KTH ROYAL INSTITUTE
OF TECHNOLOGY

Center för resilienta kritiska infrastrukturer (CERCES)

Henrik Sandberg (hsan@kth.se)
Avdelningen för reglerteknik

MSB:s forskardagar, Stockholm, 11-12 november, 2015

Outline of Presentation

- The consortium
- Background
- Main research objectives
- Sample of research in resilient control and communication

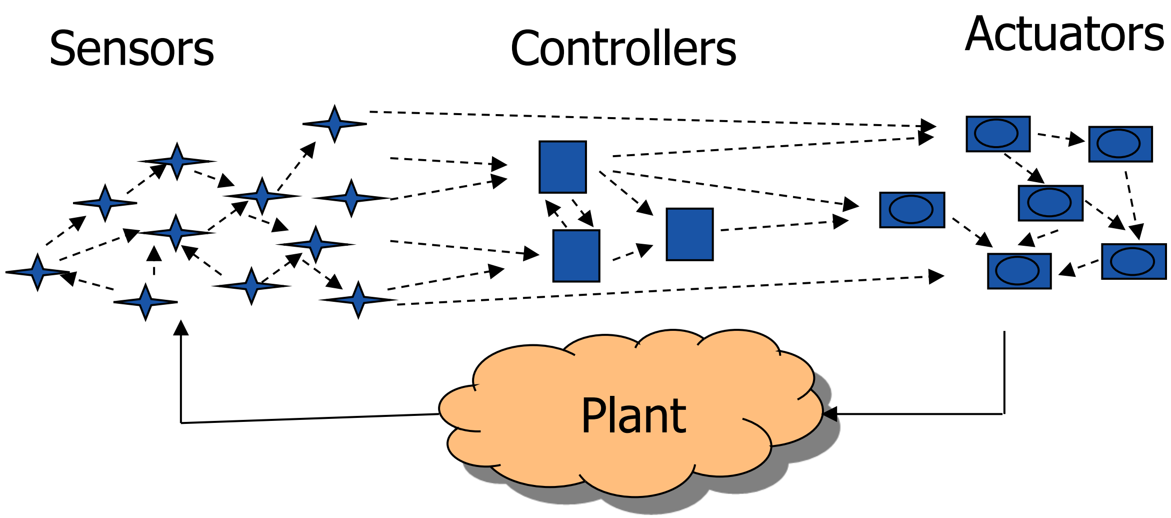
Outline of Presentation

- **The consortium**
- Background
- Main research objectives
- Sample of research in resilient control and communication

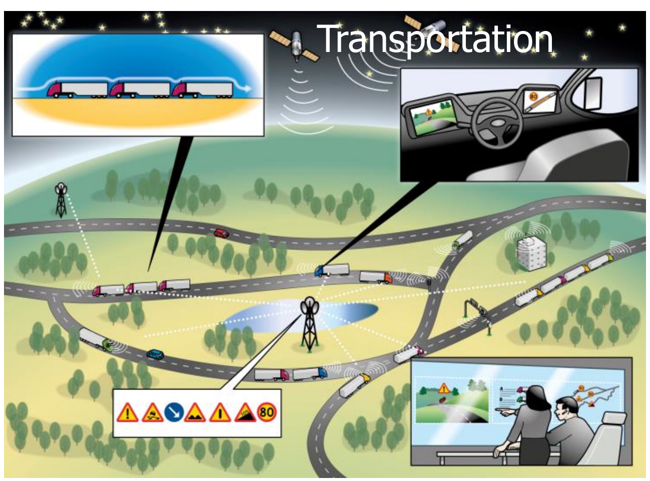
The Consortium

- Henrik Sandberg, Professor in Automatic Control (KTH)
- Mads Dam, Professor in Teleinformatics (KTH)
- György Dán, Lektor and Docent in Teletraffic Theory (KTH)
- Ragnar Thobaben, Lektor and Docent in Communication Theory (KTH)
- 4 PhD students and 1-2 post-docs
- NCS3-team at FOI in Linköping

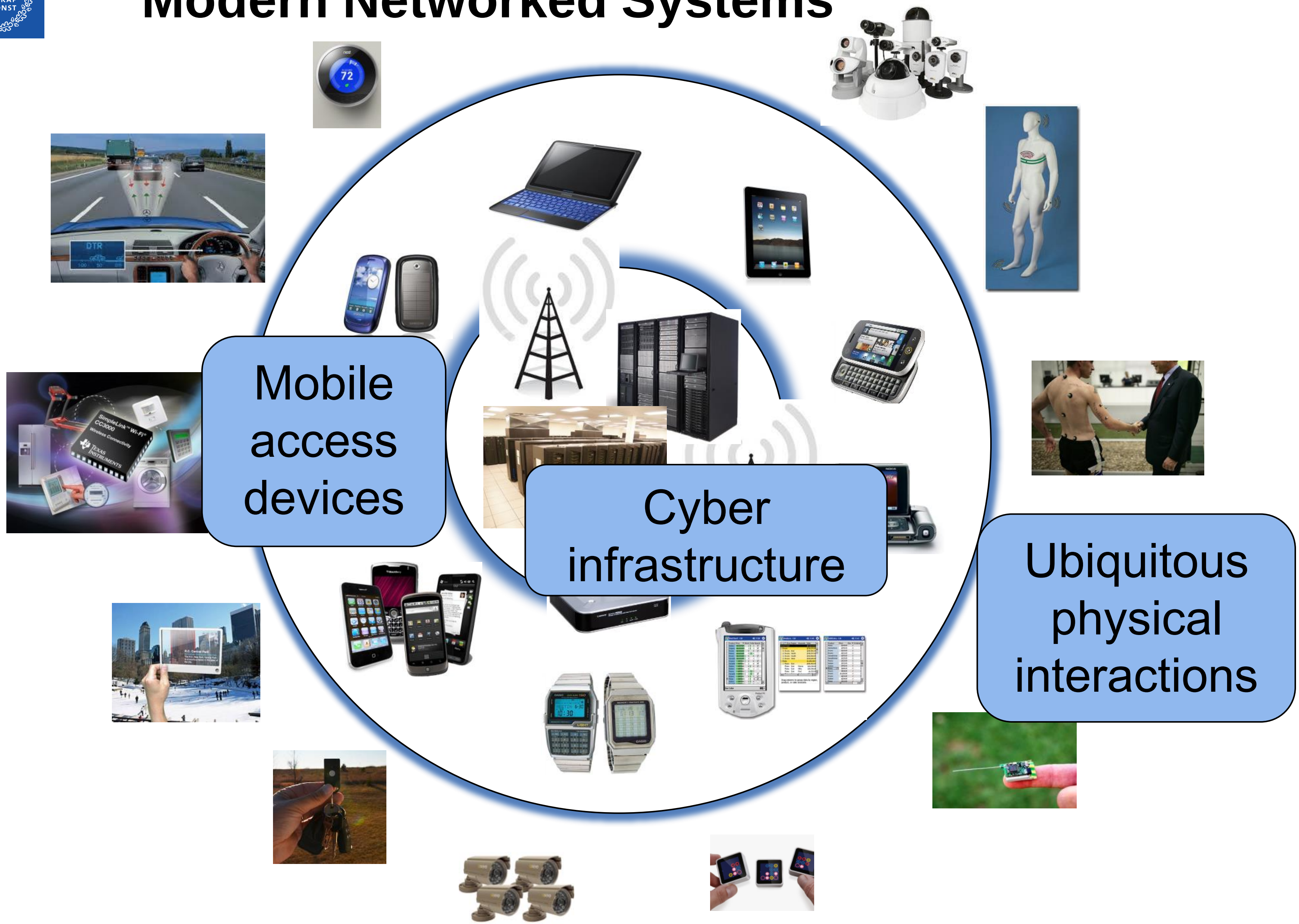
Legacy Industrial Control Systems (ICSs)



