FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Platform-based Resilience for CPS

Gabor Karsai
Vanderbilt University

Domain:
Power Transmission and Distribution Systems

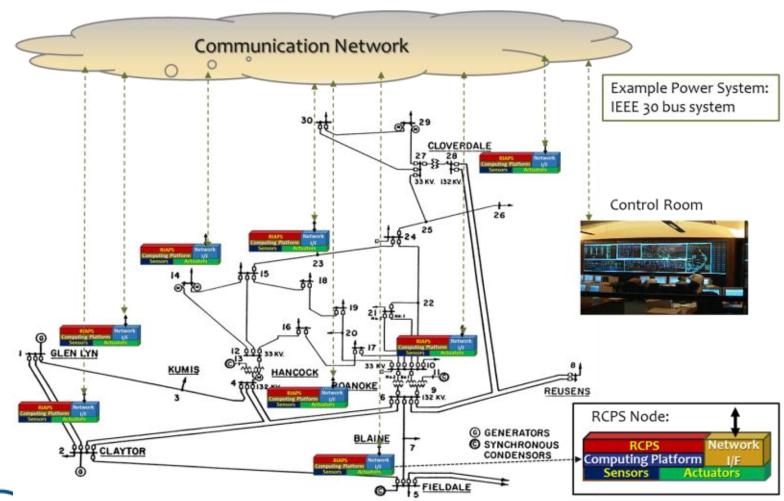
Power systems are potentially vulnerable in all components: generators, transmission and distribution system, end-user loads, protection system, power management systems –

Threat model: Physical faults + …

- Mis-operation of protective equipment
- Integrity/DDOS attack on the network
- Replay attacks, etc.

Resilience challenges:

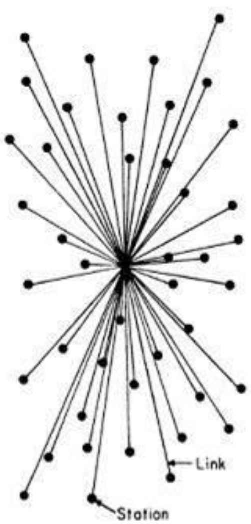
- Faults in the power system, in computing hardware and software, in the network
- Algorithms for protection, monitoring, control, energy management, state estimation, analytics..
- Defense against and recovery from cyber-attacks



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Supported, in part, by ARPA-E

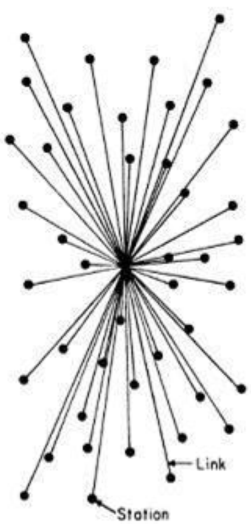
The Evolution of Energy Networks

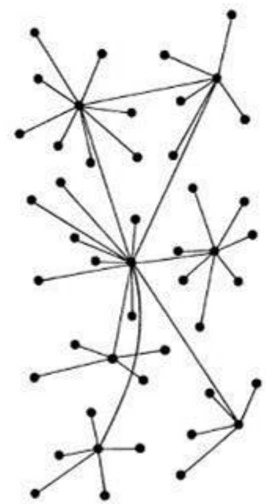


Traditional networks with transmission system operators, distribution system operators & radial distribution systems to communities

