PRESENTED BY UNIVERSITY OF HOUSTON

TAMEST NATURAL HAZARDS SUMMIT

Responding to and Mitigating the Impacts

PART I: VIRTUAL SUMMIT
10.19.2021

#NATURALHAZARDSSUMMIT

Theme Four:

ENGINEERING AND DESIGNING FOR RESILIENCE

Moderated by:
HANADI RIFAI, PH.D., P.E.
John and Rebecca Moores Professor of Civil and Environmental Engineering
University of Houston

Panel:

Engineering and Designing for Resilience

AMY BABAY, PH.D.

Assistant Professor
University of Pittsburgh

JULIE SHIYOU-WOODARD

President and CEO
Smart Home America

The need for cyber-resilience in critical infrastructure

- Successful attacks are becoming more frequent
  - Stuxnet (2010), Dragonfly/Energetic Bear, Black energy (Ukraine 2015), Crashoverride (Ukraine 2016), Florida water system hack (February 2021), Colonial Pipeline (May 2021)
- Perimeter defenses are not sufficient against determined attackers

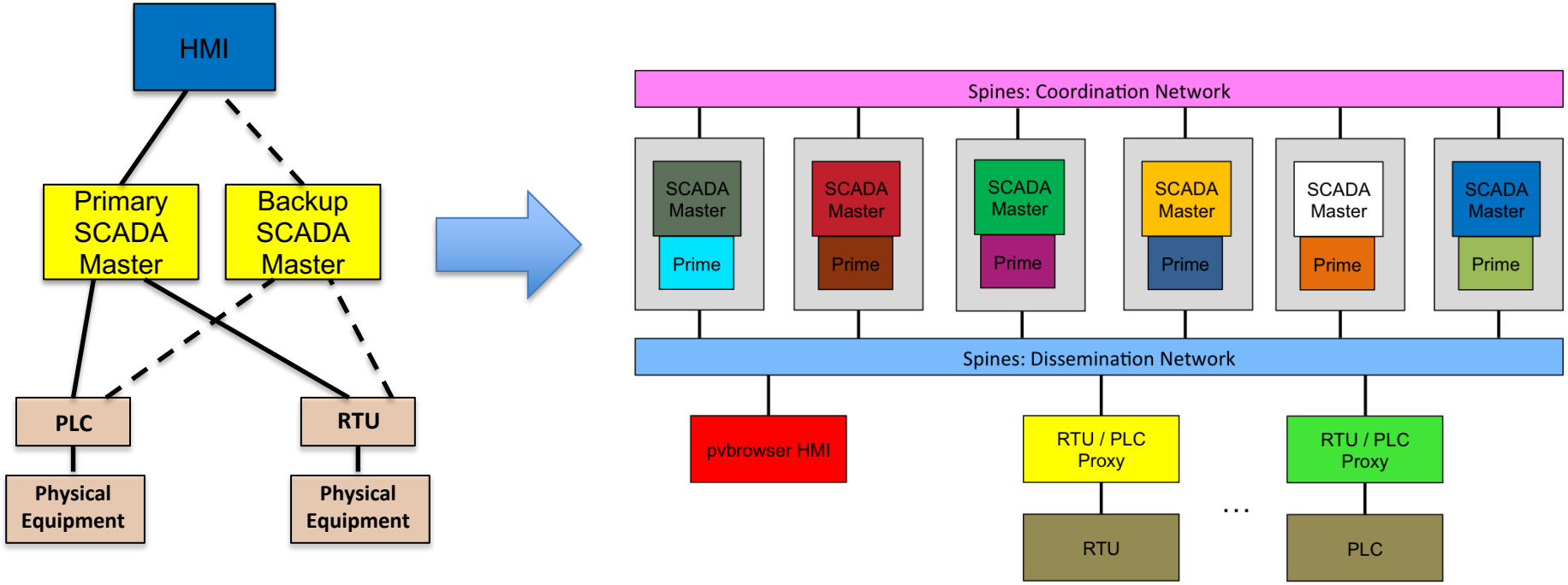
The need for cyber-resilience in critical infrastructure

- Supervisory Control and Data Acquisition (SCADA) systems form the backbone of critical infrastructure services
- Must be constantly available and running at expected level of performance (able to react within 100-200ms)
- Failures and downtime can cause catastrophic consequences, such as equipment damage, blackouts, and human casualties **and they are a target for attackers today**