- Wired
- Purpose-built computing platforms
- Proprietary solutions
- Security by obscurity
- “Isolated infrastructure”

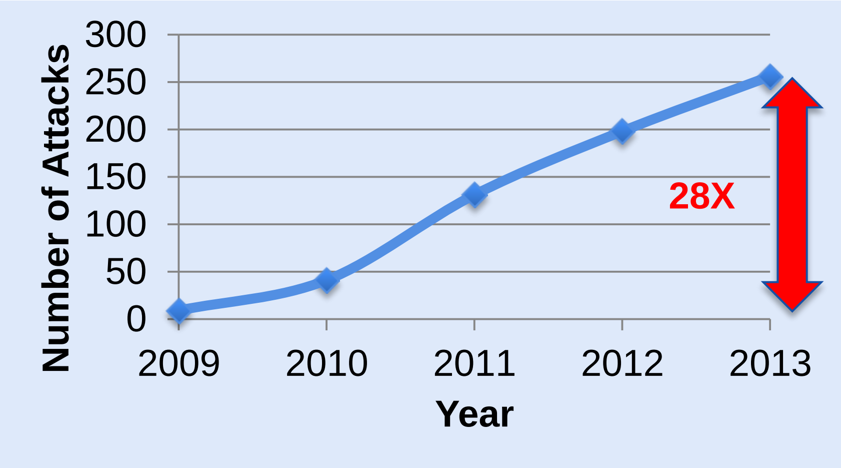


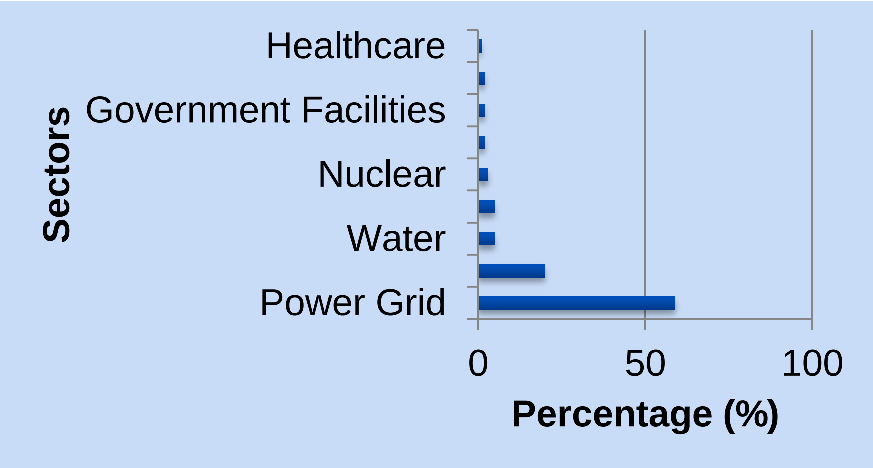
Modern Networked Systems



Some Cyber Security Statistics

Cyber incidents in critical infrastructures in the US, voluntarily reported to DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)





[ICS-CERT, 2013]
[S. Zonouz, 2014]

Outline of Presentation

- The consortium
- Background
- **Main research objectives**
- Sample of research in resilient control and communication