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

The Evolution of Energy Networks



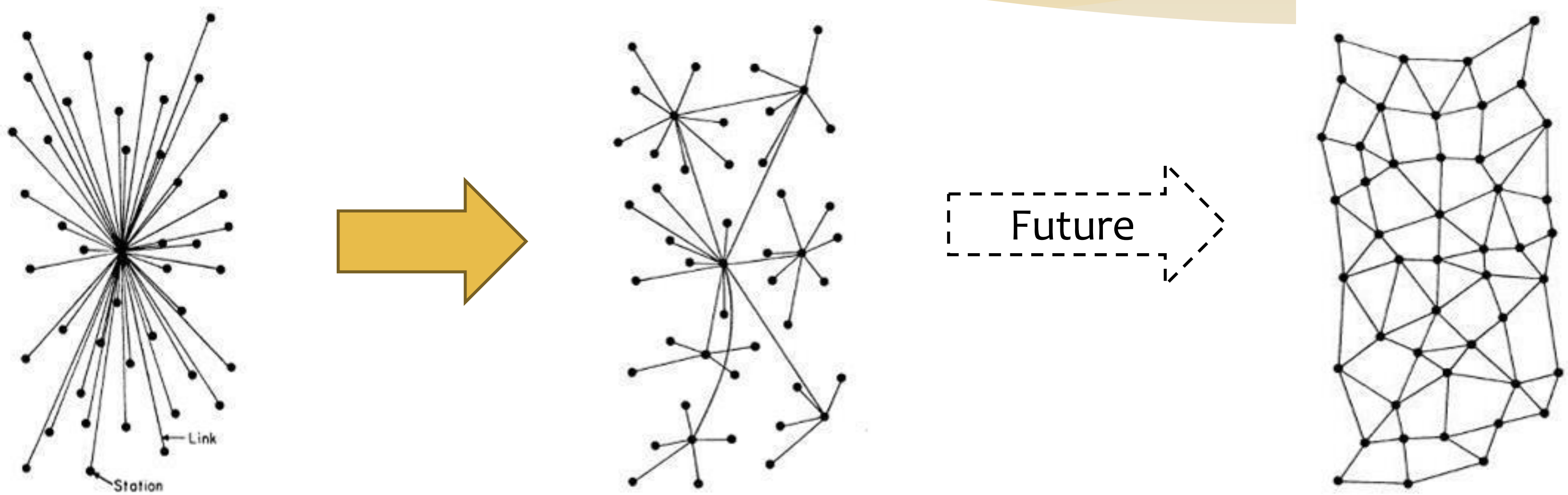


Network of distribution feeders with some microgrids with tightly integrated distributed energy resources

- Advantages of decentralization
  - Improved cyber & physical reliability by removing single point of failures
  - Faster decision making by avoiding network penalties due to round-trip to the cloud
  - Improved scalability
  - Better integration with hierarchical control systems

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

The Evolution of Energy Networks



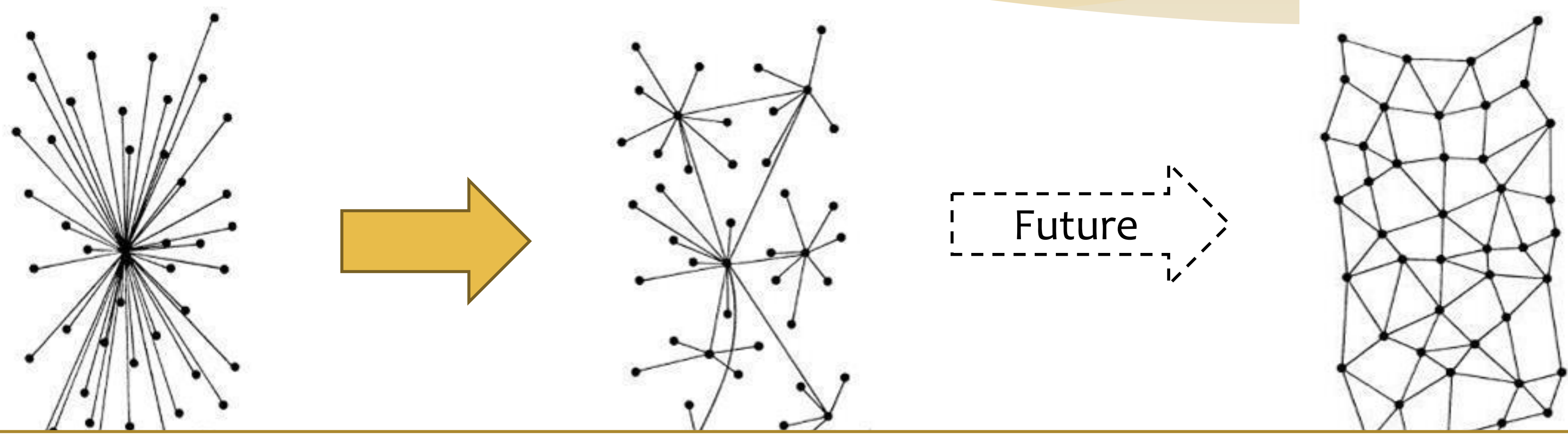
Traditional networks with transmission system operators, distribution system operators & radial distribution systems to communities

Network of distribution feeders with some microgrids with tightly integrated distributed energy resources

Network of transactive microgrids with limited role of distribution system operators

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

The trend of decentralization



This trend of decentralization can be seen around many other cyber-physical system applications, for example: smart manufacturing, smart cities, etc.

