Securing Distributed Building Automation Systems Through a Policy-Enforced Application Communication Framework

KANSAS STATE UNIVERSITY
Masaaki Mizuno
Mitchell Neilsen
John Hatcliff
Siddharth Amaravadi

USF UNIVERSITY OF SOUTH FLORIDA
Simon Ou (Project lead)
Xiaolong Wang
Richard Habeeb

Honeywell
Raj Rajagopalan
Srivatsan Varadarajan

Infrastructures have been attacked

In 2010, the cyber weapon *Stuxnet* damaged Iran's uranium enrichment plant.

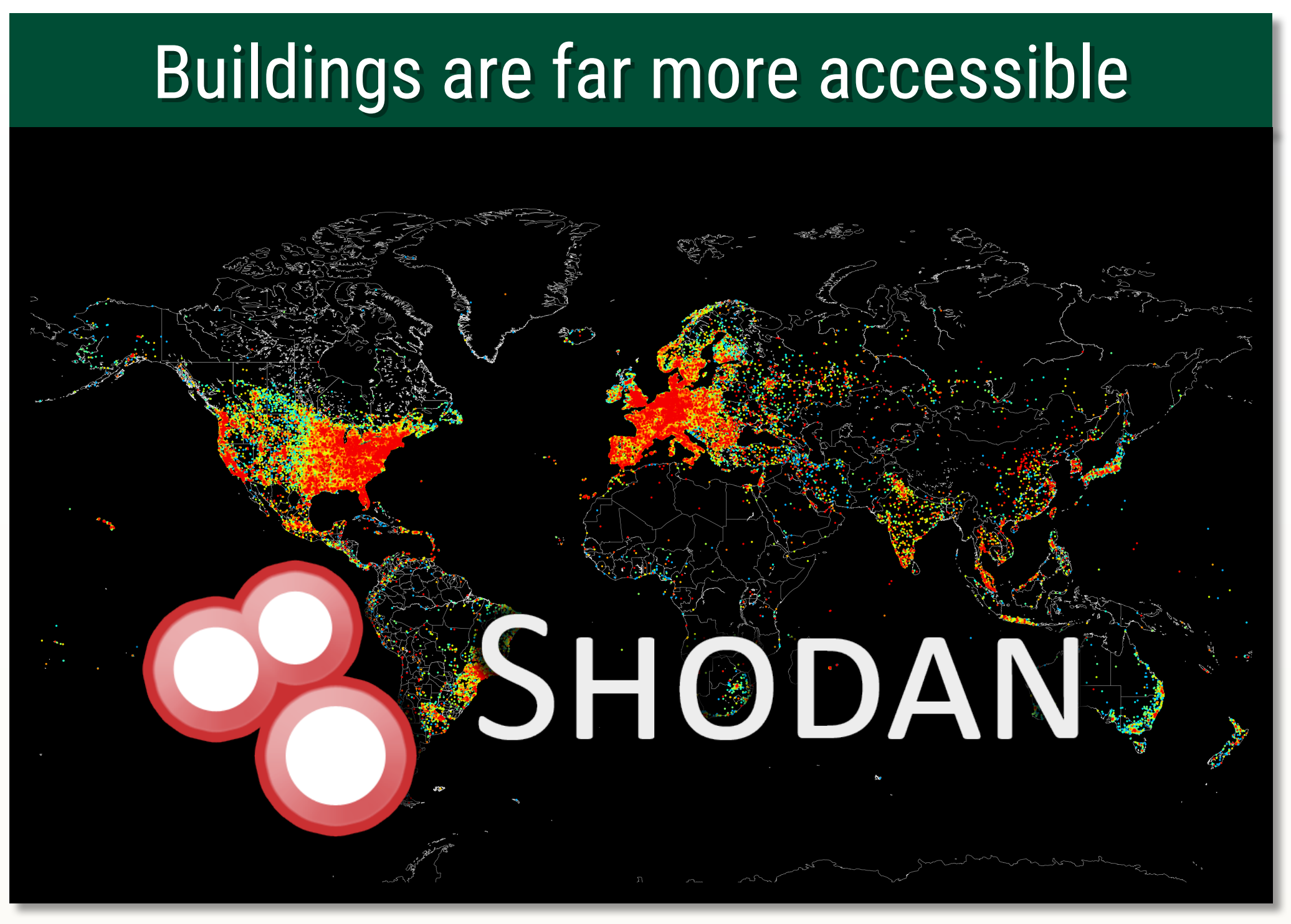
Weak security in existing systems

ASHRAE BACnet™ LonWorks

Modbus KNX

Legacy industrial control protocols and devices often lack security consideration.