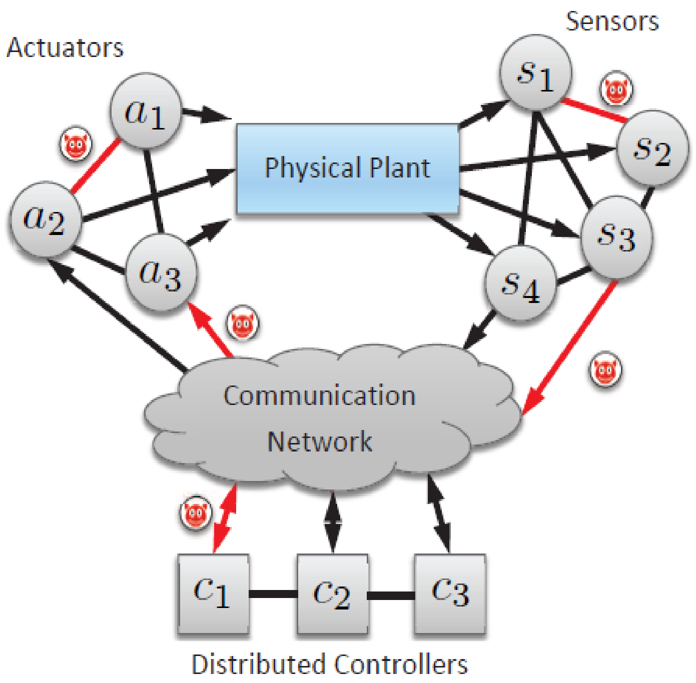
Key Challenges

Critical infrastructure ICSs in transition from

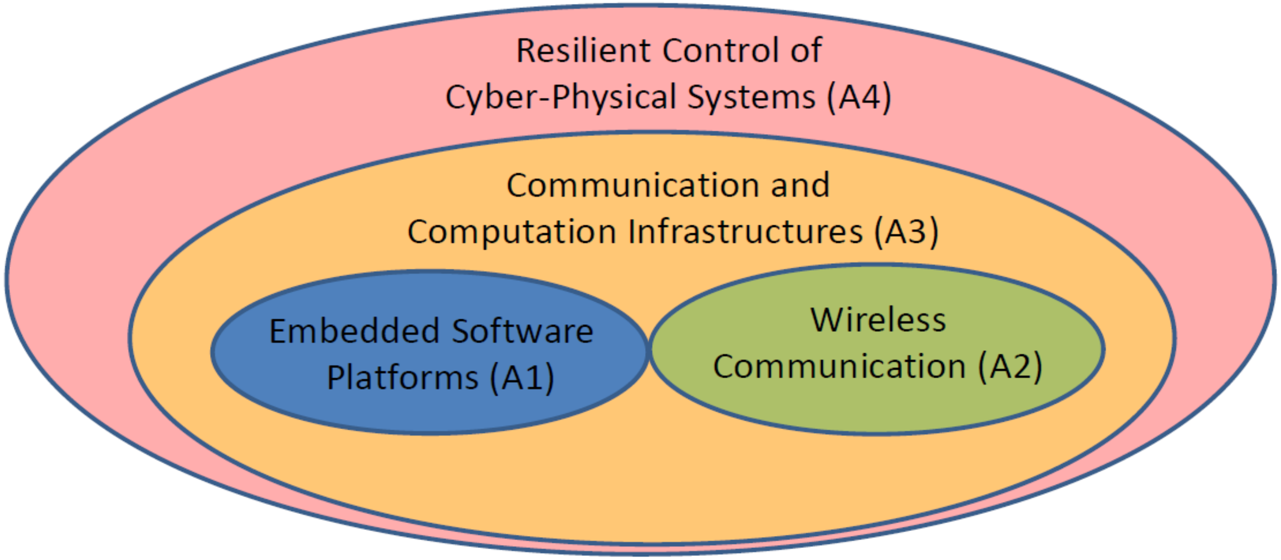
- closed proprietary solutions
- rigid, non-updatable platforms
- weak security guarantees

to

- open standard solutions (COTS)
- flexible software architectures
- runtime platform updates
- strong security guarantees using formal methods