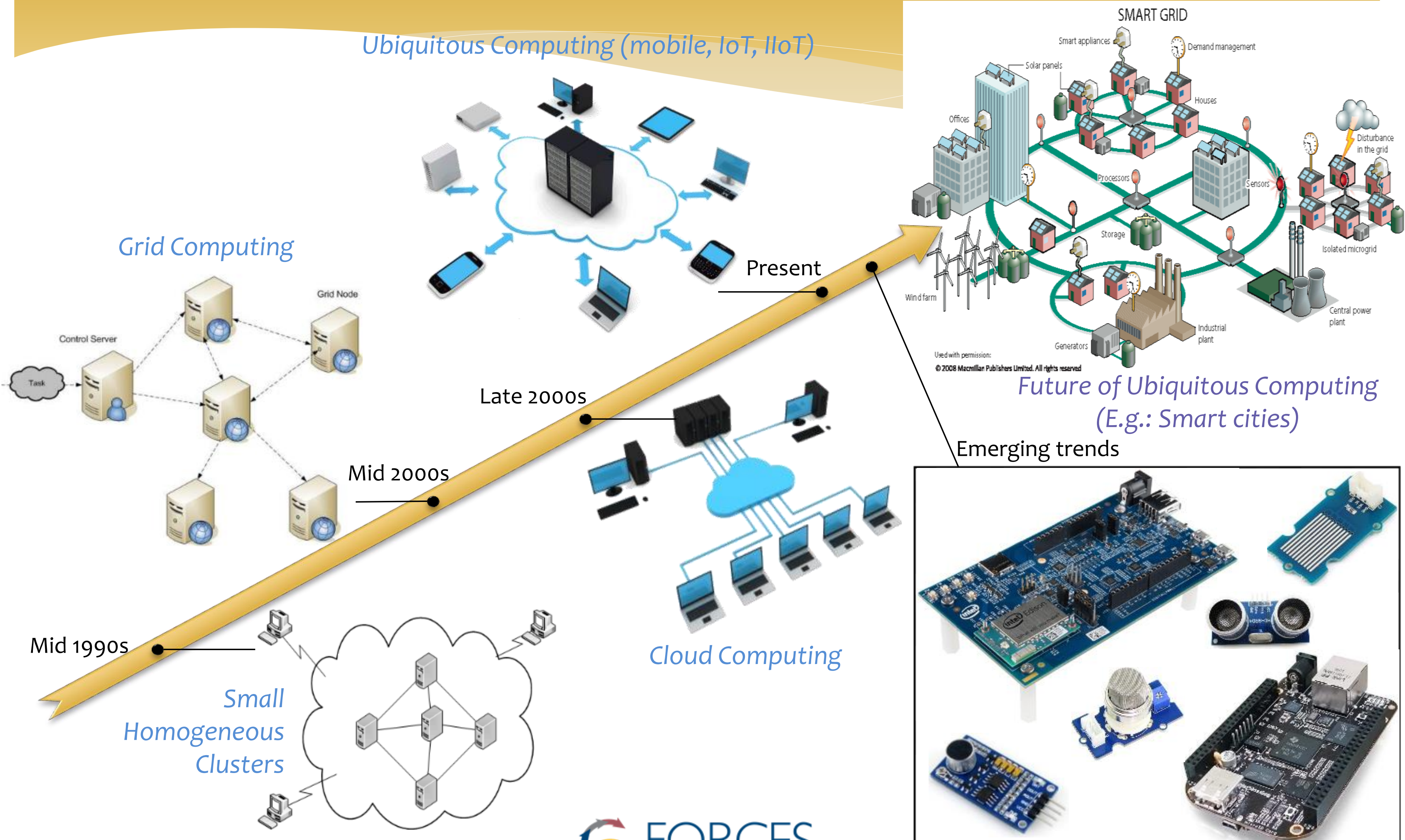
Traditional networks with transmission system operators, distribution system operators & radial distribution systems to communities

Network of distribution feeders with some microgrids with tightly integrated distributed energy resources

Network of transactive microgrids with limited role of distribution system operators

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

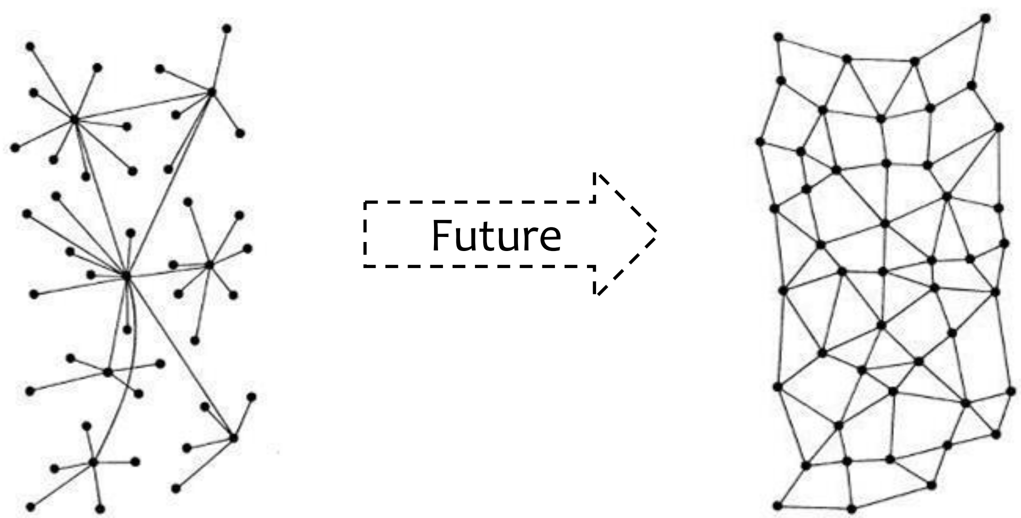
What enables this trend of decentralization?