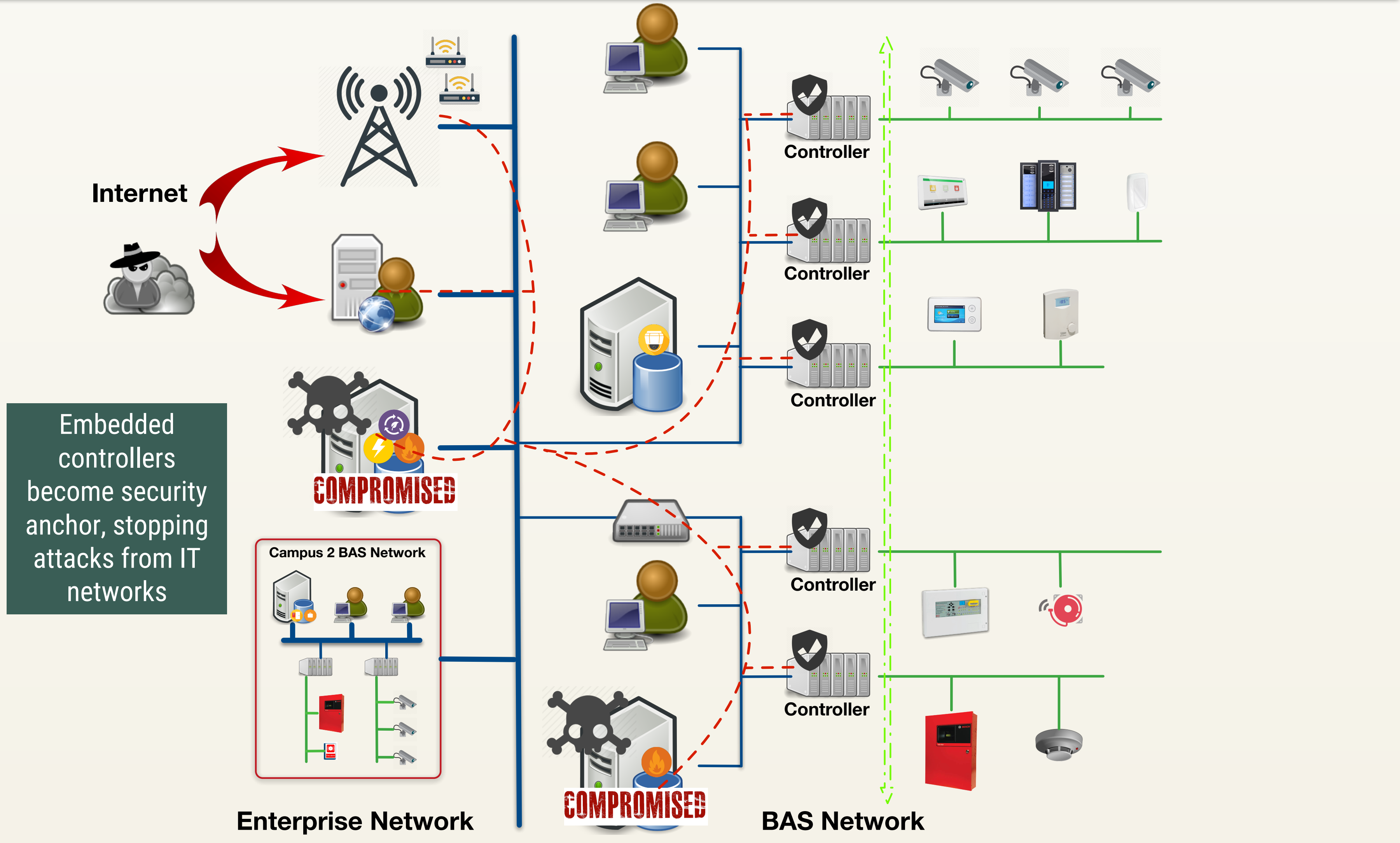
Buildings are far more accessible



Thousands of building automation networks are directly reachable from Internet.

