify risks

- Threat and failure models
- Domain specific attack and defense taxonomies
- Incorporate attacker perspectives
- Provide explicit mapping to defender resources
- Analysis tools
- Testbeds
- Safe information repositories

Industry lacks the incentive, awareness, and ability to do meaningful security tradeoffs

# Integration of Solutions & Approaches



Focused effort to develop integrated models, abstractions, approaches, and capabilities to integrate the current solutions & approaches

– Application or Domain Attributes

- Assured, available, distributed, embedded, evolvable, fault-tolerant, interoperable, power aware, mixed criticality, multi-level security, real-time, reliable, robust, safe, ubiquitous, secure, .....

– Business Attributes

- Certified, cost-effective, maintainable, evolvable, open, practical, multi-source, valuable, ....

– Constructive attributes

- Certifiable, composable, flexible, open, testable, .....

– Applicable solution technologies or techniques or attributes

- Fault isolation, freedom from crashing, time, space, I/O partitioned, .....

# Motivating Industry



Honeywell

SIEMENS



Johnson & Johnson



We need an understanding of what motivates companies to adopt new solutions

- What are the incentives?
- What are the forcing functions? (e.g. regulations, liabilities)
- What are the barriers? (e.g. politics, lobbying, & special interest groups)

Stakeholders

- Academia
- Tool providers
- Vendors
- Prime contractors
- Industry and operators
- Regulatory agencies
- Consumers & Government

**Understanding the path to industry adoption is critical to success**

# Secure, Open, Real-Time Operating Systems

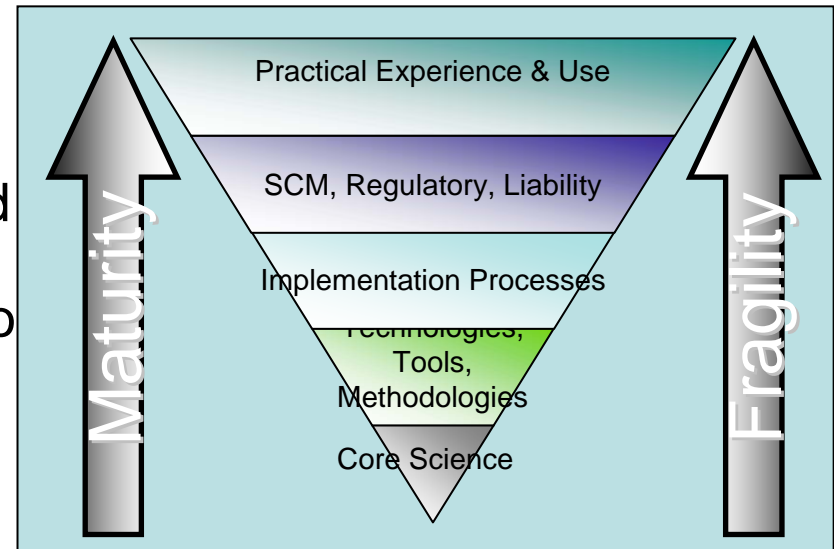
**Goal:** Enable future distributed, real-time, embedded systems that have security and assurance

**Objective:** Identify the research needed to advance the state of the art for building a new generation of systems technologies

**Issue:** Despite decades of research, the ability to build secure real-time systems remains beyond the state of the art

## Approach:

- Research basic science foundations necessary for security, safety, real-time, fault-tolerance, etc.
- Develop open systems built ‘from the ground up’ with the key attributes
- Provide enabling tools and techniques for construction, analysis, and certification of such systems



## Specific Research Needs:

- Fundamental science of security
  - Language for security requirements
  - Physical, hardware, software, social domains
  - Tools and methods for secure, real-time, fault-tolerant, mixed criticality and multi-level security development and analysis
- Threat and failure models
  - Comprehensive and evolvable domain-specific models and taxonomies
  - Real costs from security compromises
- Integration of existing plethora of partial solutions and approaches
- Motivating industry: approaches to motivate acceptance and responsibility