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

The increased DevOps complexity

* Programming, developing, managing decentralized & distributed networks is hard
* A number of services that are orthogonal to the application logic are required
  * Time synchronization
  * Messaging middleware
  * Consensus & coordination mechanisms
  * Discovery & deployment mechanisms
  * Fault-detection & recovery mechanisms
  * Distributed security mechanisms



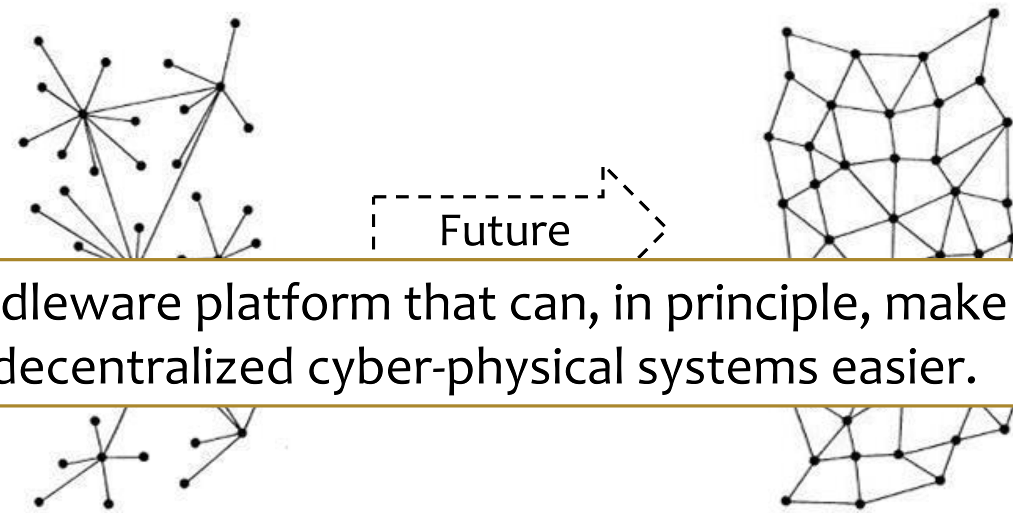
Network of distribution feeders with some microgrids with tightly integrated distributed energy resources

Network of transactive microgrids with limited role of distribution system operators

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

The increased DevOps complexity

* Programming, developing, managing decentralized & distributed networks is hard
* A number of services that are orthogonal to the application logic are required



This motivates the need for a middleware platform that can, in principle, make the task of programming these decentralized cyber-physical systems easier.

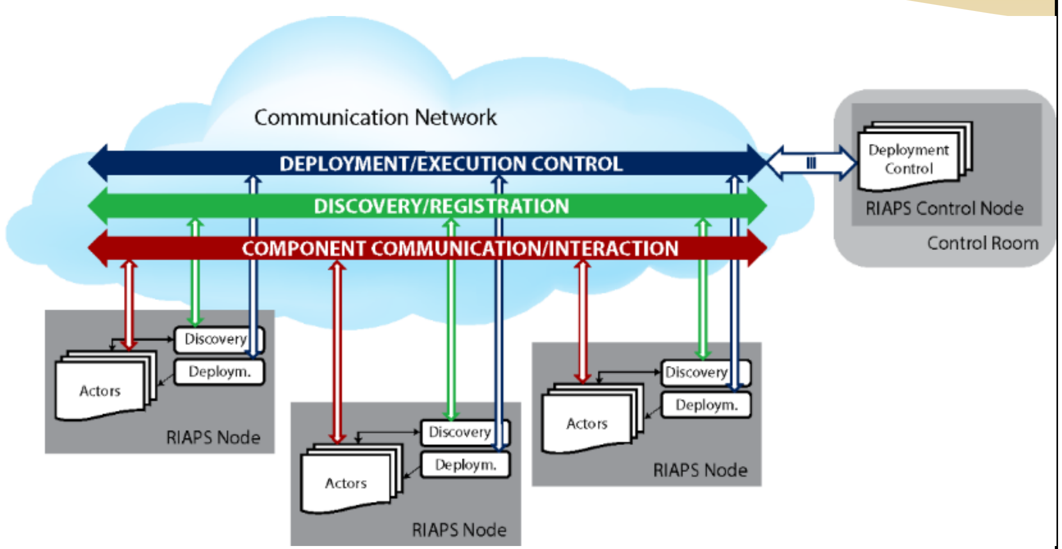
  - Consensus & coordination mechanisms
  - Discovery & deployment Mechanisms
  - Fault-detection & recovery mechanisms
  - Distributed security mechanisms