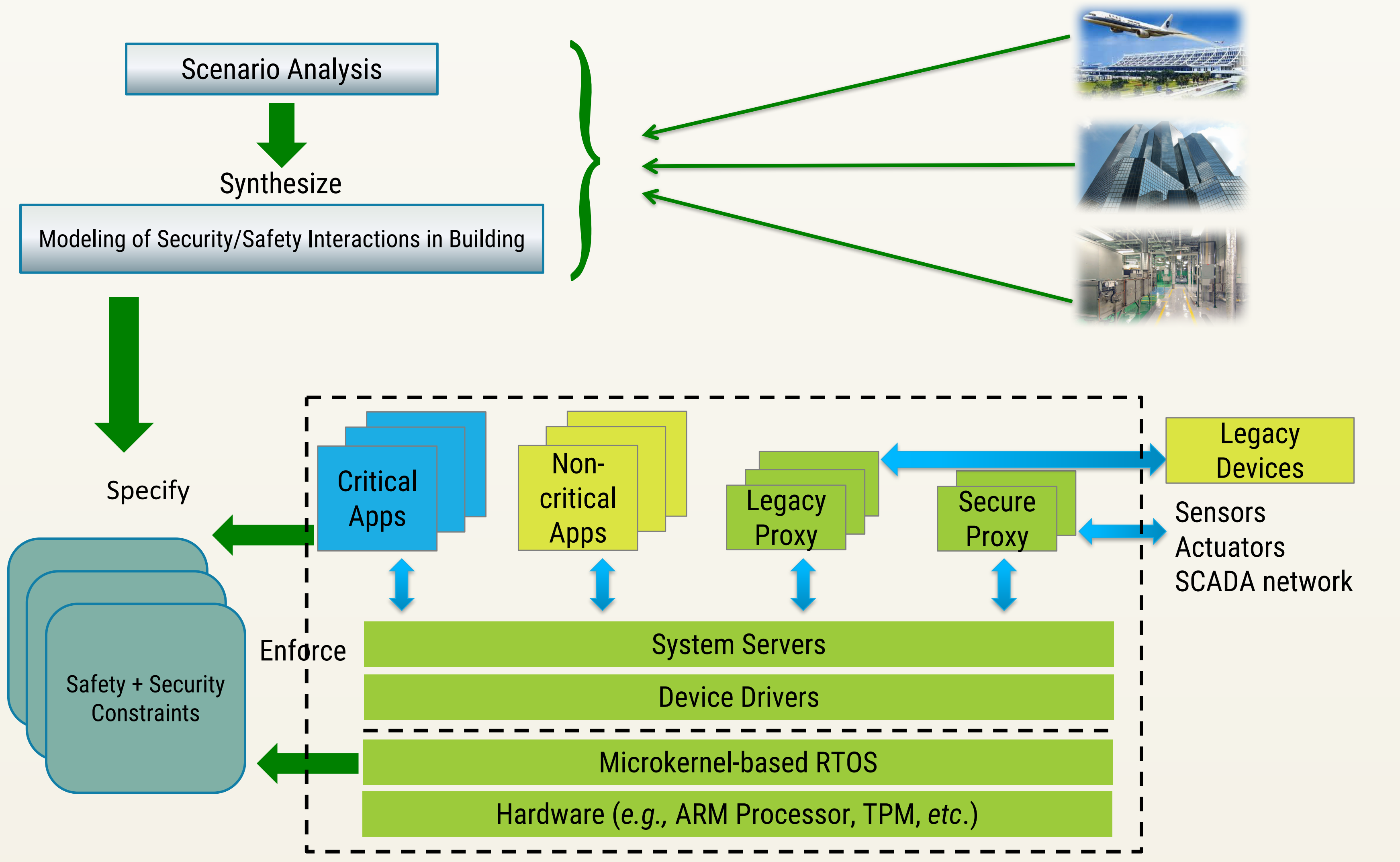
What are we doing about the cybersecurity of building automation systems?

