

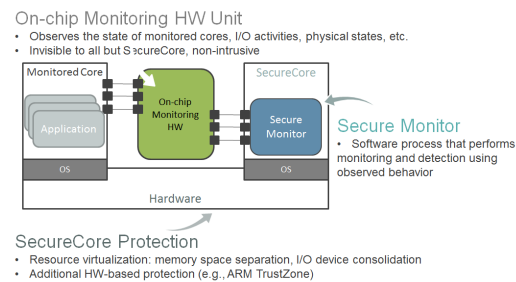
# BEHAVIOR-BASED ZERO-DAY INTRUSION DETECTION FOR REAL-TIME CYBER-PHYSICAL SYSTEMS

## Challenge:

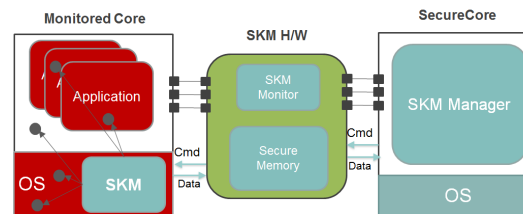
- Detect intrusions in real-time control systems (and further, in more general purpose systems)
- Ensure system remains **safe** in event of attack

## Solution:

- Use deterministic behavior of real-time embedded systems to detect deviations (anomalies).
- Developed an architectural framework that can be used to detect anomalies and also take away control (to maintain safety) when an intrusion is detected.
- Developed innovative methods to capture the behavior of systems and for checking at runtime.



## SecureCore Architecture



## DragonBeam Architecture

## Scientific Impact:

- Innovative methods to capture the behavior of systems for IDS
- Architectural frameworks (SecureCore, DragonBeam) that enable better IDS based on observation of runtime behavior
- Results/methods developed here can be used to understand how to detect anomalies in both, real-time embedded systems as well as general purpose systems.

## Broader Impact:

- Real-time control systems are everywhere (automobiles, avionics, power systems, industrial control systems, etc.) and are now being attacked – so these methods can make such systems more secure and safe.
- This work has been included in a graduate course on Cyber-Physical Systems at UIUC.