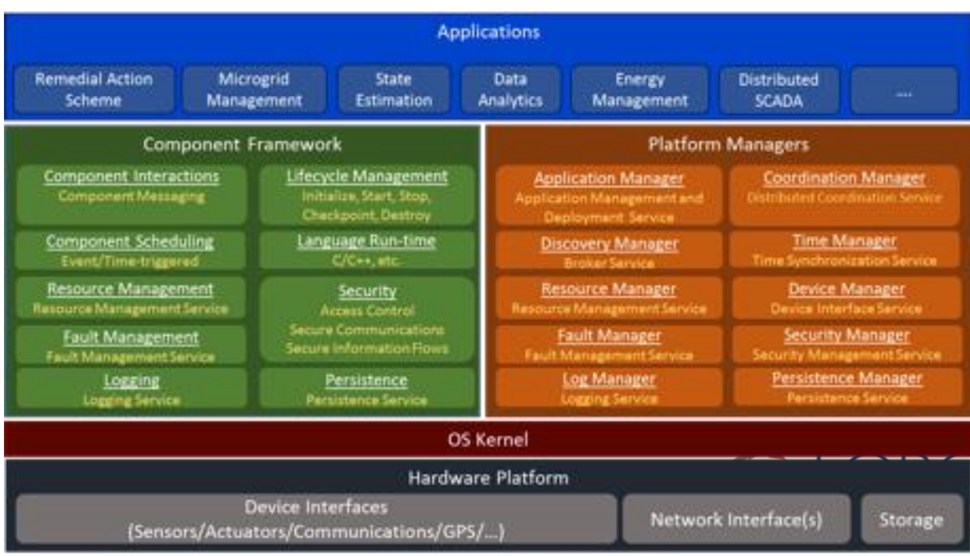
Network of distribution feeders with some microgrids with tightly integrated distributed energy resources

Network of transactive microgrids with limited role of distribution system operators