Protect building environment using secure microcontrollers

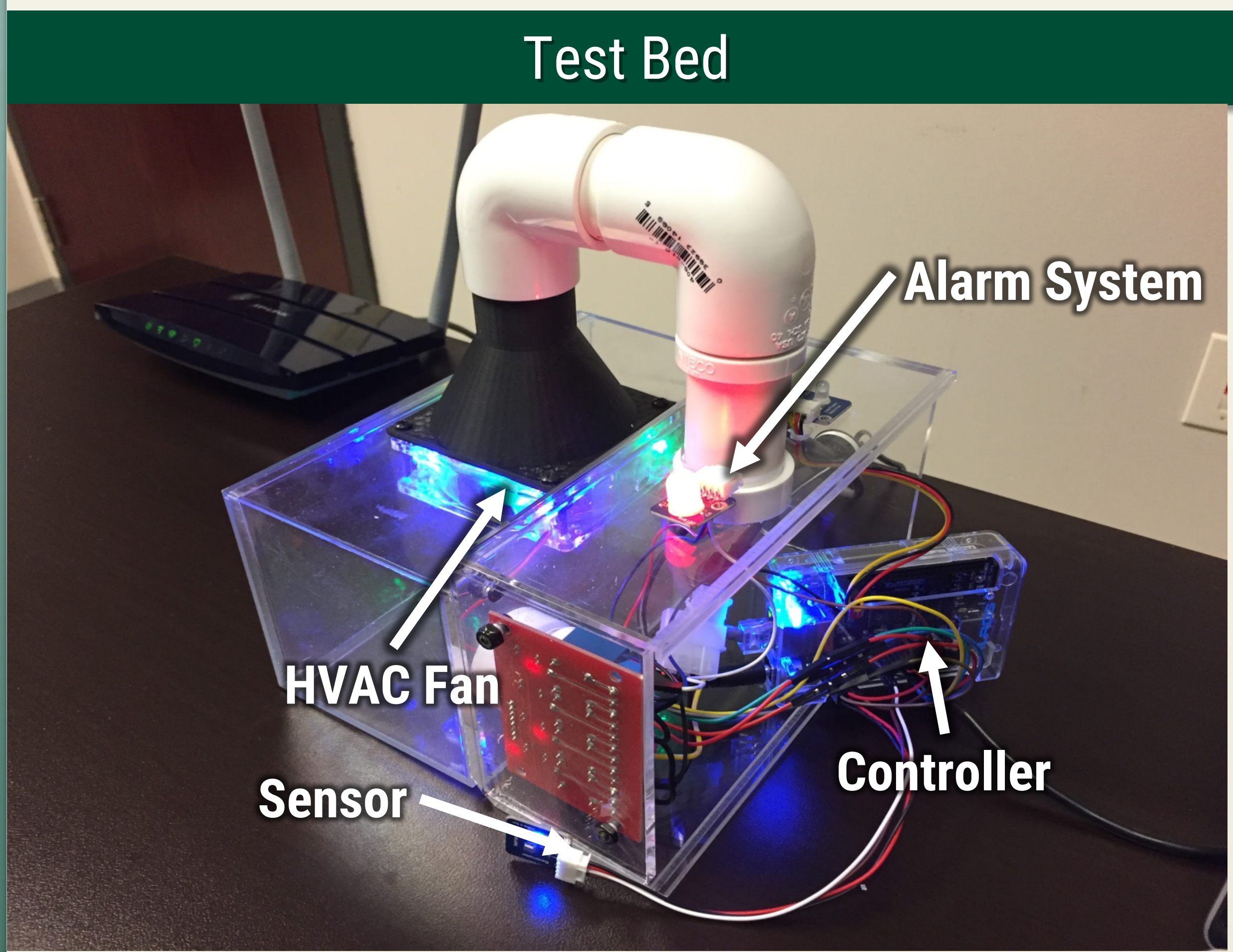


Embedded controllers become security