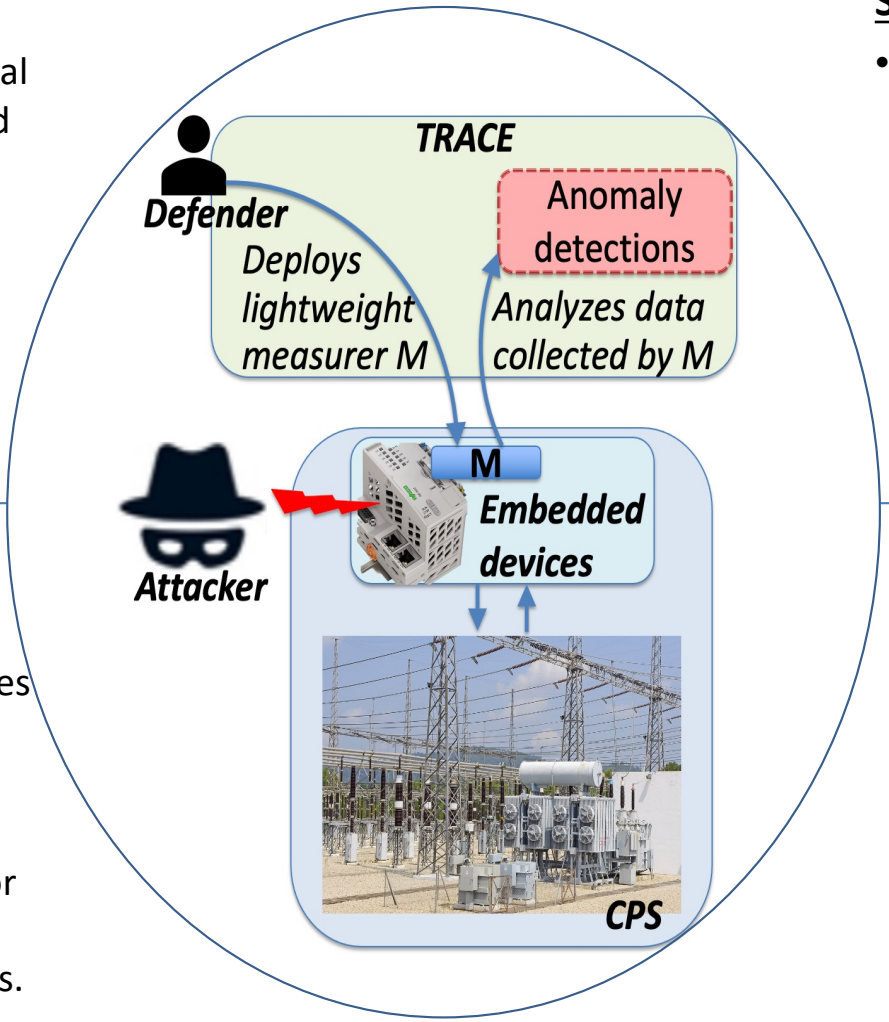
NSF SATC: TTP: Small:
Tracking Run-time Anomalies in Code Execution (TRACE)

Challenge:

- Robust cybersecurity is crucial in interconnected embedded devices in cyber-physical systems (CPS); in particular, power grid devices.
- In-field integrity verification and anomaly detection for fielded devices is a crucial capability.

Solution:

- TRACE: automated, lightweight, multi-modal measurers onto target devices + off-device analysis + ML-based threat detection.
- In-field anomaly detection leveraging temporal behavior and code structure characteristics of CPS devices.



Scientific Impact:

- TRACE mitigates security threats in embedded CPS devices by enabling on-demand/continuous integrity verification of embedded CPS devices, focusing on power grid devices (e.g., substation automation controllers).

Broader Impact and Broader Participation:

- Near-zero-cost solution to detect and characterize malware in CPS devices.
- TRACE TTP builds on NYU's work in DARPA RADICS and will expand operating envelope, increase automation, reduce deployment friction, and license/commercialize TRACE.

NSF SaTC TTP Award 2039615, NYU Tandon School of Engineering

F. Khorrami (Lead PI); R. Karri (Co-PI); P. Krishnamurthy (Senior Person)