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

RIAPS: Middleware for Decentralized Computing

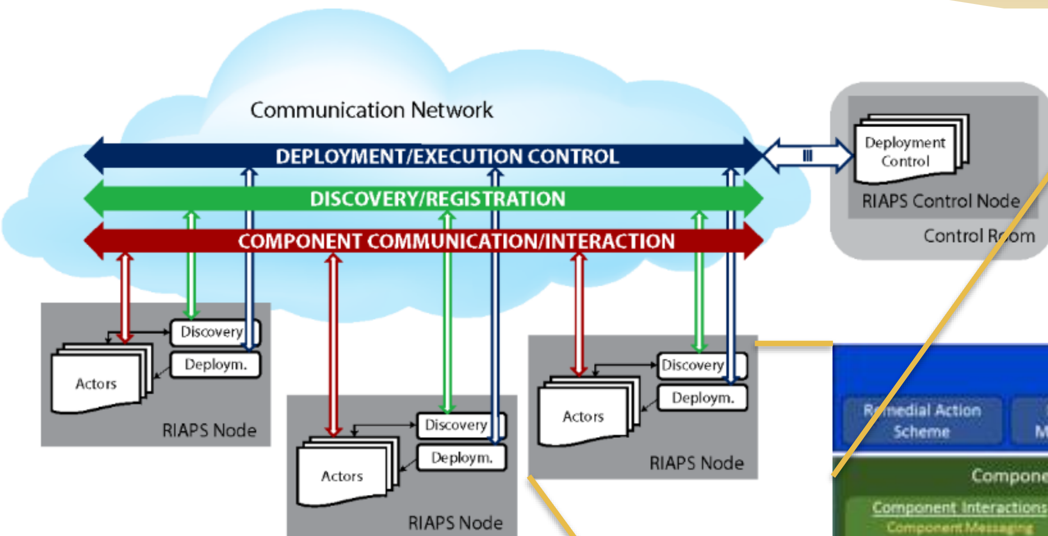


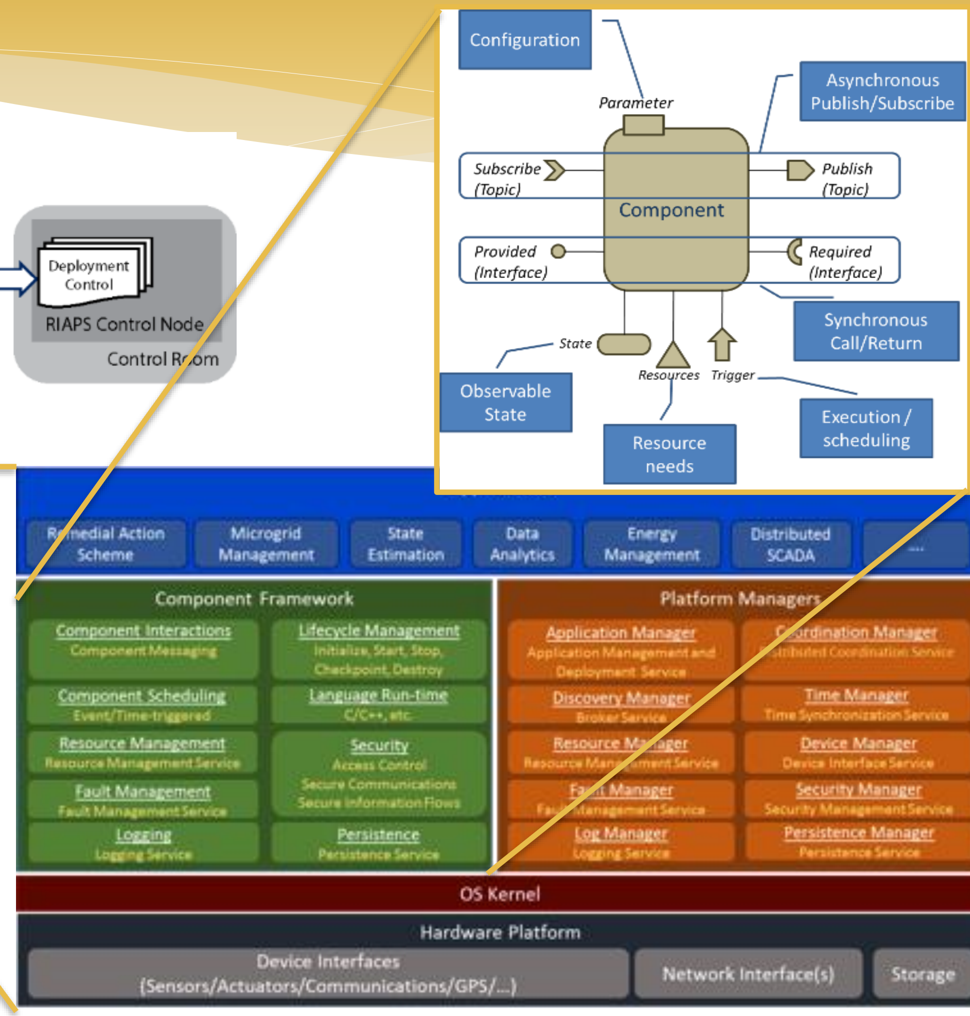


- Goal: Build a *software platform* to run Smart Grid applications and demonstrate it through *selected applications*
- This software platform defines:
  - Programming model (for distributed real-time software)
  - Services for
    - Time synchronization
    - Messaging middleware
    - Robust consensus and coordination
    - Secure discovery and deployment
    - Fault-detection and recovery
    - Distributed security
  - Development toolkit (for building and deploying apps)
- Uniqueness:
  - Focus on distributed applications not only on networking
  - Focus on **resilience** – fault recovery
  - Focus on **security** – maintain confidentiality, integrity, availability