Intrusion Tolerance: an approach for resilience

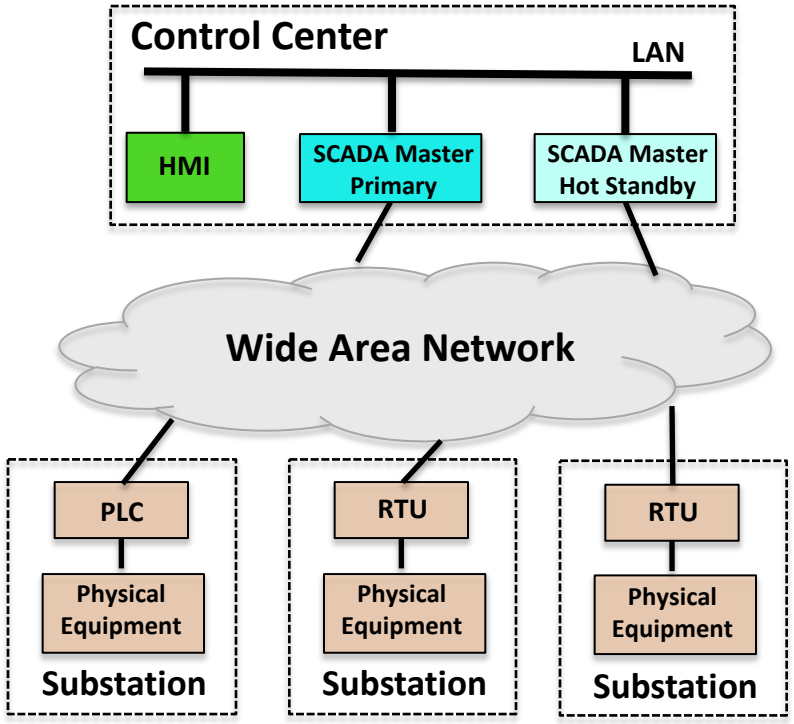
- **Intrusion tolerance** is the ability to continue to operate **correctly**, and at an **expected level of performance**, despite attacks that **succeed in compromising part of the system**

Spire: Intrusion Tolerant SCADA for the Power Grid



Continues to work correctly (and meet performance guarantees) even if some critical components have been compromised

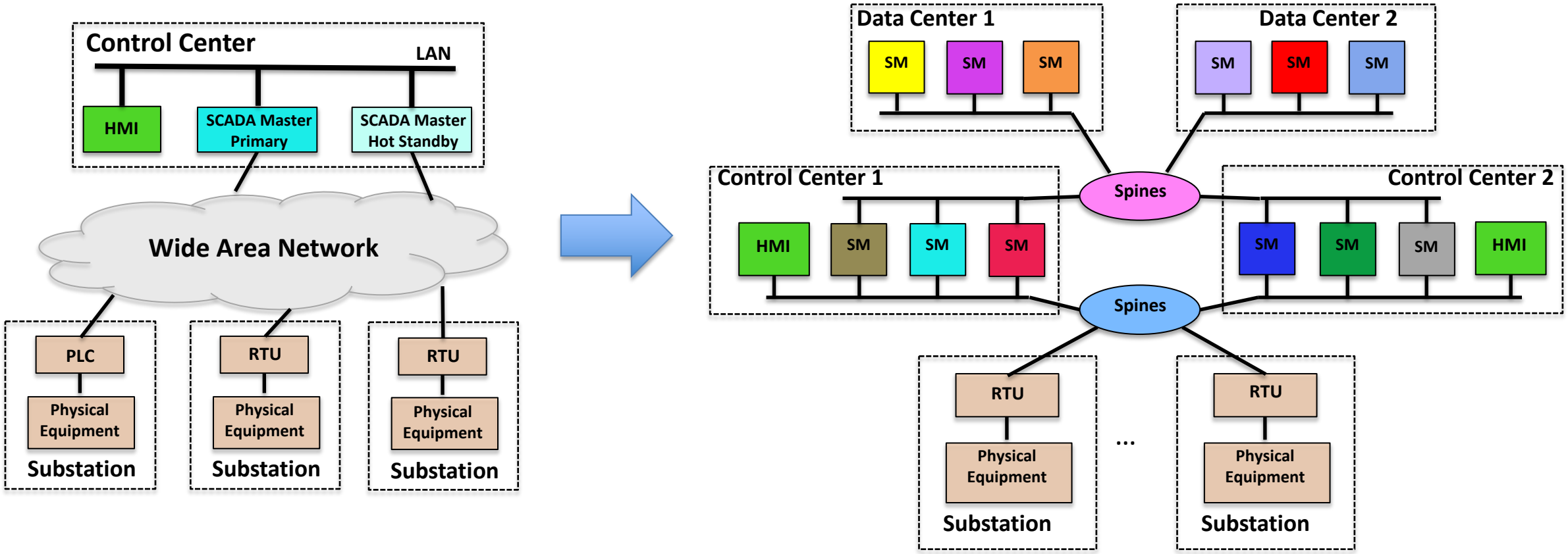
What about the network?