anchor, stopping attacks from IT networks

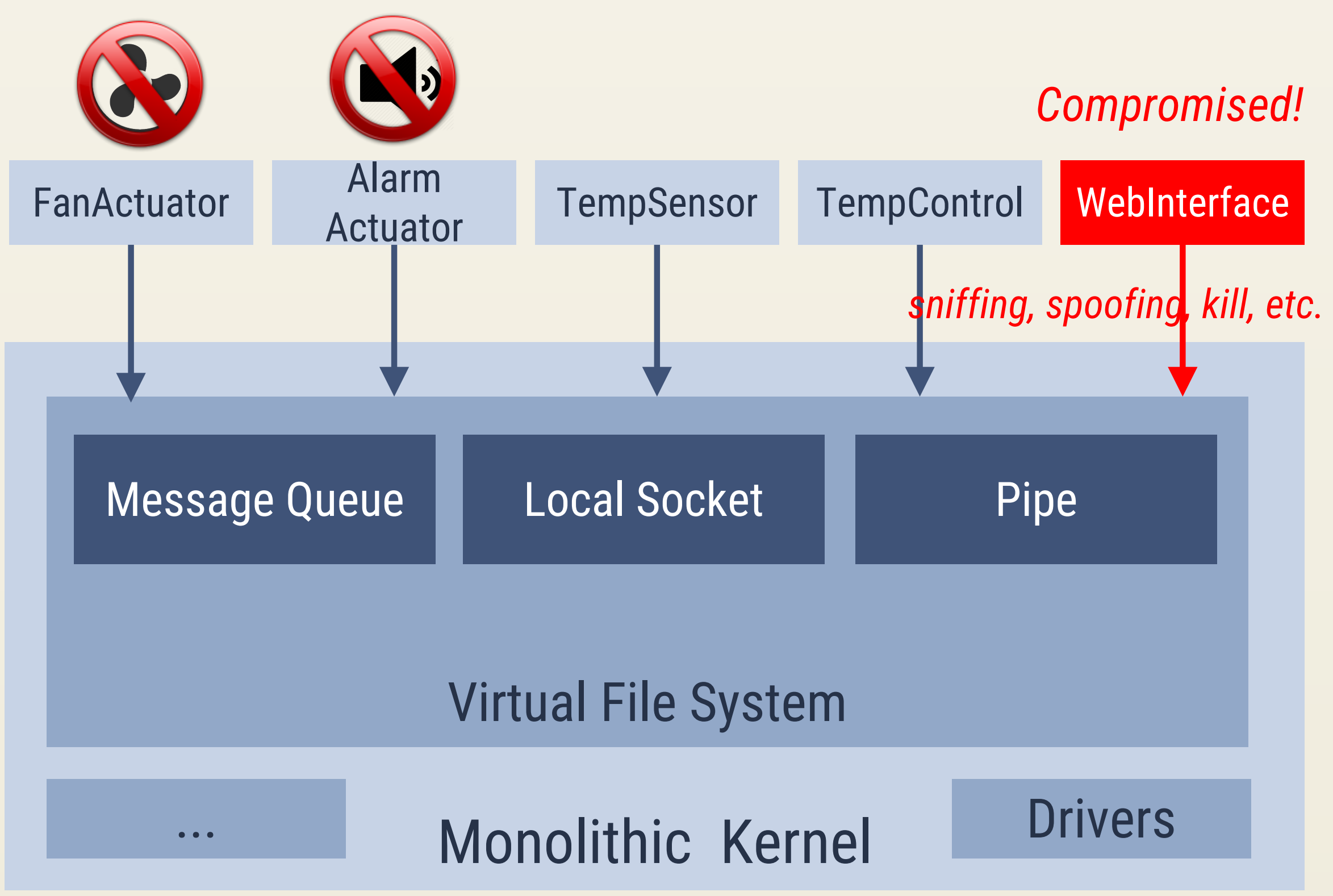
A new framework leveraging microkernel-based RTOS



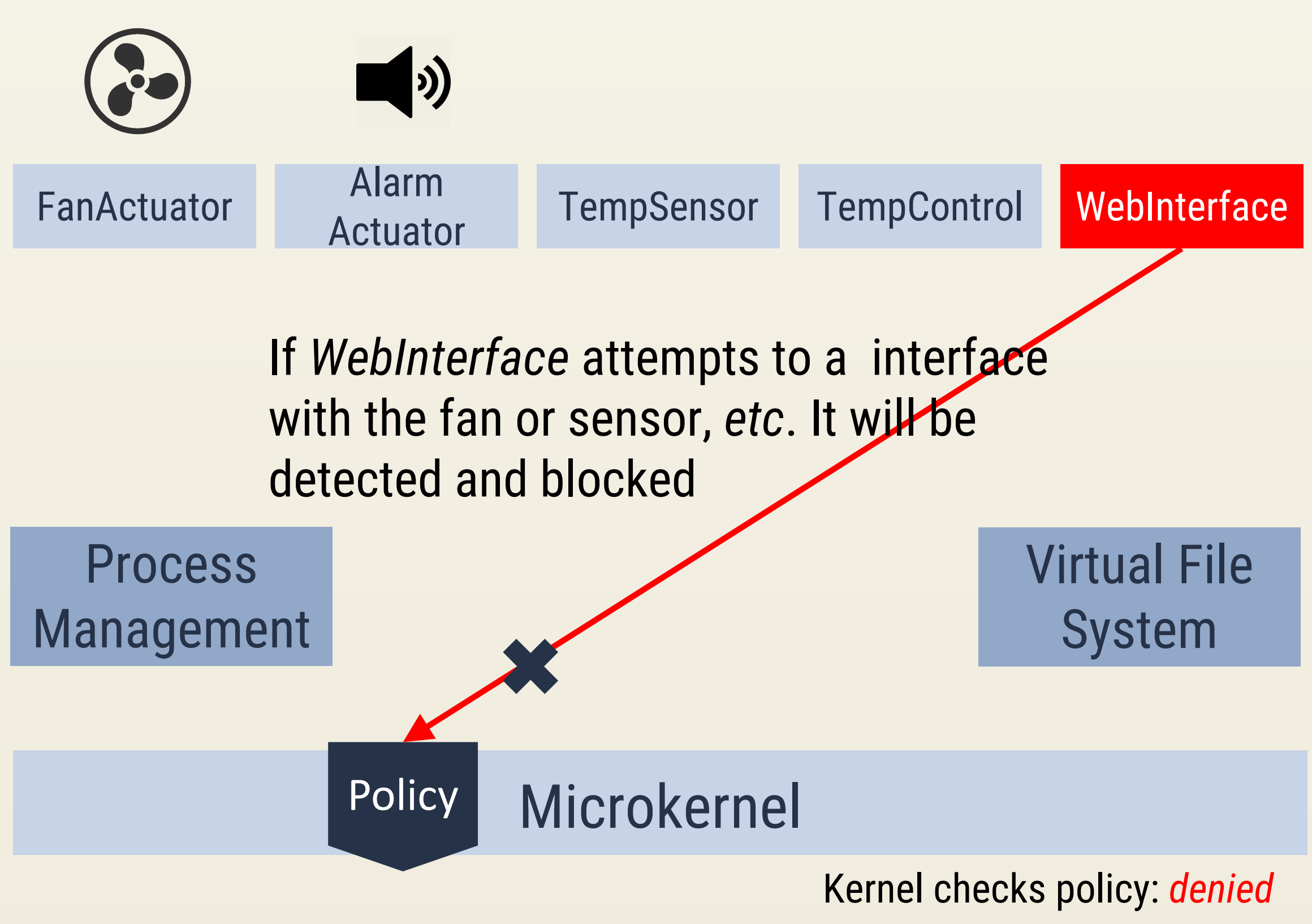
Test Bed



Traditional Monolithic Kernel Architecture



Secure Enhanced Microkernel Architecture



If *WebInterface* attempts to a interface with the fan or sensor, *etc.* It will be detected and blocked

Kernel checks policy: *denied*

Benefits

- Build security in – fundamentally change the "breach and patch" cycle
- Manage security and safety in the same framework
- Support diverse constraints for different types of buildings; extensible to other CPS domains
- Developed models drive the design of a secure controller framework for Internet of Things (IoT)
- Minimize barrier to adoption by supporting existing legacy devices

Acknowledgements

This research is supported by the Department of Homeland Security under contract number D15PC00303. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Department of Homeland Security.