Supported, in part, by ARPA-E and Siemens CT

RIAPS: Middleware for Decentralized Computing

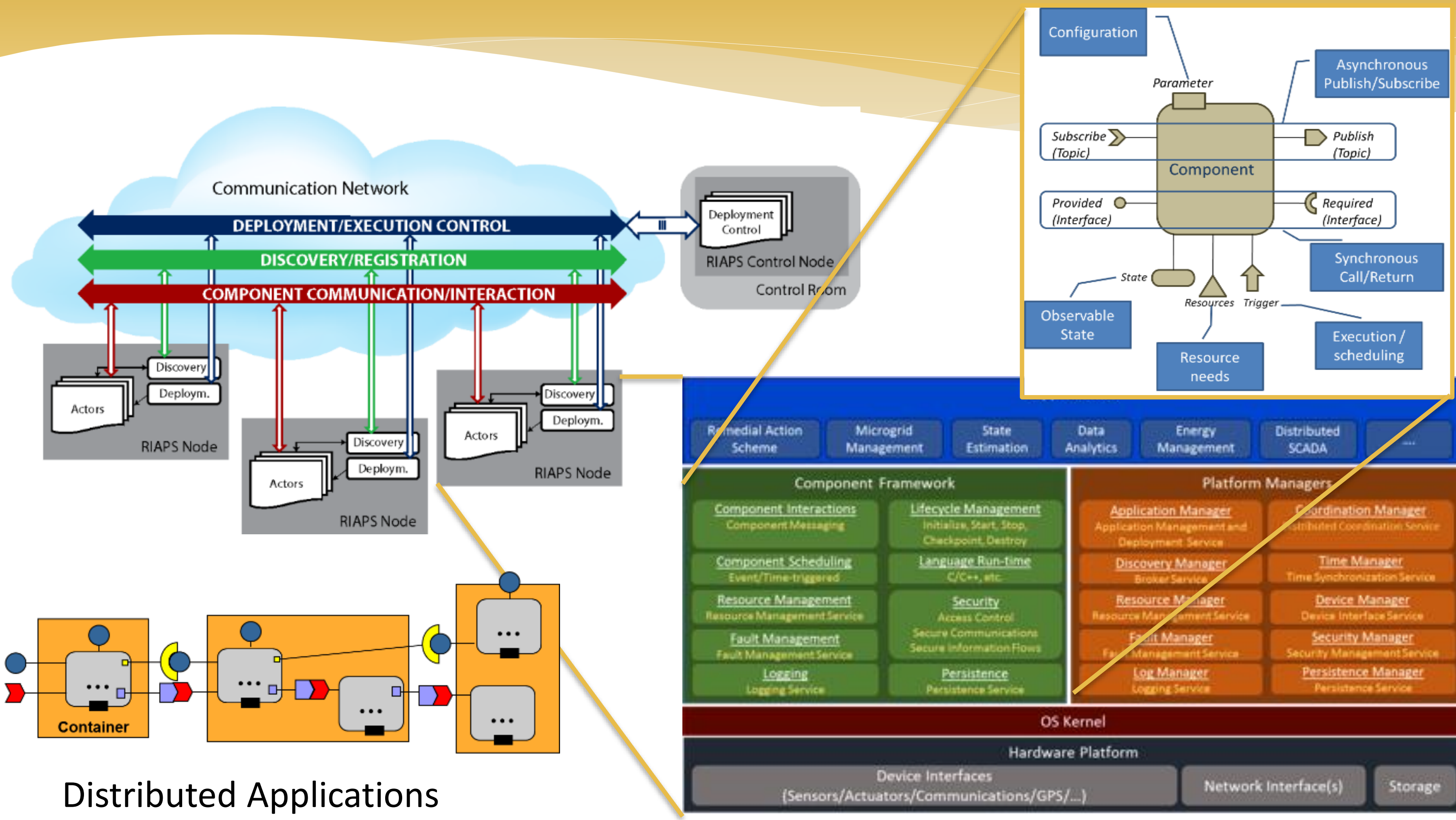




Loosely connected componentized applications are important for portability, interoperability, modularity & maintainability

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

RIAPS: Middleware for Decentralized Computing



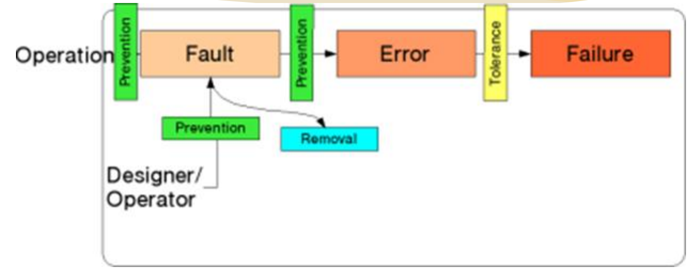
https://riaps.isis.vanderbilt.edu

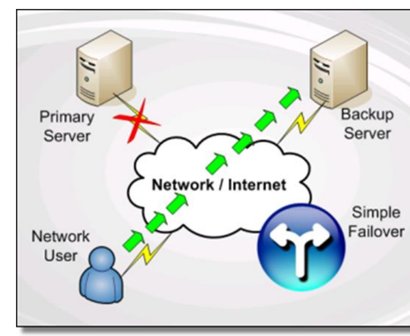
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

RIAPS: Middleware for Decentralized Computing
Steps Towards Resilience

Fault management

- Assumption: Faults can happen anywhere: application, software framework, hardware, network
- Goal: Developers must be able to develop apps that can recover from faults anywhere in the system.
- Use case: An application component hosted on a remote host stops permanently, the rest of the application detects this and 'fails over' to another, healthy component instead.
- Philosophy: The platform provides the mechanics, but app-specific behavior must be supplied by the app.