- SCADA systems for **wide-area transmission systems** support large power grids with PLCs in many substations spanning hundreds of miles

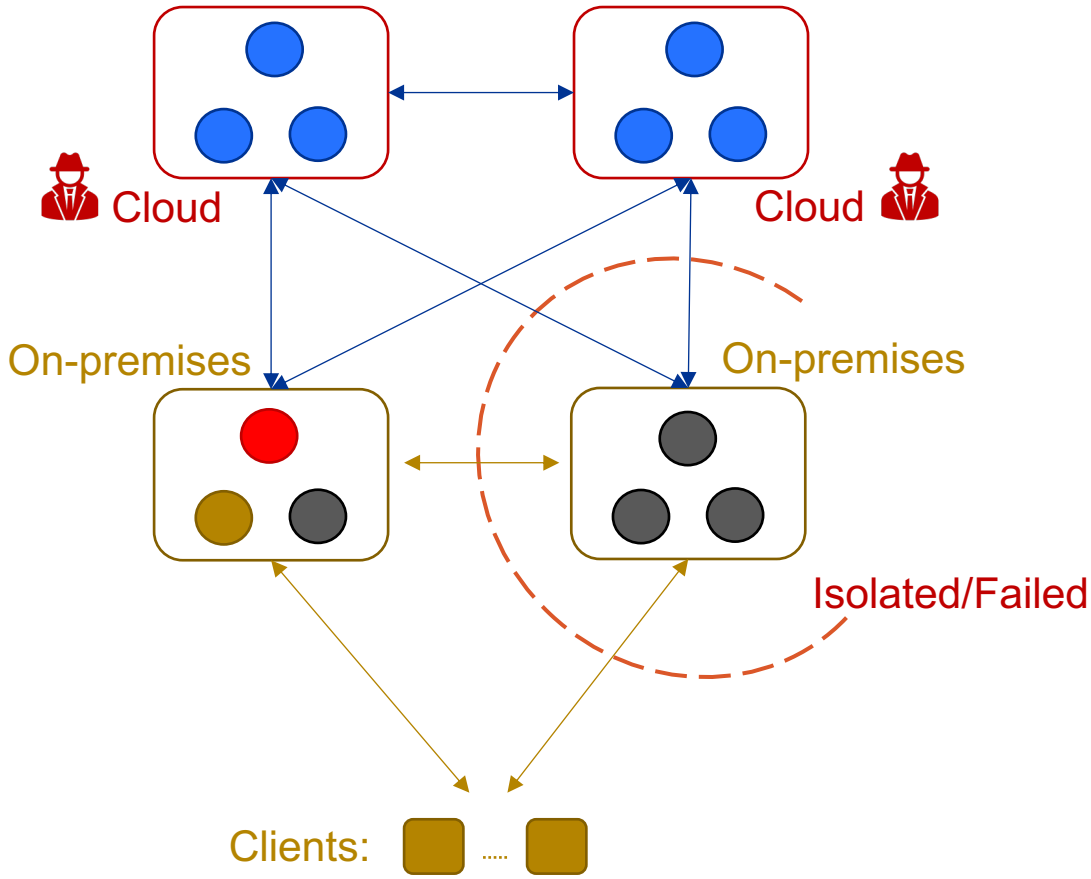
- What happens if the control center is disconnected?

What about the network?



Remaining challenges

- **How can we make this easy for power grid operators to deploy?**
- Our recent work shows how we can offload management of part of the system to cloud providers, even if we don't fully trust them with our data!



Remaining challenges

- **Is this threat model enough?**
- Unfortunately, probably not…our ongoing work is investigating **compound threats** (natural disaster + follow-on cyberattacks)