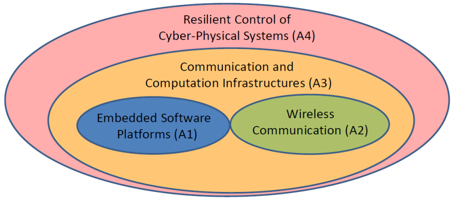


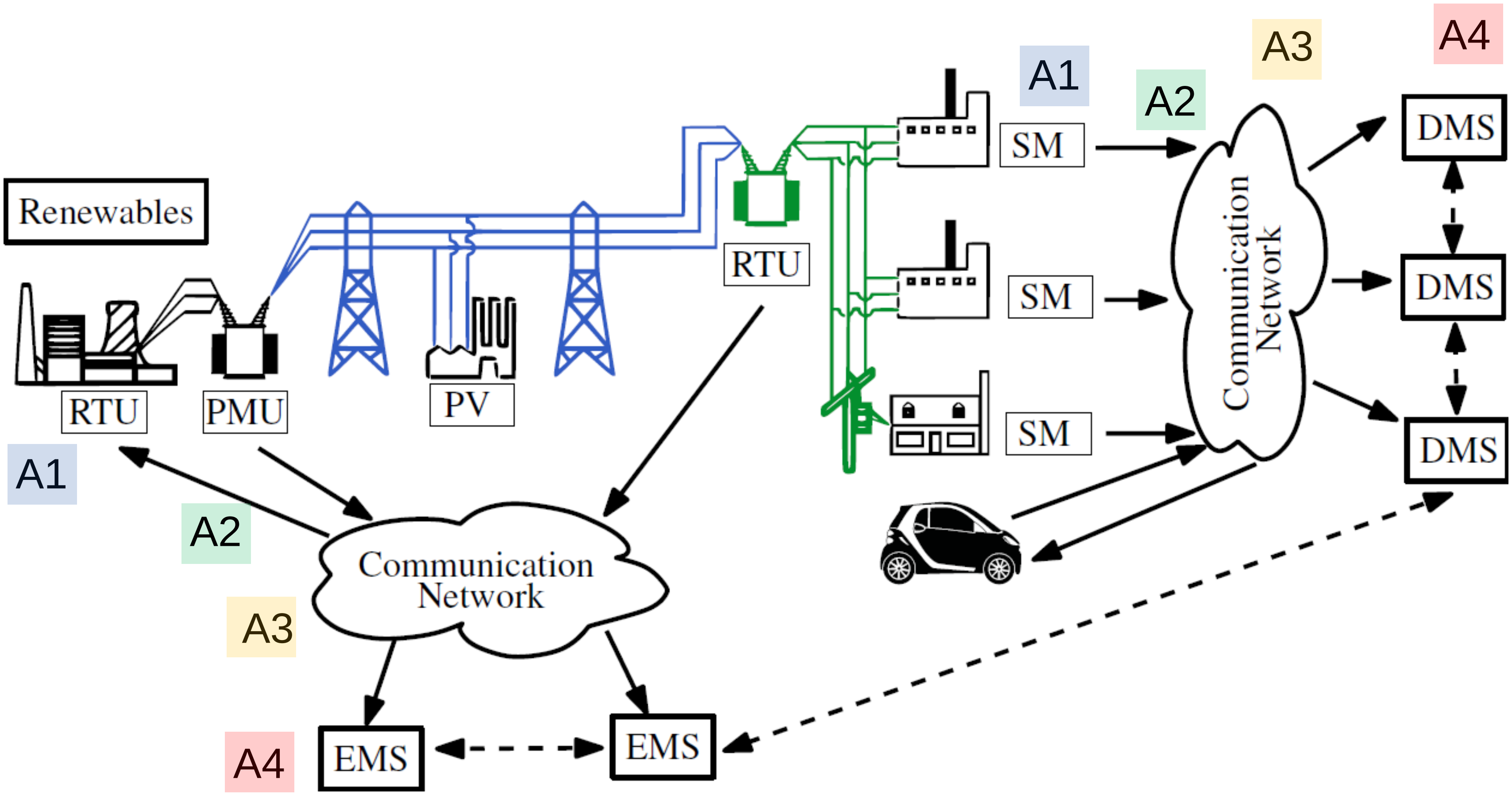
CERCES Main Research Areas



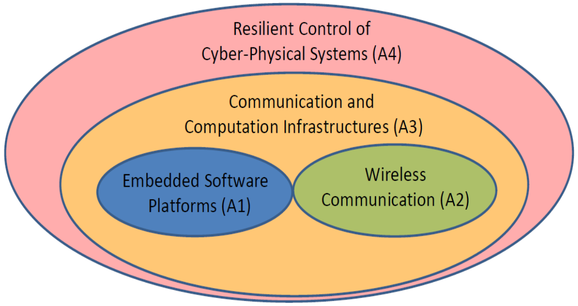
- Area 1: Embedded Software Platforms (Dam)
- Area 2: Wireless Communication (Thobaben)
- Area 3: Communication and Computation Infrastructure (Dán)
- Area 4: Resilient Control of Cyber-Physical Systems (Sandberg)

Example: The Smart Grid





A1: Embedded Software Platforms (Dam)



Challenges

- Closed, proprietary HW+SW stacks
- Weak security guarantees
- No runtime platform updates

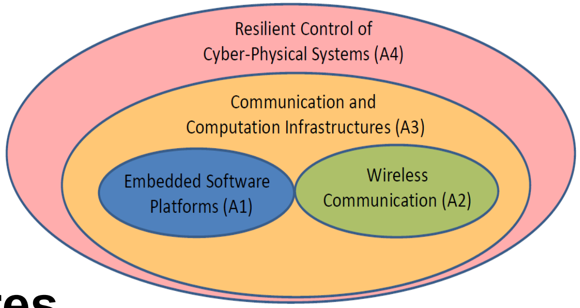
Goals

- Demonstrate that SCADA field devices built on COTS hardware can be certifiably secured at high EAL (5+)

Contributions

- Experimental, formally verified, software components and platforms
- Verified services for e.g. secure kernel updates

A2: Wireless Communication (Thobaben)



Challenge: Wireless SCADA infrastructures

- New classes of attacks in the wireless domain: eavesdropping, jamming, impersonation, data injection,...
- Low-complexity devices: standard security features are too complex; latency issues

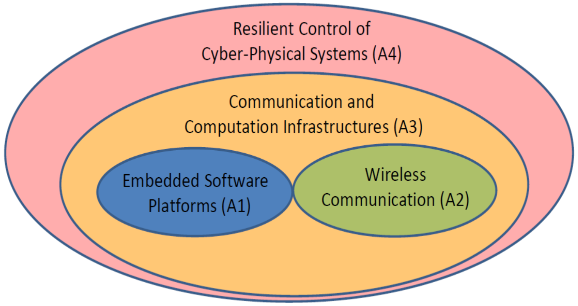
Goals

- Reduce the overall security overhead by protecting wireless SCADA infrastructures directly at the wireless interface (*physical-layer security*)

Contributions

- Low-complexity, low-latency physical layer security algorithms and protocols: authentication, key distribution, jamming protection
- Fundamental theory and experimental validation

A3: Communication and Computation Infrastructures (Dán)



Challenges

- CIA under delay, computational, and scaling constraints
- Virtualized and highly interconnected environments

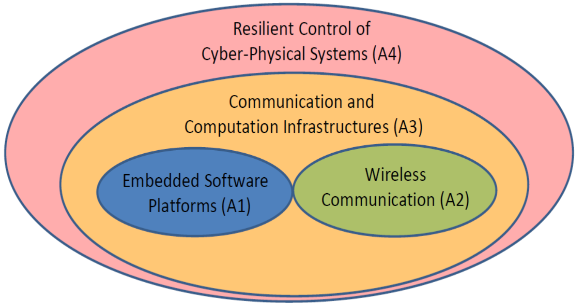
Goals

- Secure and resilient algorithms and protocols for SCADA communication and computation in shared environments

Contributions

- Secure communication protocols and networked-based synchronization
- DoS-resilient communication protocols/architectures
- Composing secure services in shared environments

A4: Resilient Control of Cyber-Physical Systems (Sandberg)



Challenges

- Critical infrastructures are cyber-physical systems
- Physical components introduce safety and reliability requirements qualitatively different from those in general purpose computing

Goals

- Secure and resilient large-scale control systems
- Exploit cyber-physical modeling

Contributions

- Critical infrastructure modeling tools for physical impact and vulnerability analysis
- Model-based intrusion detection methods
- Resilient control design methodology

Organisation

A1 Embedded Software Platforms	A2 Wireless Communication	A3 Communication and Computation Infrastructures	A4 Resilient Control of Cyber-Physical Systems
Dam (10%) PhD student (80%)	Thobaben (10%) PhD student (80%)	Dán (10%) PhD student (80%)	Sandberg (15%) PhD student (80%)

CERCES and CRATE Testbeds

Postdoc 1 (~50%)
Postdoc 2 (~50%)

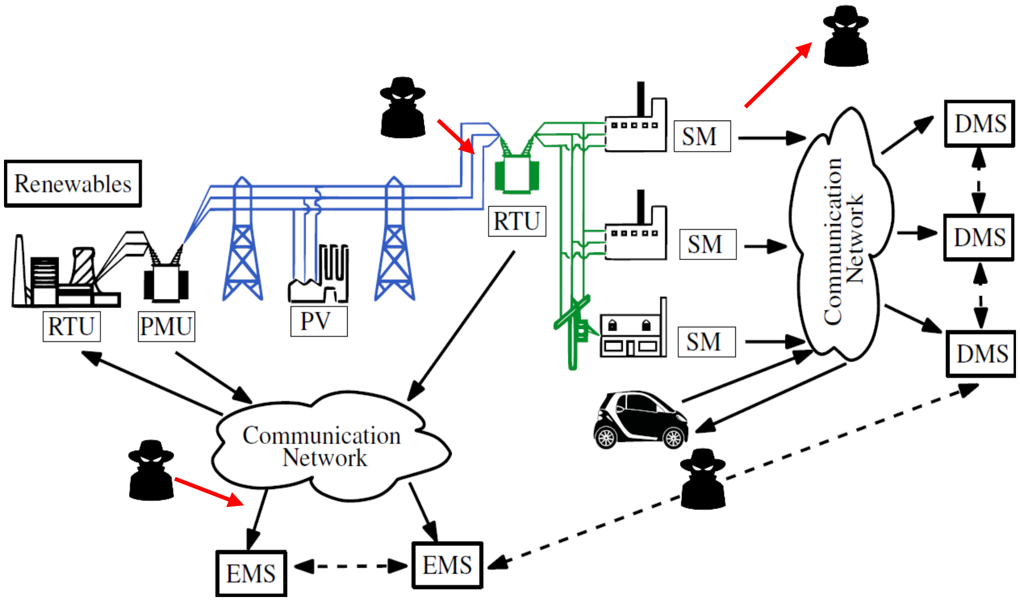
Outline of Presentation

- The consortium
- Background
- Main research objectives
- **Sample of research in resilient control and communication (A3-A4)**
  - **Cyber-physical defense in the smart grid**

The Smart Grid and Its Cyber Threats

Smart Grid

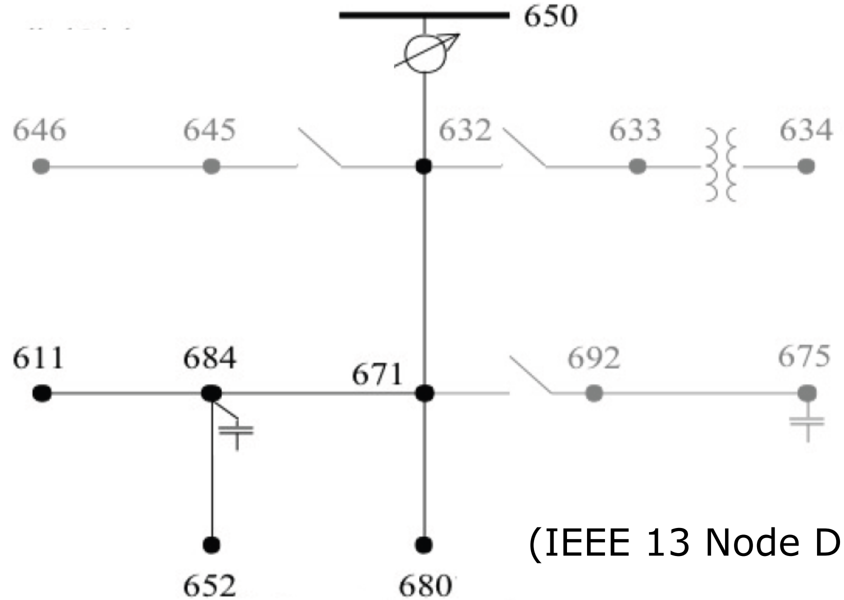
- More smart devices and control loops
- Large increase in communication and data
- Leads to increasing vulnerability to cyber-physical threats with many potential points of attacks



Integrated Volt/VAR Control

- Maintain voltage at end of line within limits and minimize losses

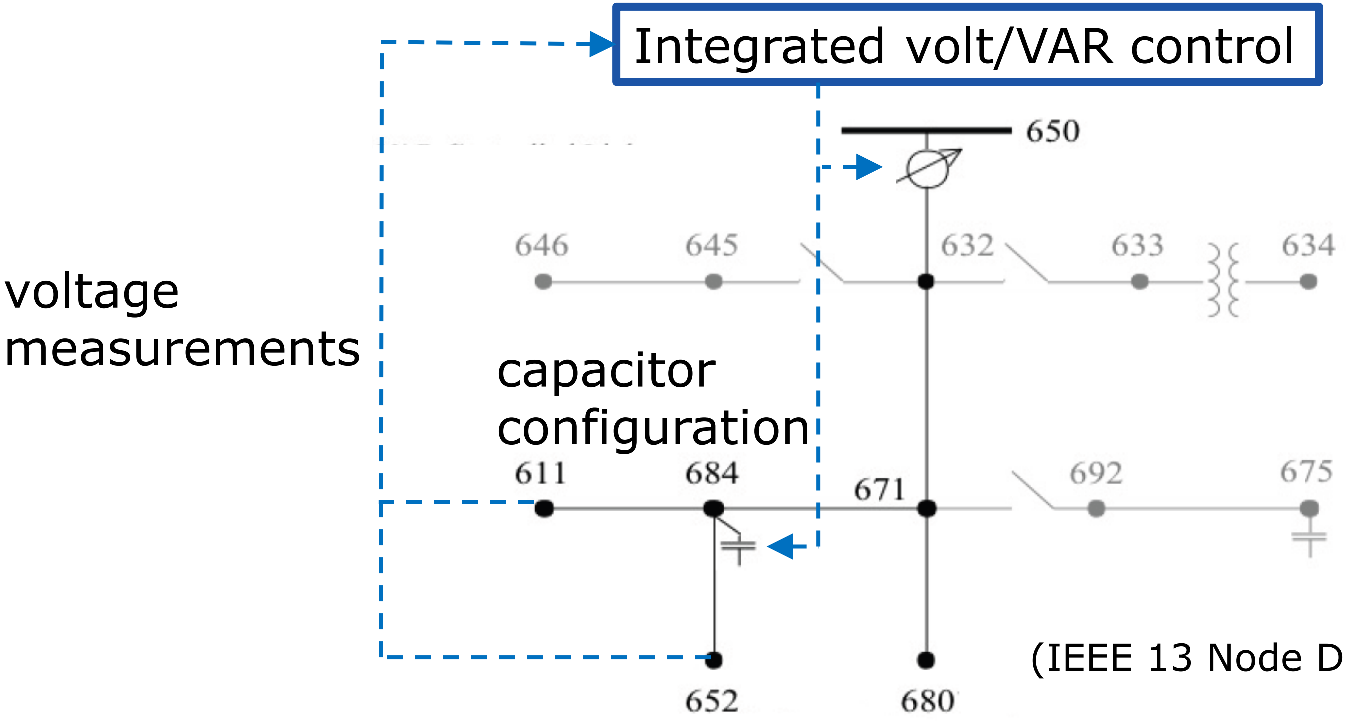
Main feeder
connected to
transmission grid



(IEEE 13 Node Distribution System)

Integrated Volt/VAR Control

- Maintain voltage at end of line within limits and minimize losses
- Energy saving around 3 % [Roytelman and Landenberger, 2009]

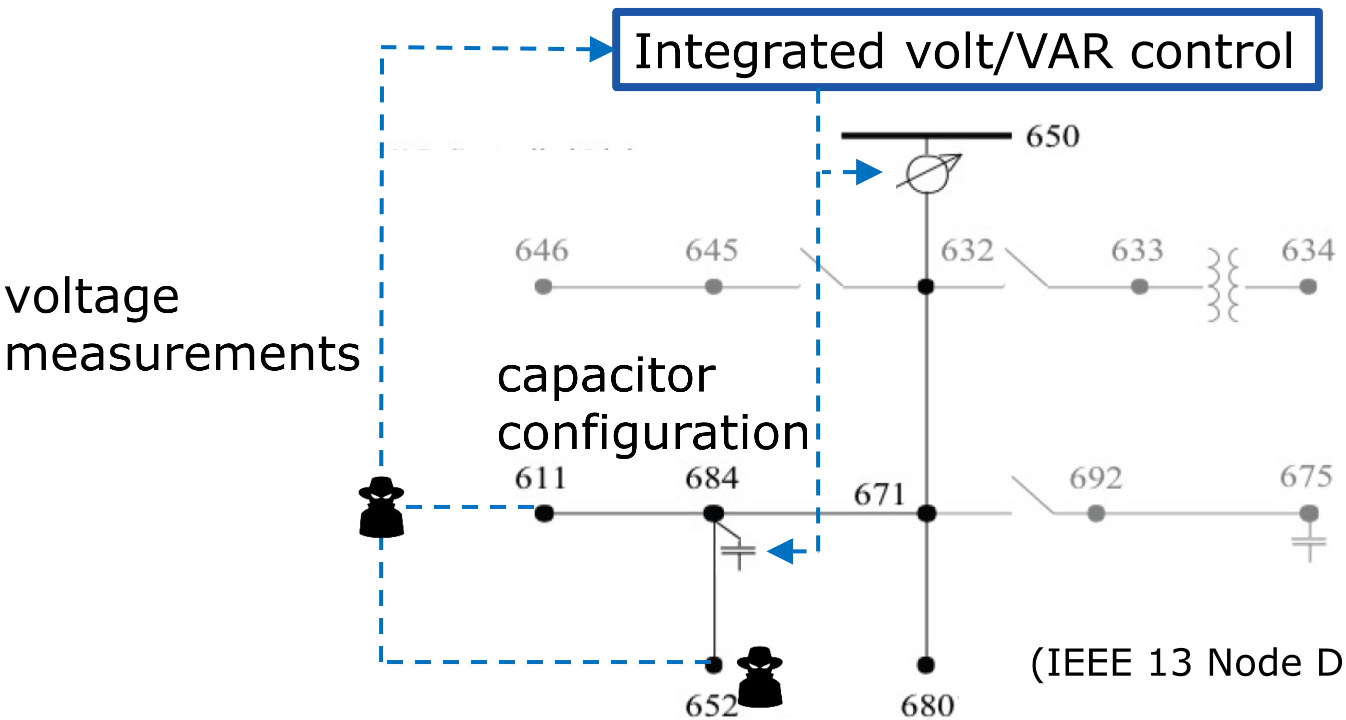


(IEEE 13 Node Distribution System)

KTH Electrical Engineering

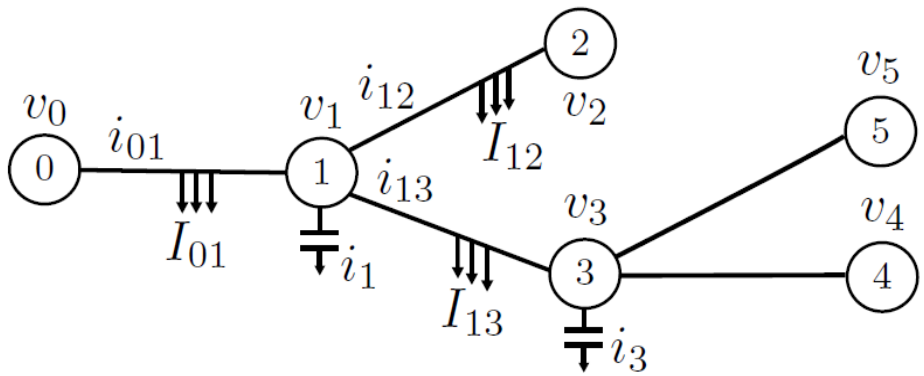
Integrated Volt/VAR Control

- Maintain voltage at end of line within limits and minimize losses
- Energy saving around 3 % [Roytelman and Landenberger, 2009]
- **Our scenario:** Compromised measurements



(IEEE 13 Node Distribution System)

Distribution Grid Model ("the Physics")



- Kirchoff's current law: $$i_{ij} = I_{ij} + i_j + \sum_{k \in \mathcal{N}_j \setminus \{i\}} i_{jk}$$
- Kirchoff's voltage law: $$v_j = v_i - Z_{ij} \left(\frac{1}{2} I_{ij} + \sum_{k \in \mathcal{N}_j} i_{jk} + i_j \right)$$
- System state: $\mathbf{y} = \begin{pmatrix} I_{01} & I_{12} & \ldots & \end{pmatrix}^\top \in \mathbb{C}^n$ and v_0
- Control (capacitor configuration): $C_k = \{\sigma_1, \ldots, \sigma_m\}$

Consumer and Operator Models ("the Cyber Part")

1. **Consumer model:**
   - The state $\mathbf{y}$ (current loads) and v_0 (main feeder voltage) is independent on capacitor configuration C_k
   - Consumers report voltage violations

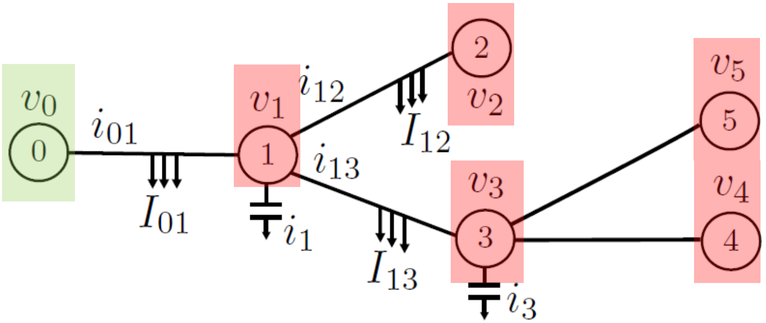
2. **Operator model:** Integrated volt/VAR controller optimizes the capacitor configuration

$$C^*(\mathbf{x}) = \arg \min_{C \in \mathcal{C}_{\mathcal{F}}(\mathbf{x})} V(\mathbf{x}, C)$$

   - minimize cost function (e.g., V = total power injection)
   - subject to end-of-line voltage constraints
   - $\mathbf{x}$ is estimated, possibly corrupted, system state

Adversary Model

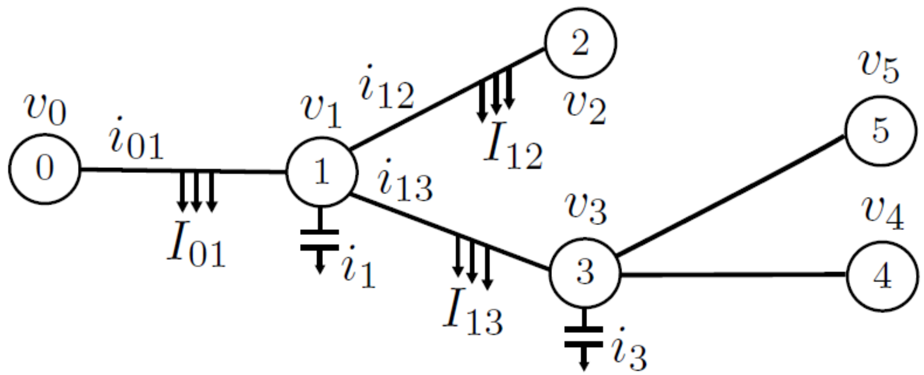
3. **Adversary's goal:** Increase operator's cost (V), while remaining undetected
   - The adversary may alter voltage measurements $\mathbf{v}$, but not main feeder power injection and voltage



   - The adversary performs a one-shot attack $\mathbf{v} \to \mathbf{v} + \mathbf{a}$

- **Questions:**
   - When can the volt/VAR controller detect the attacks $\mathbf{a}$?
   - How can it limit the effects of the attacks?

Example: Operators Control Actions



- Control configurations:

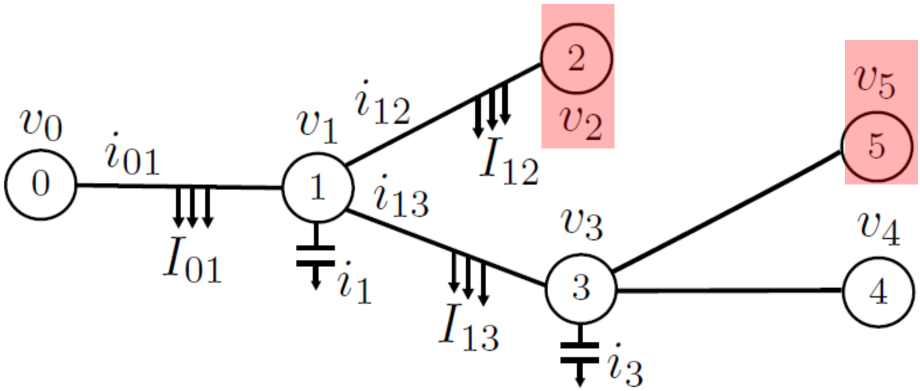
$$C_1: \quad z_1 = -0.28j\,\text{pu} \qquad z_3 = -1.66j\,\text{pu}$$

$$C_2: \quad z_1 = \infty\,\text{pu} \qquad z_3 = -1.66j\,\text{pu}$$

$$C_3: \quad z_1 = -0.28j\,\text{pu} \qquad z_3 = \infty\,\text{pu}$$

$$C_4: \quad z_1 = \infty\,\text{pu} \qquad z_3 = \infty\,\text{pu}$$

$\mathcal{C}$-Stealth Attack Example

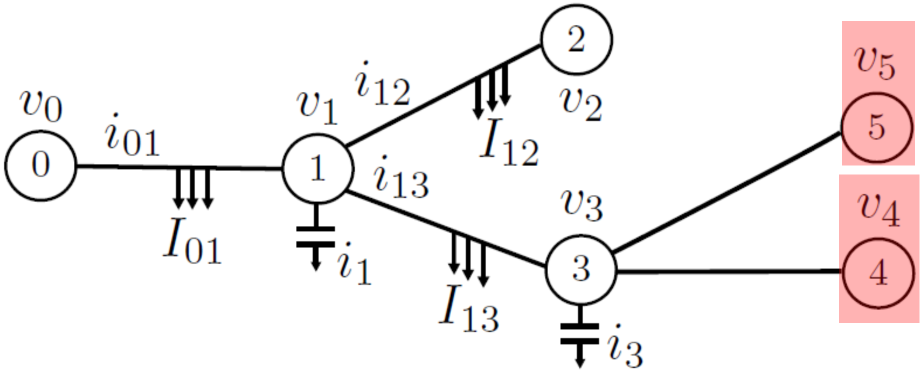


- Basis of all $\mathcal{C}$-stealth attacks:

$$H_v(C_1)B_{\mathcal{C}} = \begin{pmatrix} 0.00 & 0.00 \\ 1.00 & 0.00 \\ 0.00 & 0.00 \\ 0.00 & 1.00 \\ 0.25 & -1.00 \end{pmatrix}$$

[Teixeira *et al.*, ACC 2014]

$\mathcal{C}$-Stealth Attack Example



- Basis of all $\mathcal{C}$-stealth attacks:

$$H_v(C_1)B_{\mathcal{C}} = \begin{pmatrix} 0.00 & 0.00 \\ 1.00 & 0.00 \\ 0.00 & 0.00 \\ 0.00 & 1.00 \\ 0.25 & -1.00 \end{pmatrix}$$

[Teixeira *et al.*, ACC 2014]

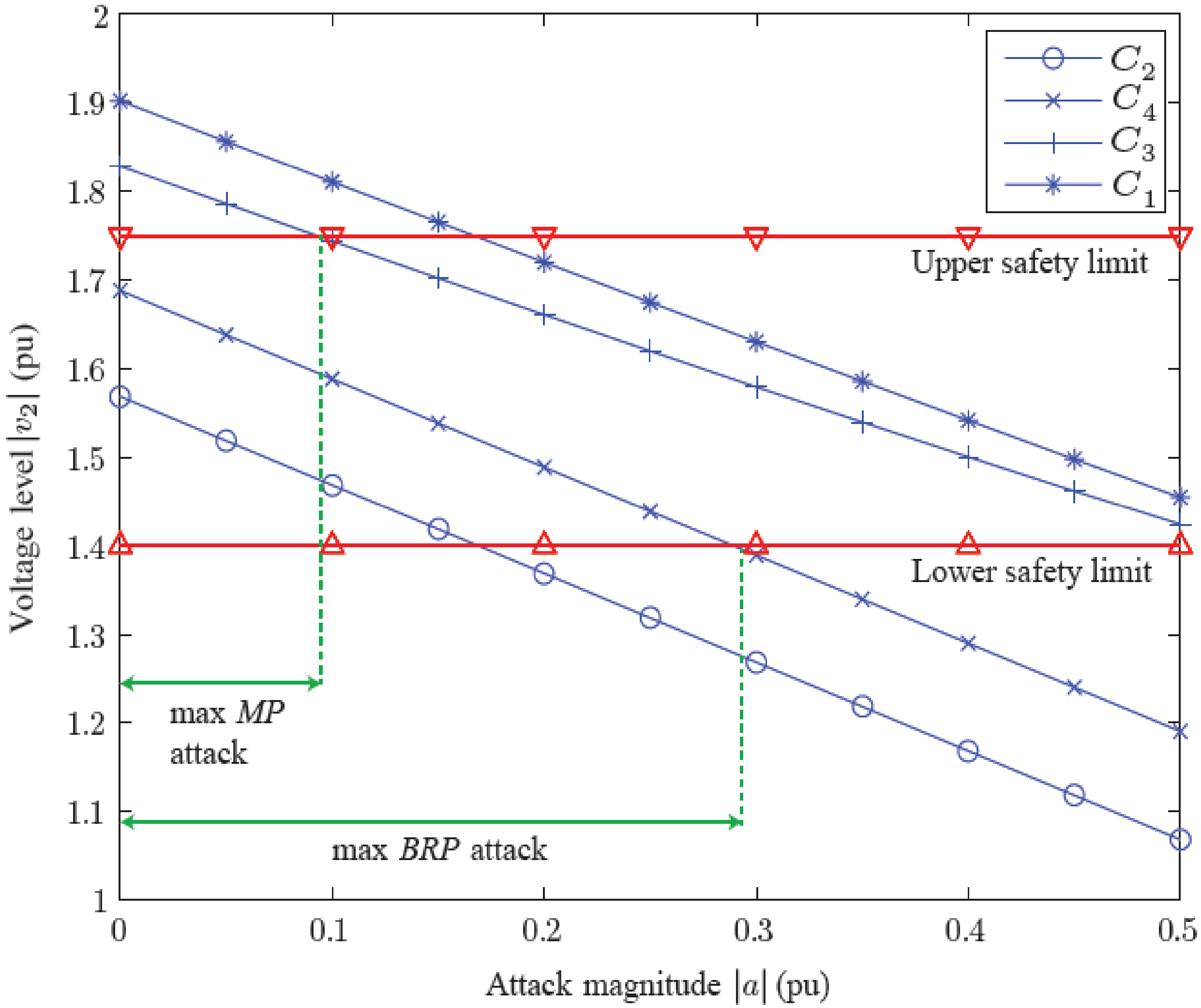
The Operator vs the Adversary

- Stealthy measurement attacks exist
- Attacks may even be stealthy under arbitrary control actions
- Use **game theory** and **mixed strategies** to limit impact
  - Pure strategy: use $C^*(\mathbf{x}) = \arg \min_{C \in \mathcal{C}_{\mathcal{F}}(\mathbf{x})} V(\mathbf{x}, C)$
  - Mixed strategy: use $C^*(\mathbf{x})$ with high probability
- Example next

[Teixeira *et al.*, ACC 2014]

KTH Electrical Engineering

Operator vs Adversary Game



MP=Mixed operator strategy **BRP=Pure operator strategy**

Summary of Research Sample

- Cyber attacks against the smart grid a great concern
- Characterization of stealth attacks against volt/VAR control
- Use game theory and mixed strategies:
  - Quantitative worst-case analysis
  - New control strategies
- Future work:
  - More realistic consumer, operator, adversary models
  - Automatic detection system

CERCES Contributions to a Resilient and Secure Society

- **Defense in depth:** Provide new set of tools in several system layers (mobile systems, IoT, power systems, etc.). Tests in NSC3's CRATE testbed
- **Education and training:** Raise awareness, new courses, industrial workshops (target groups: students, government agencies, industrial partners)
- **Scientific community:** Cross-disciplinary contributions in security
- **New possible business opportunities:** Analysis tools, secure platforms

KTH ROYAL INSTITUTE
OF TECHNOLOGY

Center för resilienta kritiska infrastrukturer (CERCES)

Henrik Sandberg (hsan@kth.se)
Avdelningen för reglerteknik

MSB:s forskardagar, Stockholm, 11-12 november, 2015