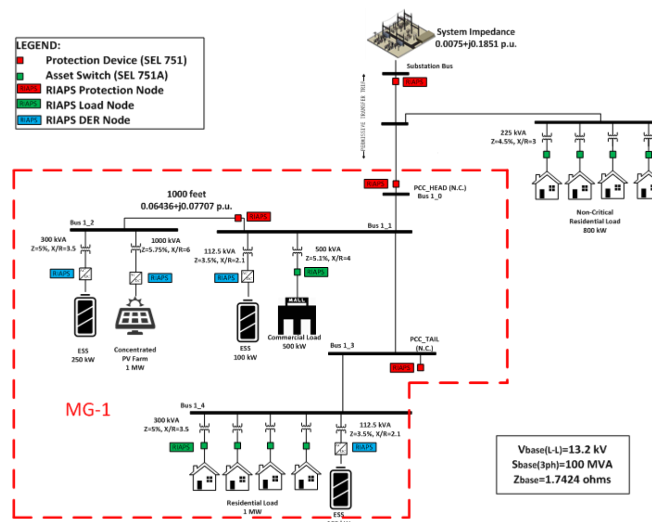


FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

RIAPS: Middleware for Decentralized Computing Steps Towards Resilience

Distributed Coordination

* The need: Reusable distributed coordination algorithms implemented in the framework
* Use case: Nodes implementing a microgrid controller need to dynamically form a group for the purpose of disconnecting from the main grid. They need to reach consensus on the future point in time when the disconnection happens.

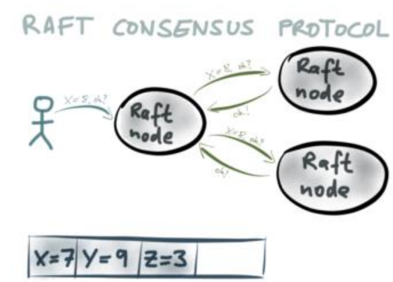


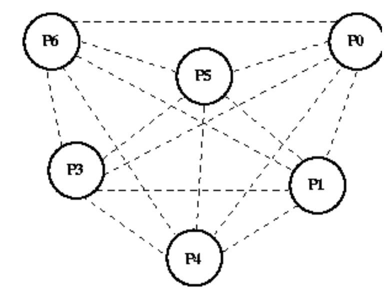
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

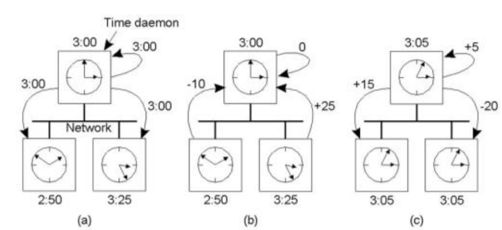
RIAPS: Middleware for Decentralized Computing Steps Towards Resilience

Distributed coordination

* Group membership
  * During run-time, application components can dynamically generate and form a group
  * Features: communication among group members, tracking membership changes
  * Dynamic group membership is maintained by the service in a fault-tolerant manner
* Leader election
  * Group members start a leader election process that results in a leader
  * When the leader drops out (fails or leaves the group) a new leader will be elected
  * Members are notified about leadership changes
* Consensus
  * Nodes attempt to reach agreement on a value, submit proposals
  * Each node can accept or reject the proposed value of the other nodes
  * The process stops when nodes reach consensus
* Time-synchronized action
  * Nodes are to execute a coordinated (control) action in the future
  * Each application component schedules an operation for itself
  * Fault tolerant, high-precision time synchronization service ensures that the operation is executed at the right time, on all nodes involved







RIAPS: Middleware for Decentralized Computing
Steps Towards Resilience

Security features

* Secure deployment and application management
  * Secure interactions with control nodes
  * Strong, cert-based authentication on everything
  * HW-based root of trust in the platform
* Secure communications
  * Secure messaging among application components
  * Secure discovery service
  * Secure information flows: process separation, isolated file systems
* Security management
  * Monitoring and logging
  * Renewable security

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Summary and Future Work

* A robust *software platform* is essential for implementing resilient systems
* The platform should provide features and services for
  * Fault management
  * Distributed coordination
  * Security defense and mitigation
* Application examples:
  * Microgrid Control
  * Remedial Action Schemes
  * Transactive Energy
  * Distributed SCADA
  * Real-time Analytics
* Development is in progress, early demonstrations are available

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS