Simulation & Emulation in Smart Grid Assessment

David M. Nicol
Director, Information Trust Institute
Professor, Electrical & Computer Engineering
University of Illinois at Urbana-Champaign

I have a dream…

That one day we will have the capability to embed a Smart Grid subsystem within a high fidelity virtual environment and quantitatively assess

- Behavior under realistic conditions
- Reliability in the face of faults
- Effectiveness of security defenses
- The presence of un-known vulnerabilities

I have a dream…

That one day we will have the capability to embed a Smart Grid subsystem within a high fidelity virtual environment and quantitatively assess

- Behavior under realistic conditions
- Reliability in the face of faults
- Effectiveness of security defenses
- The presence of un-known vulnerabilities

The high fidelity virtual environment is key

I have a dream…

That one day we can operate a Smart Grid assessment facility

- User requests hardware, software, simulators
- User describes experimental design (including output saved)
- Facility manages multiple requests
  - Allocates, auto-configures, and checkpoints resources
  - Runs experiments according to design
  - Stores output, releases resources, notifies users
  - Depending on experimental objective, suggests additional experiments

I have a dream…

That one day we can operate a Smart Grid assessment facility

- User requests hardware, software, simulators
- User describes experimental design (including output saved)
- Facility manages multiple requests
  - Allocates, auto-configures, and checkpoints resources
  - Runs experiments according to design
  - Stores output, releases resources, notifies users
  - Depending on experimental objective, suggests additional experiments

Virtualization and adaptive configuration are key

Pieces of the puzzle : devices

Relay
Phasor Measurement Unit
Phasor Data Collector
Programmable Logic Array
Meters
Sensors

AMI Relay
F-Net
Inverters
ICS Firewall
Data acquisition devices
Gigabit firewall

Pieces of the puzzle : software systems

Data historians

Control Systems

Home Energy Management Systems

Display + Visualization

On-line analysis

Intrusion detection systems

Meter Data Management Systems

Pieces of the puzzle : simulators

Electric flow	Communication	AMI
Powerworld	S3F	Trilliant Testbench
RTDS	RINSE	
PSCAD	PRIME	
PSLF	ns-3	
	Opnet	

Pieces of the puzzle : assessment tools

DSAtools

DynRed

Testbench

LabView

Mu Dynamics

Fortify

Testbed Donations Provided By

byres security inc
intrinsically secure

Mu Dynamics

Itron

OSIsoft.

OSI

endace

Electric Power Group

IBM

PowerWorld Corporation
The Visual Approach to Analyzing Power Systems

SPACE-TIME INSIGHT

BAYSHORE NETWORKS

Trilliant

NATIONAL INSTRUMENTS

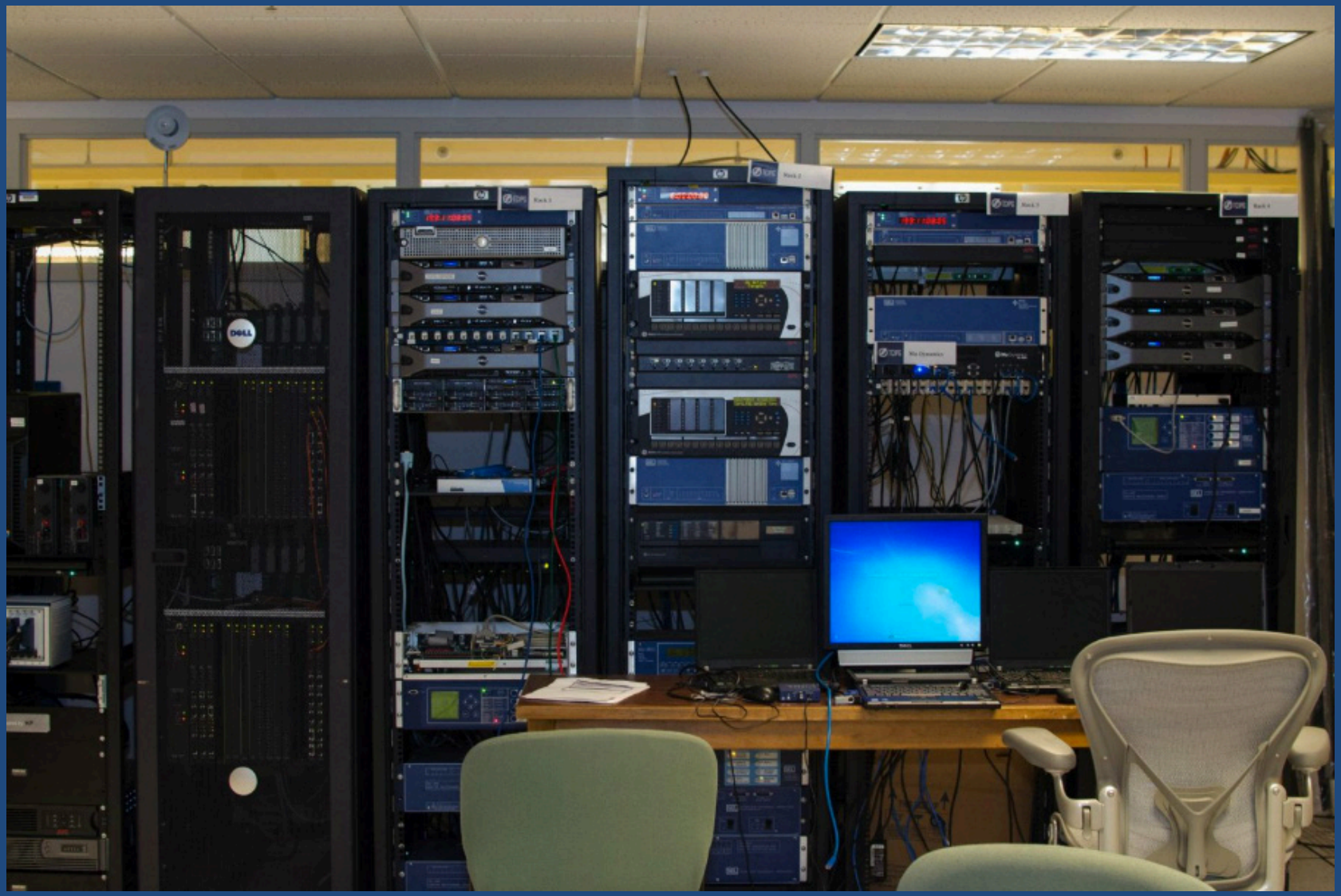
INSTEP

SISCO

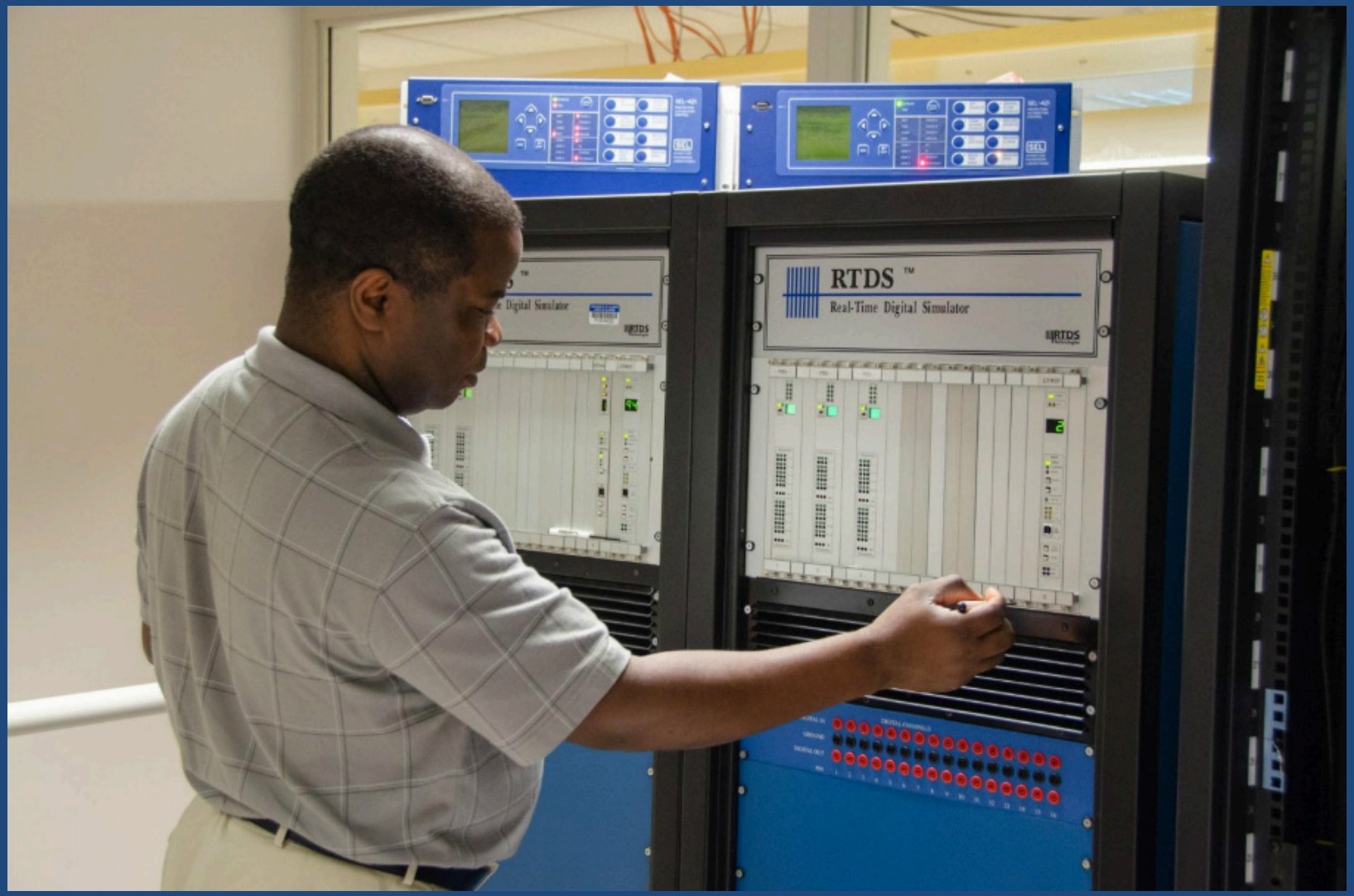
SEL SCHWEITZER ENGINEERING LABORATORIES

U.S.NRC
United States Nuclear Regulatory Commission

We've got it

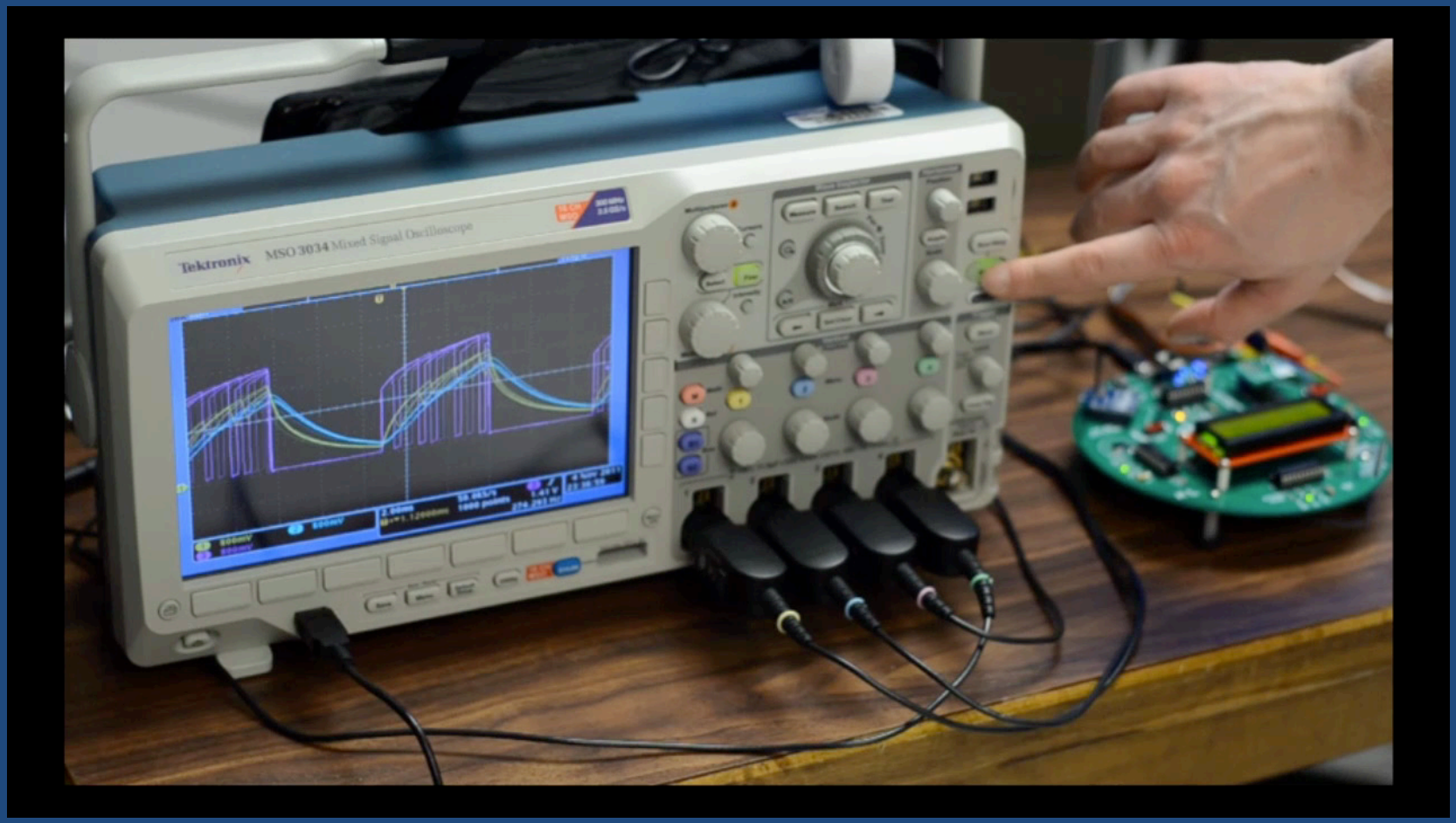


We've got it



We've got it

We’ve got it

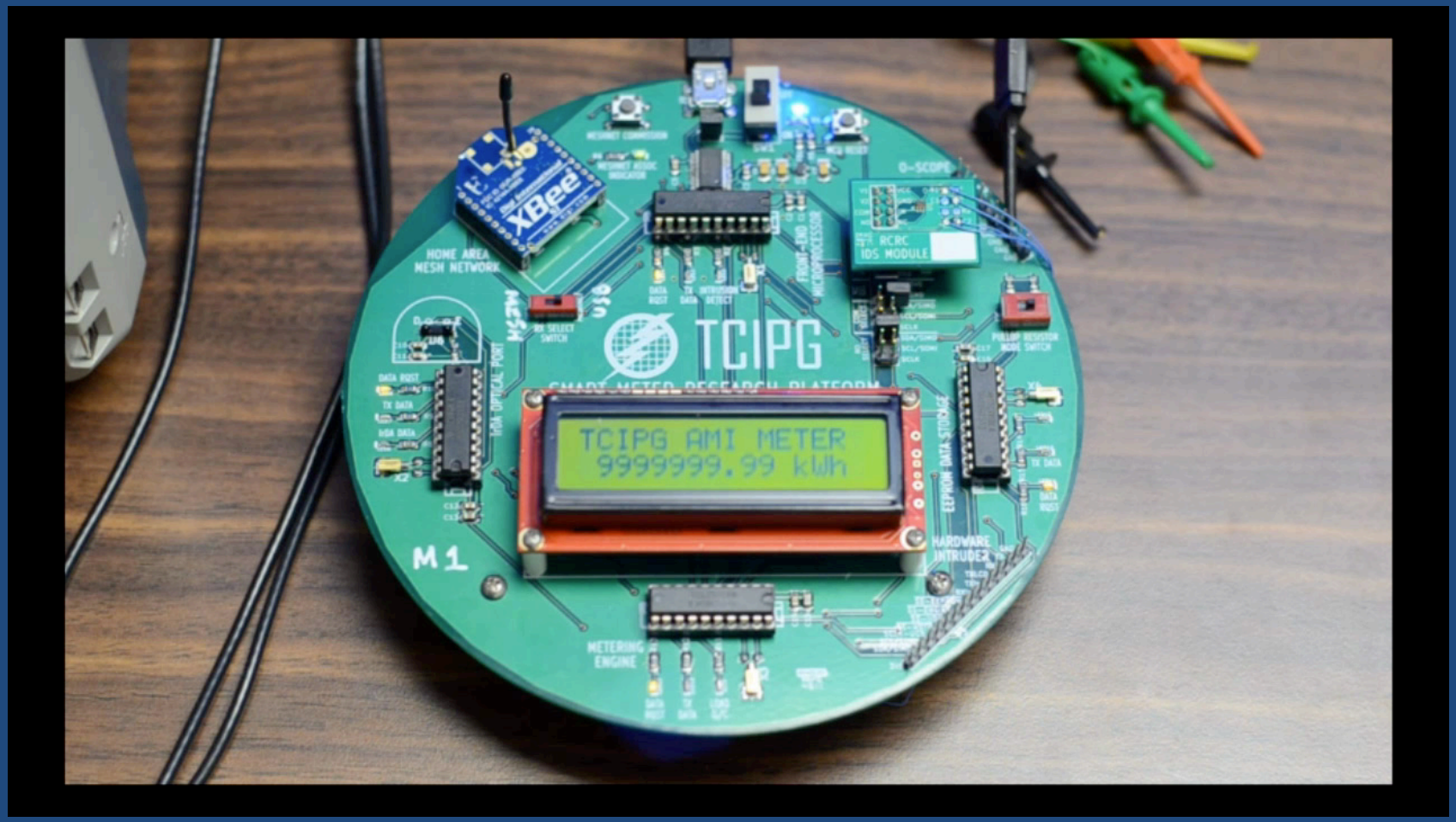


We've got it

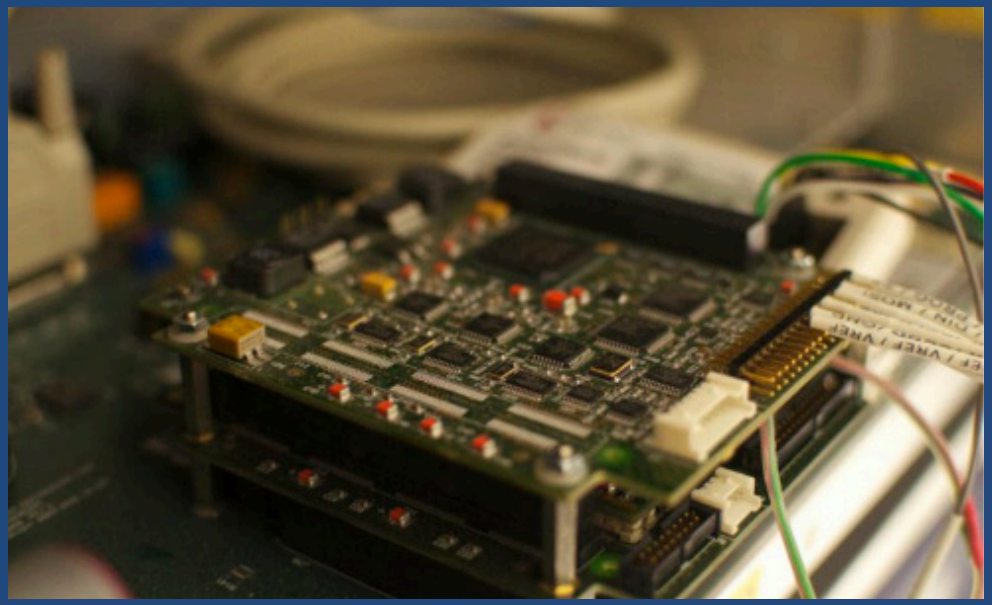
We've got it


120VAC/DC
PASS
FAIL
ALARM
TEMP
BAT LOW
POWER MODULE
MODEL 8310
120VAC/DC
TRICONEX
BATTERY
NI PXI-1033
NATIONAL INSTRUMENTS

We've got it


TCIPG
TCIPG AMI METER
9999999.99 kWh
M1
HOME AREA
MESH NETWORK
METERING
ENGINE
HARDWARE
INTRUDER
RCRC
IDS MODULE
XBee

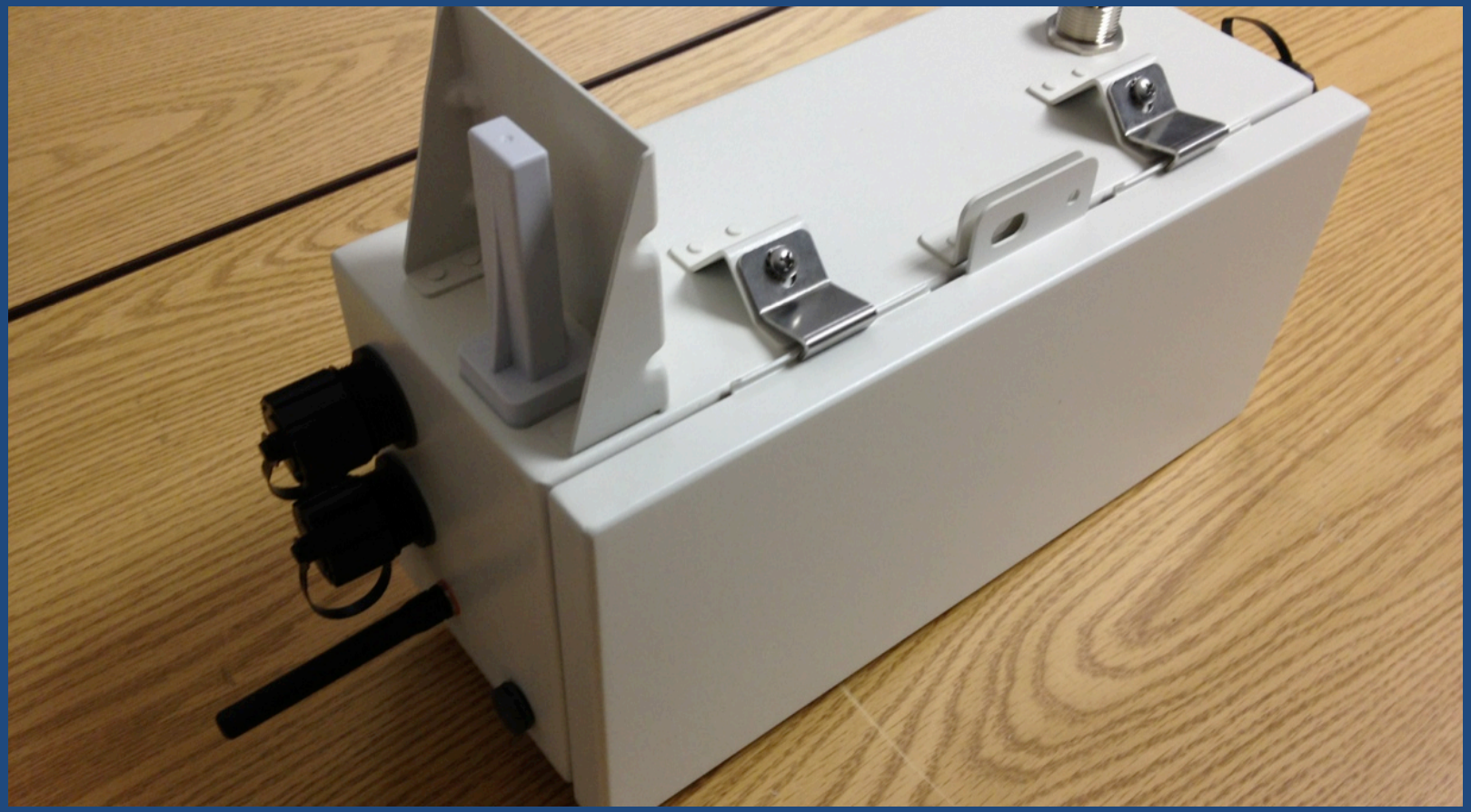
We've got it




SEL
137:14:42


SEL-3530
REAL-TIME AUTOMATION
CONTROLLER
ETH F
USB A
AUX 7
AUX 8
AUX 9
Mu Dynamics

We’ve got it



We've got it


DANGER / PELIGRO
DANGER / PELIGRO
HAZARD OF ELECTRICAL SHOCK OR BURN
MARKETING SAMPLE
306 382 289

I have a dream

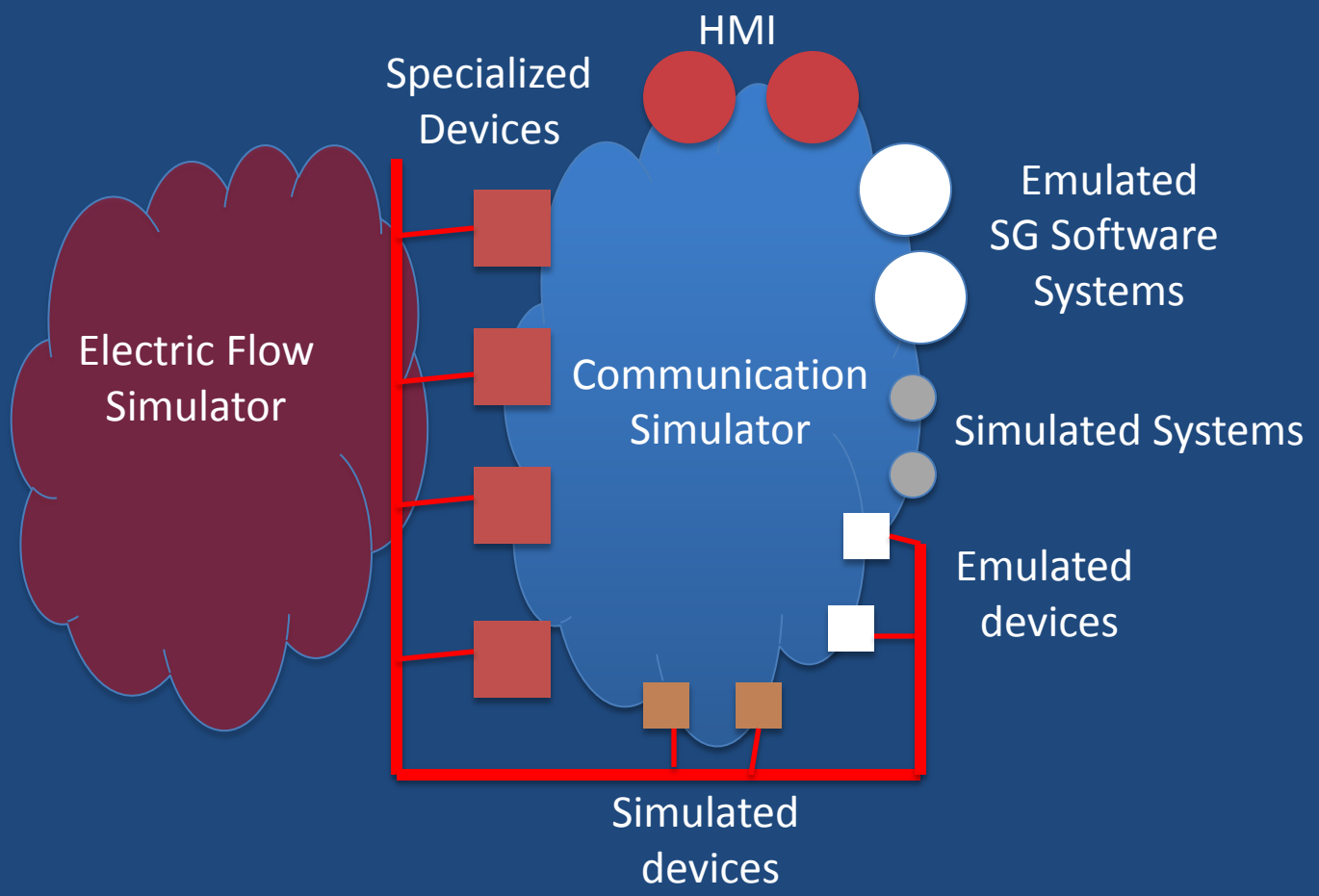
To make the whole greater than the sum of the parts

We need an infrastructure that includes all this reality, but also *models* of real stuff

We need simulation, and emulation

Assembling the puzzle

A high fidelity virtual environment presents to each interface a realistic representation of the environment



Emulation & Simulation

Emulation --- executing “native” software to produce behavior

Simulation --- executing model software to produce behavior

Emulation

- High fidelity functional behavior
- Typically tied to “wall-clock” time
- Resource intensive
- Little extra effort needed to include

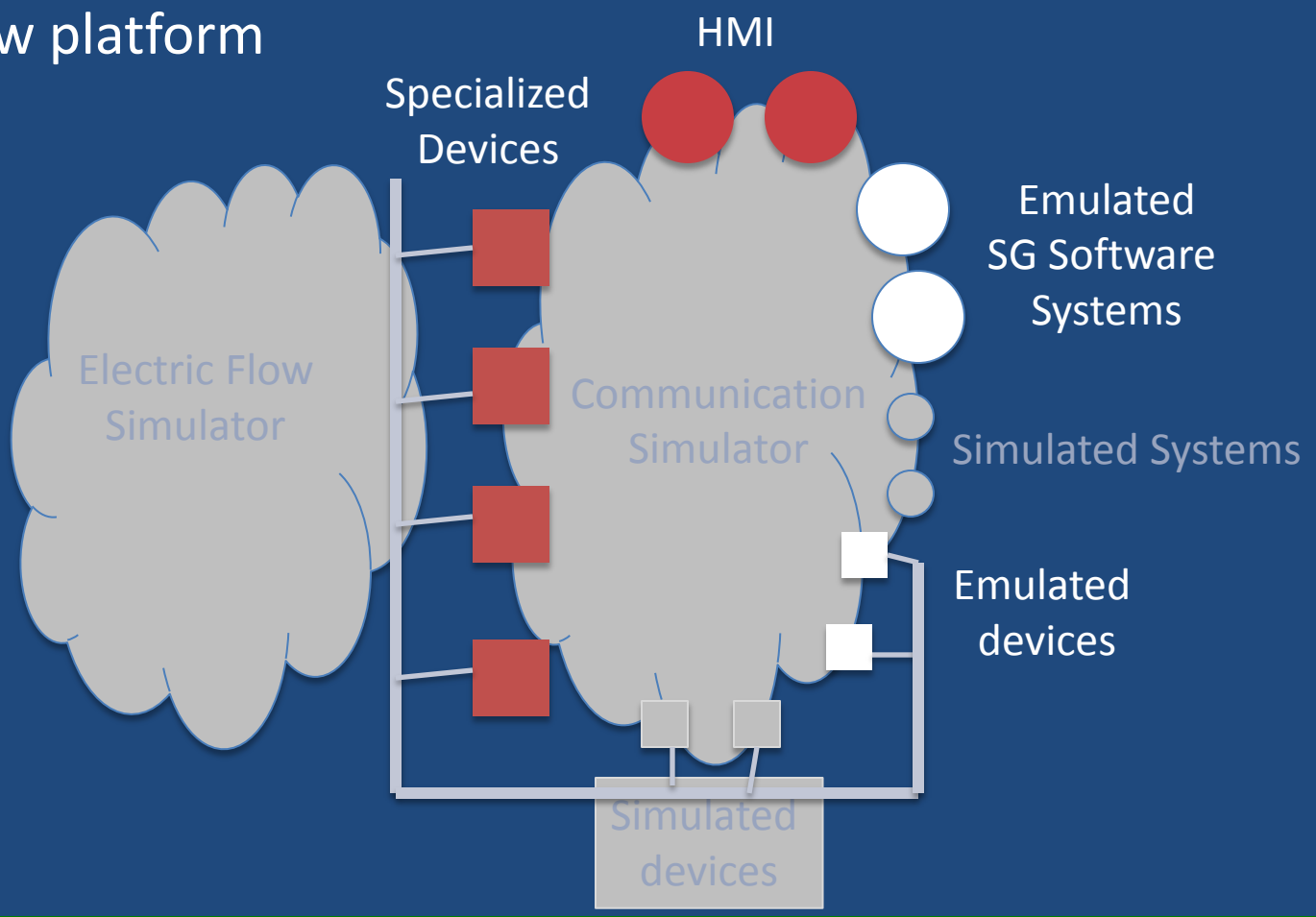
Simulation

- Uses abstraction to accelerate changes to model state
- May run faster or slower than real-time
- Low(er) memory needs
- Effort needed to develop models

Emulation vs Native Execution

Emulation runs software in "Virtual Machine"

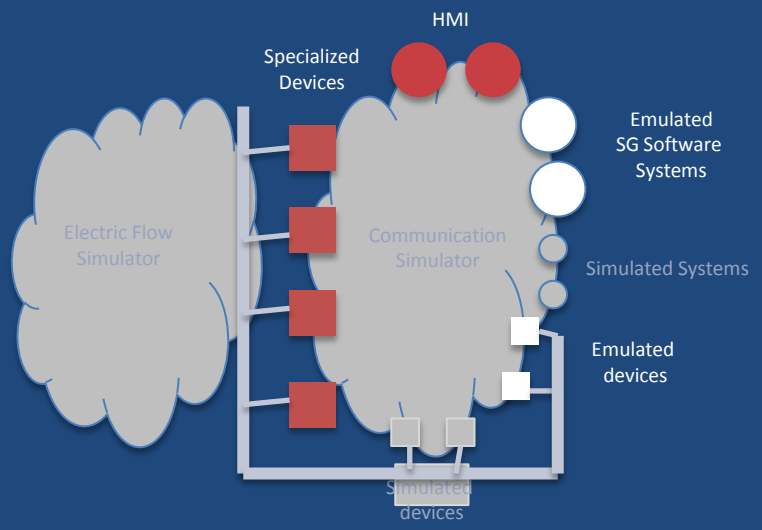
- Shares lower layer resources transparently
  - Even hw platform



Emulation vs Native Execution

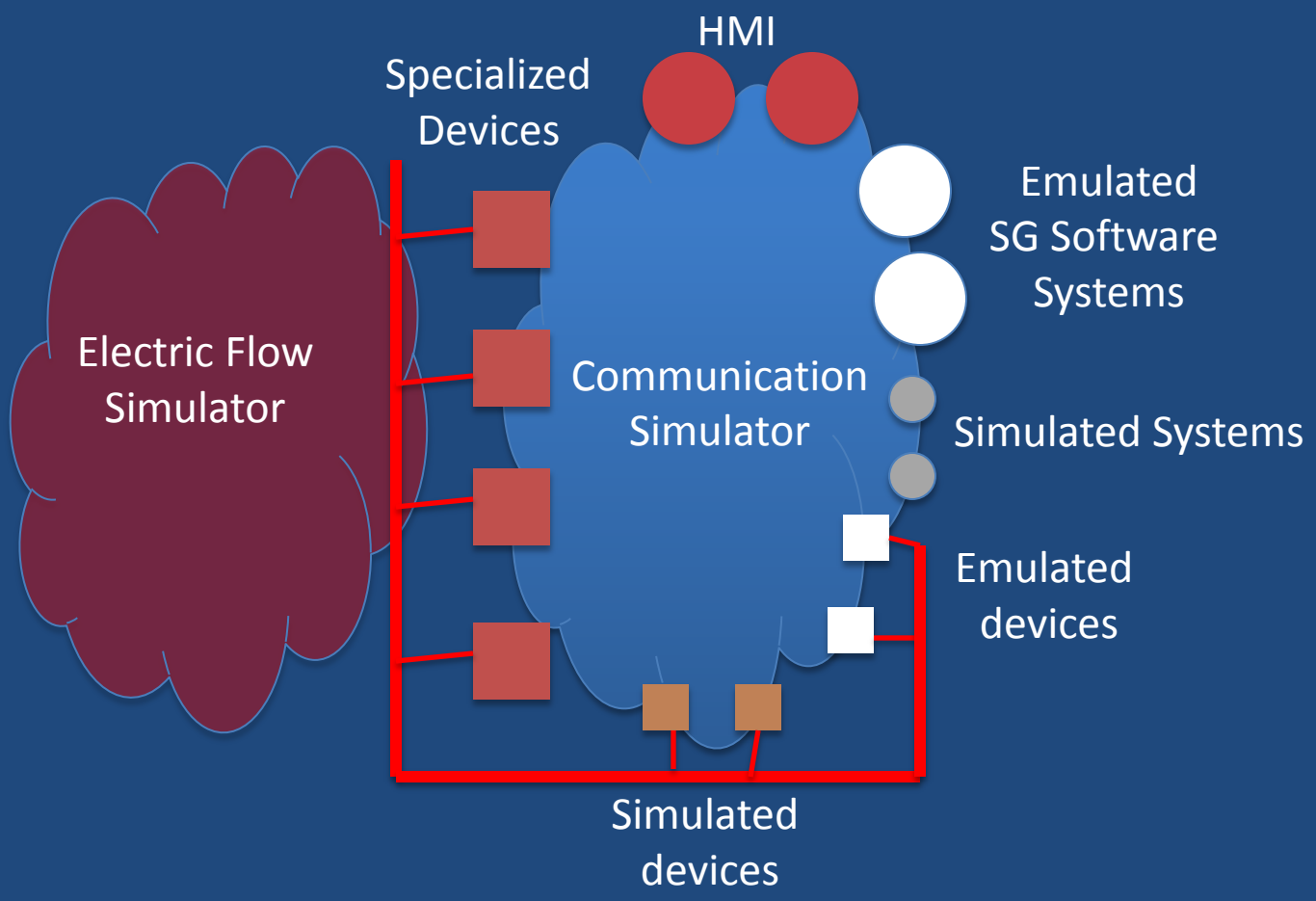
Emulation runs software in "Virtual Machine"

- Shares lower layer resources transparently
  - Even hw platform
- Critical differences
  - Native execution tied to wall-clock time
  - Interface to emulation is standard networking
  - Specialized hardware functionality (e.g. DSP) hard to emulate



Interfacing Electrical & Communication Simulations

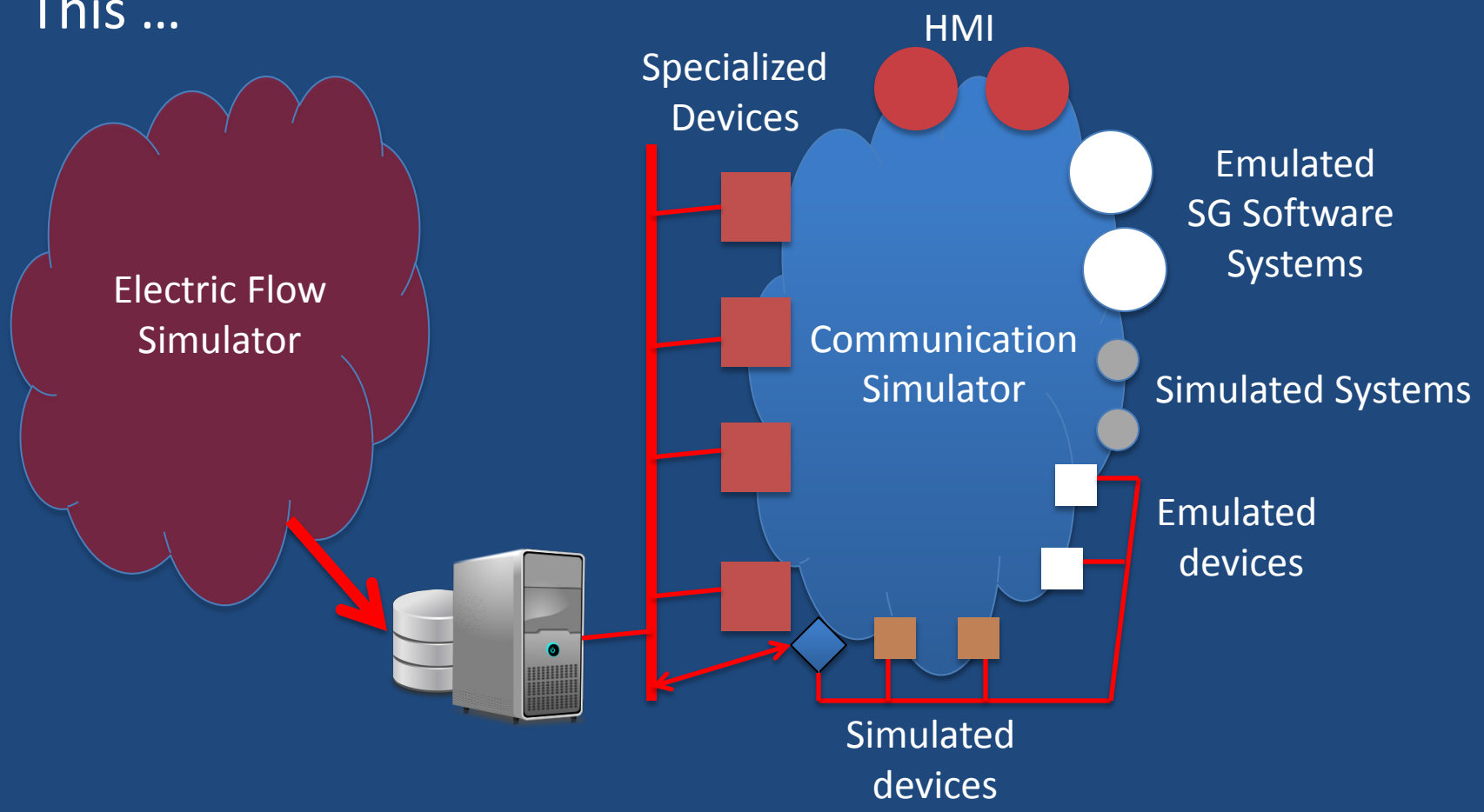
This …



Is really

Interfacing Electrical & Communication Simulations

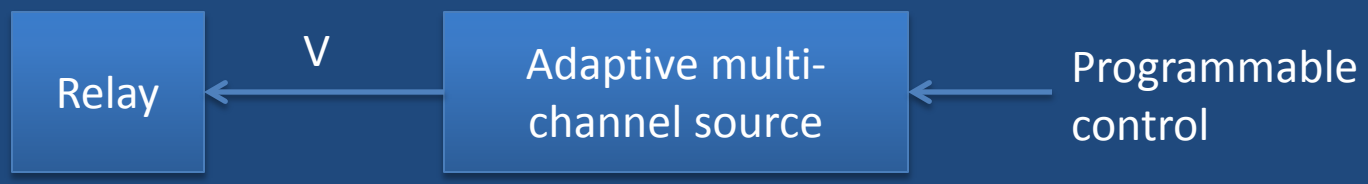
This …



Closed loop is harder…much harder…

Configurable integration of physical devices

How do you make a relay think it's in the field?

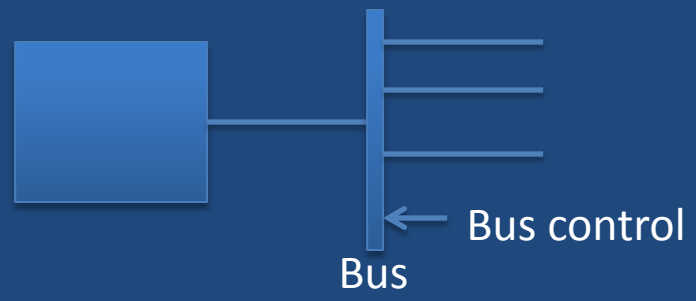


Relay built to respond to voltage as well as current

- Included by manufactorer for testing, we use it for simulation
- We program an AMS to represent electrical state from a simulator

Configurable integration of physical devices

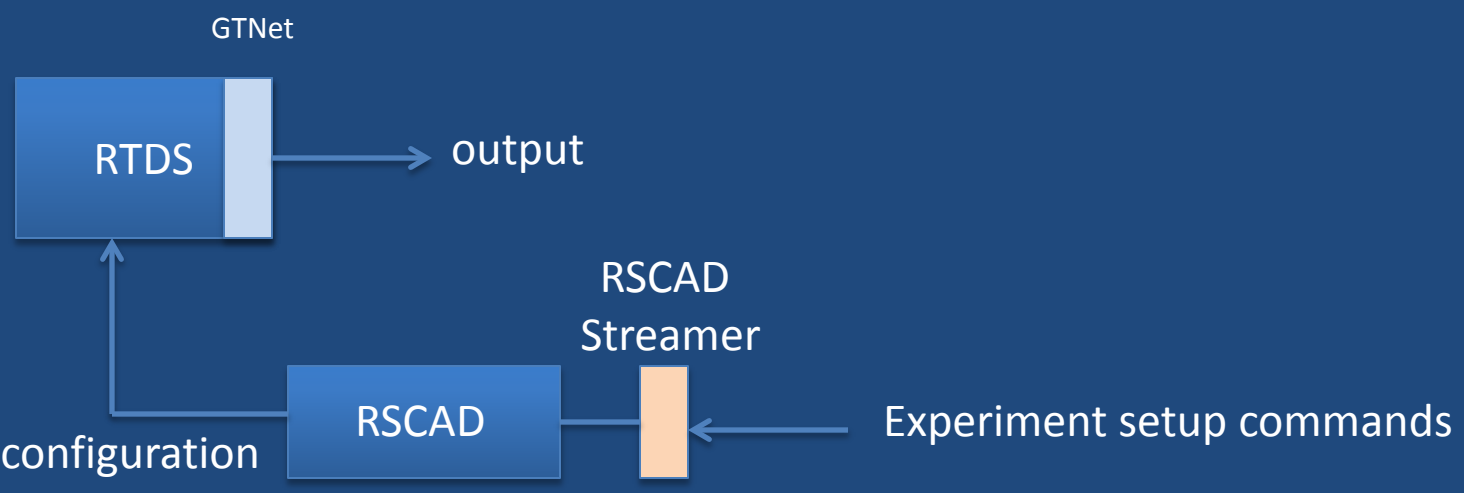
How do you multiplex inputs/outputs of an analog device?



Put onto a bus (analog multiplexor (/demultiplexor)), select input/output line through programmed bus control

Configurable integration of physical devices

How do you automatically configure an RTDS for a given experiment?

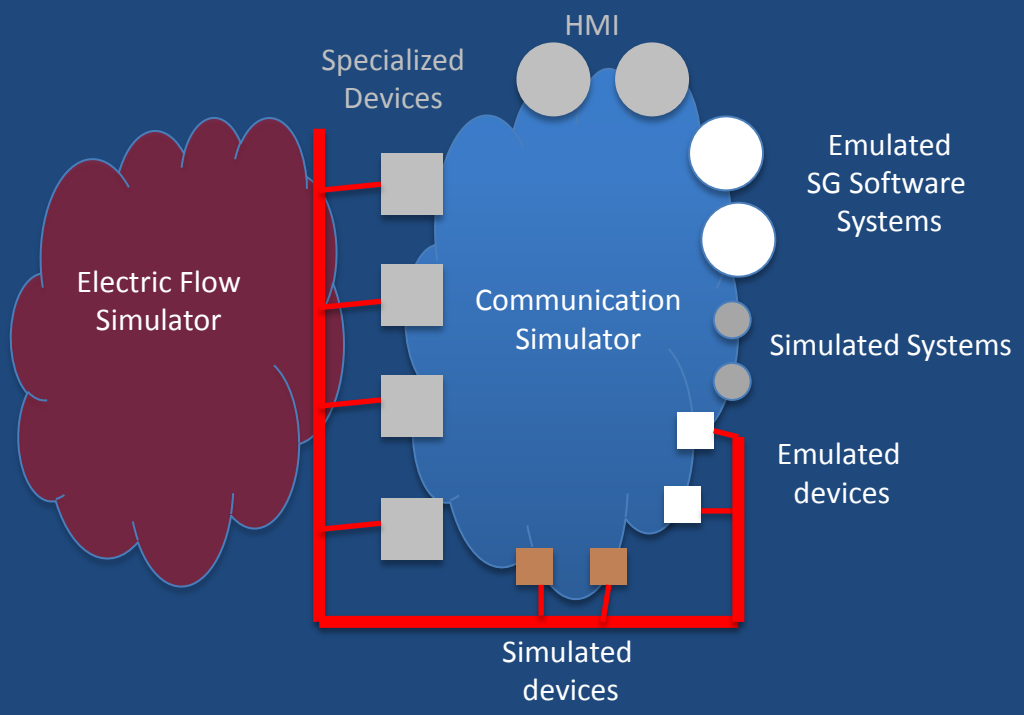


- Selection of configuration
- Load models
- Run-time interaction

Integrating Emulation & Simulation

Ordinary emulators embedded in real-time, BUT

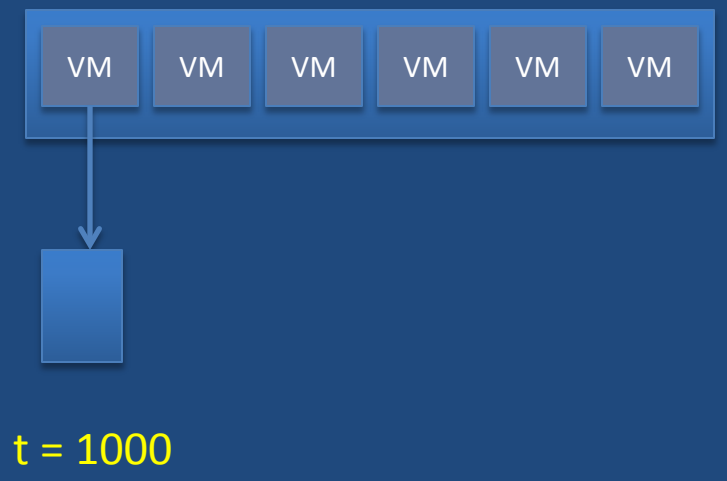
- Integration with virtual time causes issues
- TCIPG research effort shows how to embed a lightweight emulator in virtual time



Integrating Emulation & Simulation

Why is this needed? Imagine a set of synchronized emulated devices that in the real system all generate a message within the same small δ of time.

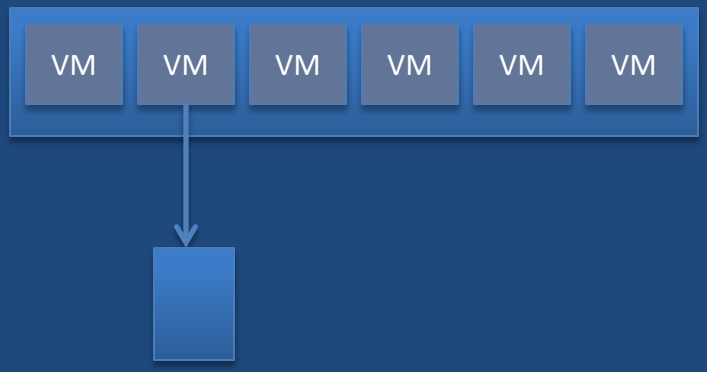
VMM separates generation in real-time by time-slice allocation



Integrating Emulation & Simulation

Why is this needed? Imagine a set of synchronized emulated devices that in the real system all generate a message within the same small δ of time.

VMM separates generation in real-time by time-slice allocation

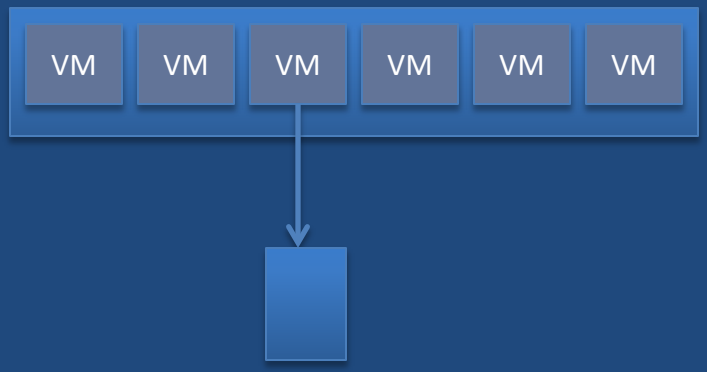


t = 2000

Integrating Emulation & Simulation

Why is this needed? Imagine a set of synchronized emulated devices that in the real system all generate a message within the same small δ of time.

VMM separates generation in real-time by time-slice allocation

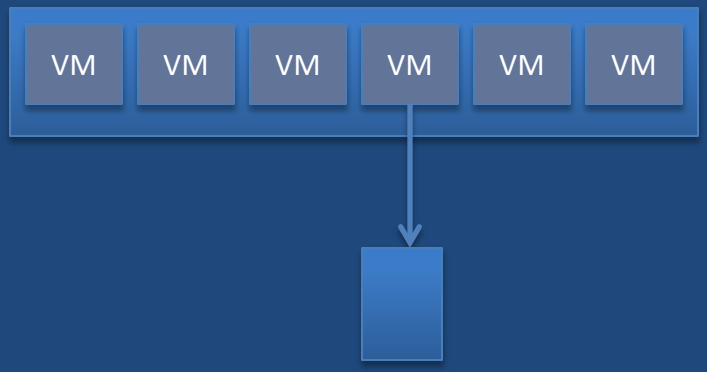


t = 3000

Integrating Emulation & Simulation

Why is this needed? Imagine a set of synchronized emulated devices that in the real system all generate a message within the same small δ of time.

VMM separates generation in real-time by time-slice allocation

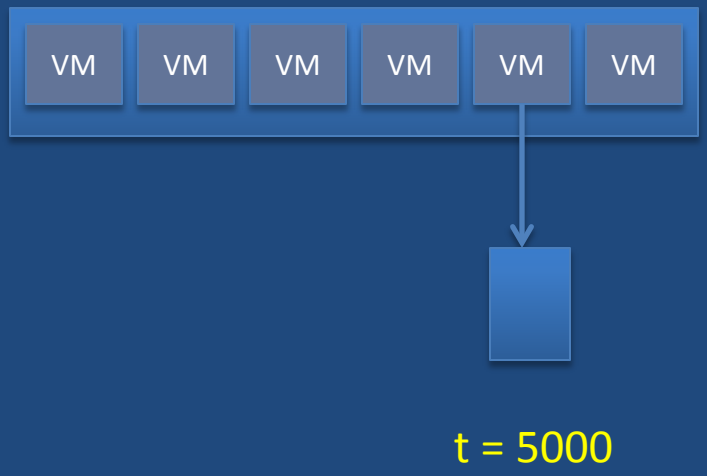


t = 4000

Integrating Emulation & Simulation

Why is this needed? Imagine a set of synchronized emulated devices that in the real system all generate a message within the same small δ of time.

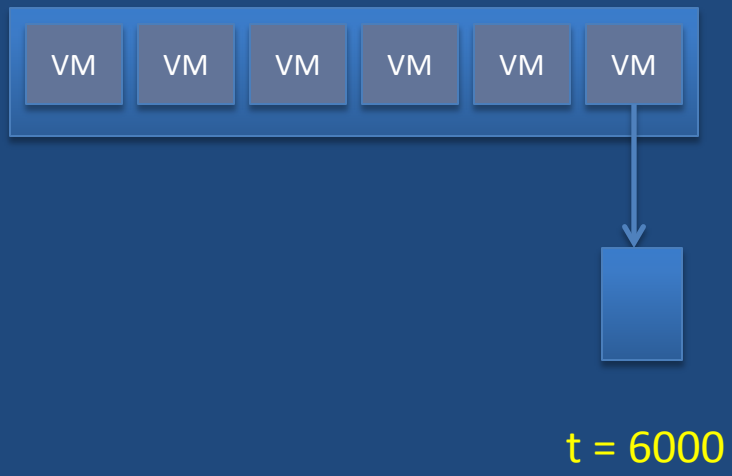
VMM separates generation in real-time by time-slice allocation



Integrating Emulation & Simulation

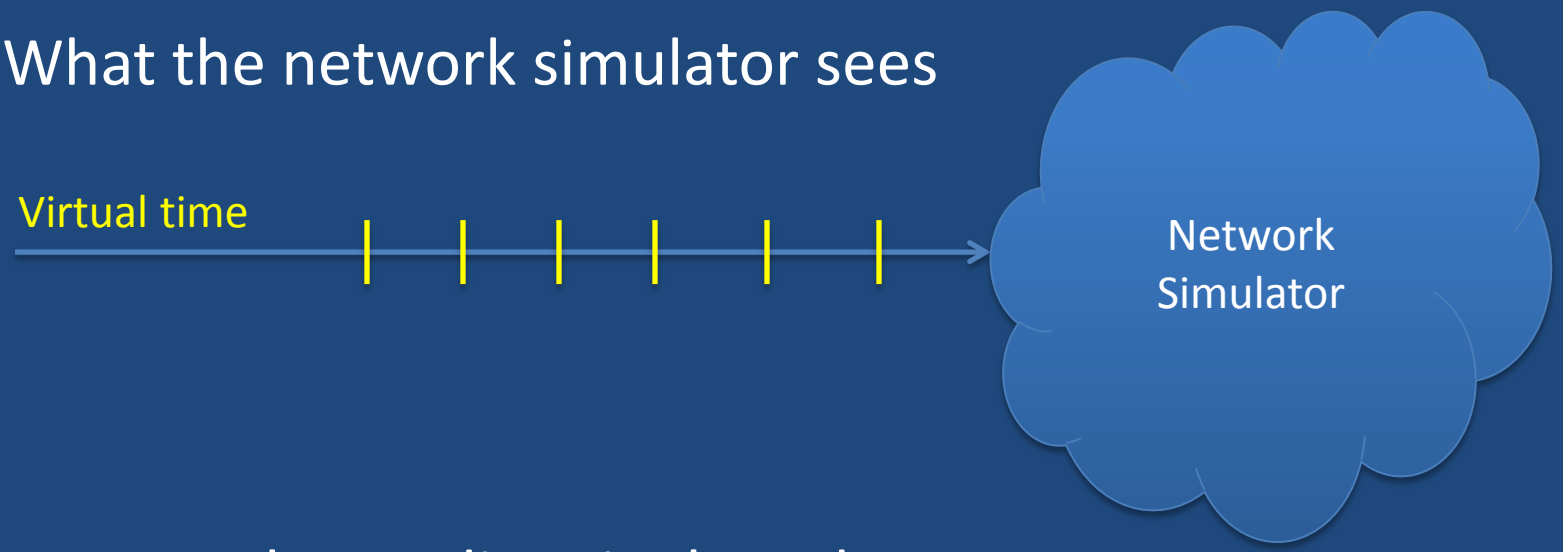
Why is this needed? Imagine a set of synchronized emulated devices that in the real system all generate a message within the same small δ of time.

VMM separates generation in real-time by time-slice allocation



Integrating Emulation & Simulation

What the network simulator sees



Suppose the medium is shared access…

Suppose the packets all join the same queue….

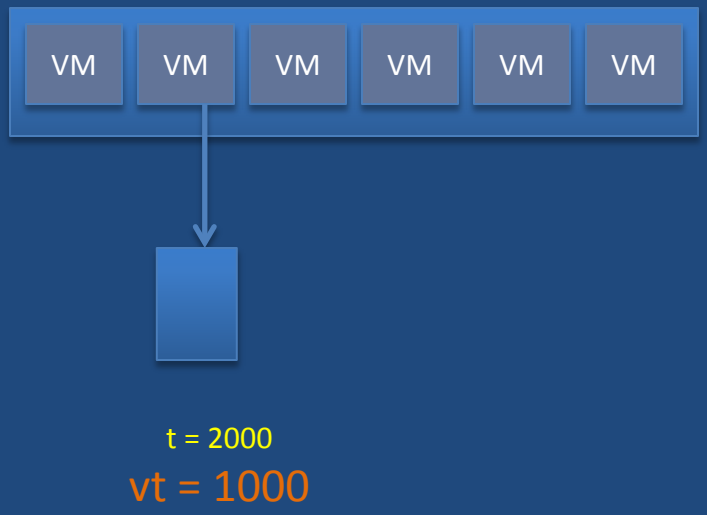
The emulator's serialization of the time presents the wrong input behavior to the simulator

Integrating Emulation & Simulation

When the emulator is embedded in virtual time, time stamps on messages are closer to reality

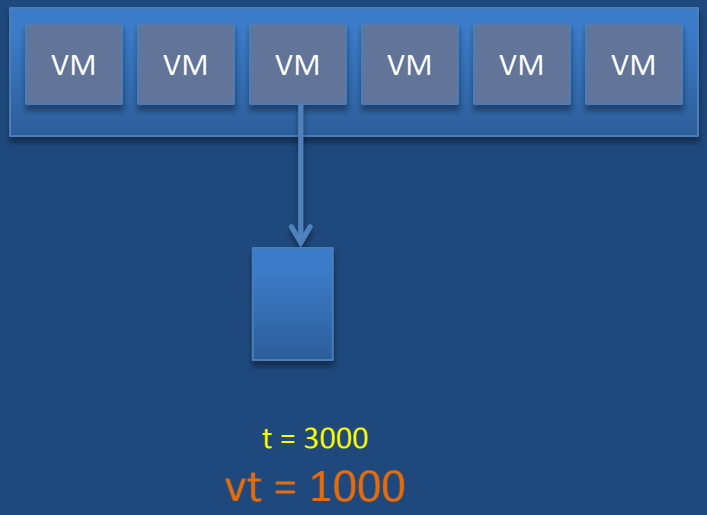
Integrating Emulation & Simulation

When the emulator is embedded in virtual time, time stamps on messages are closer to reality



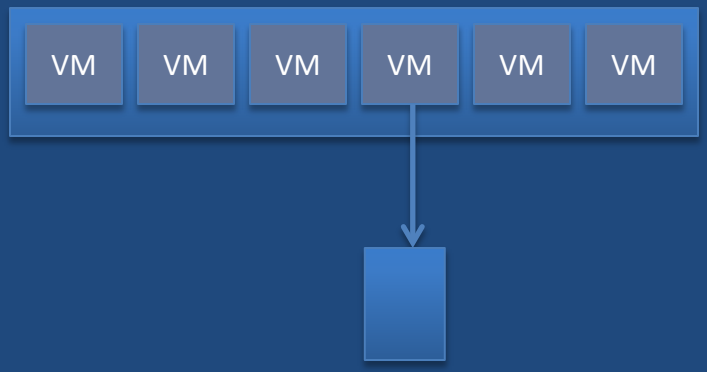
Integrating Emulation & Simulation

When the emulator is embedded in virtual time, time stamps on messages are closer to reality



Integrating Emulation & Simulation

When the emulator is embedded in virtual time, time stamps on messages are closer to reality

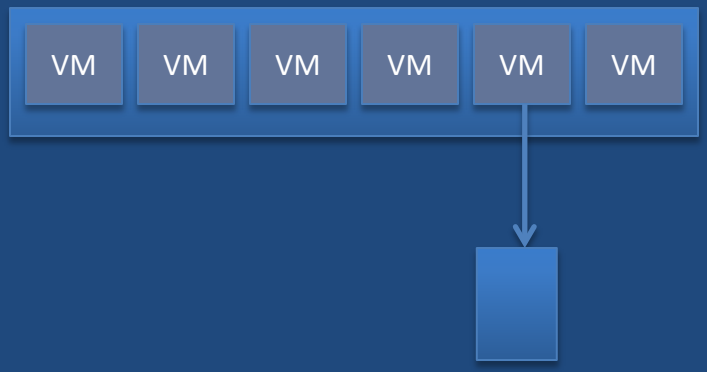


t = 4000

vt = 1000

Integrating Emulation & Simulation

When the emulator is embedded in virtual time, time stamps on messages are closer to reality

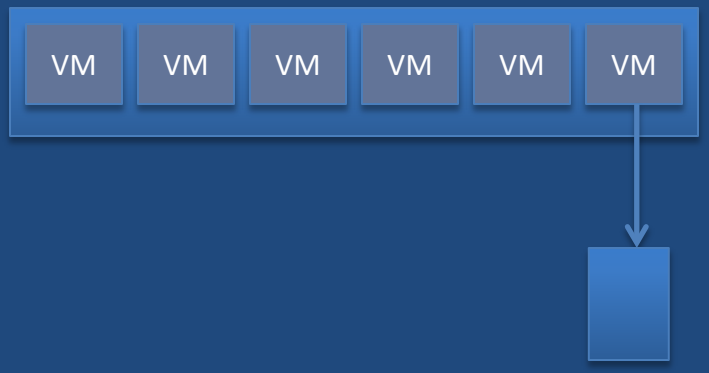


t = 5000

vt = 1000

Integrating Emulation & Simulation

When the emulator is embedded in virtual time, time stamps on messages are closer to reality



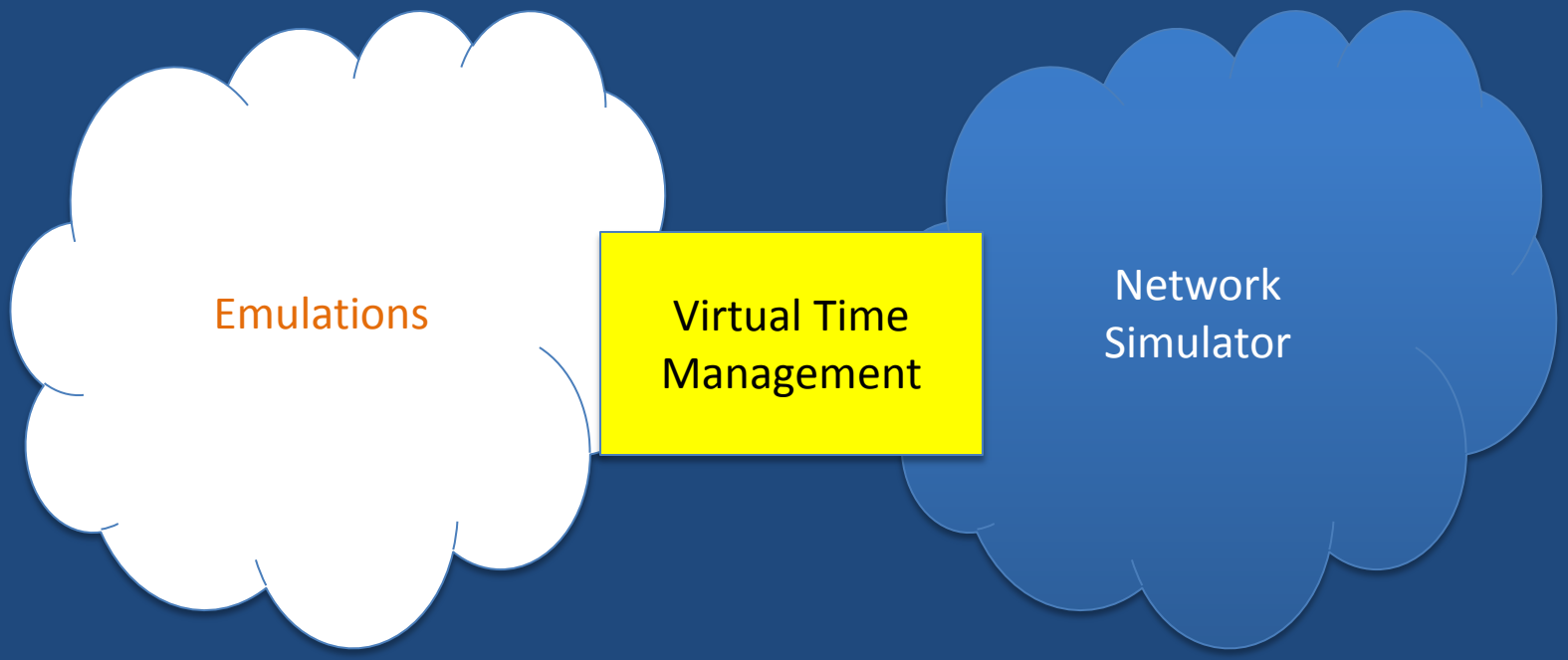
t = 6000

vt = 1000

Integrating Emulation & Simulation

Research problems related to interactions and management of virtual time between emulations and simulation

- Inherent errors due to VM control
- Exploitation of parallelism



Network Simulation

Smart grid systems have

- Wired networks and specialized protocols, e.g.,
  - 61850, IP, TCIP, DNP3, DLMS/COSEM
  - Routing protocols
- Wireless networks
  - Requires radio channel model
  - Protocols such as c12.22, Zigbee, 802.11
  - Mesh architecture

A ***lot*** of work involved in developing a library of models

Network Simulation

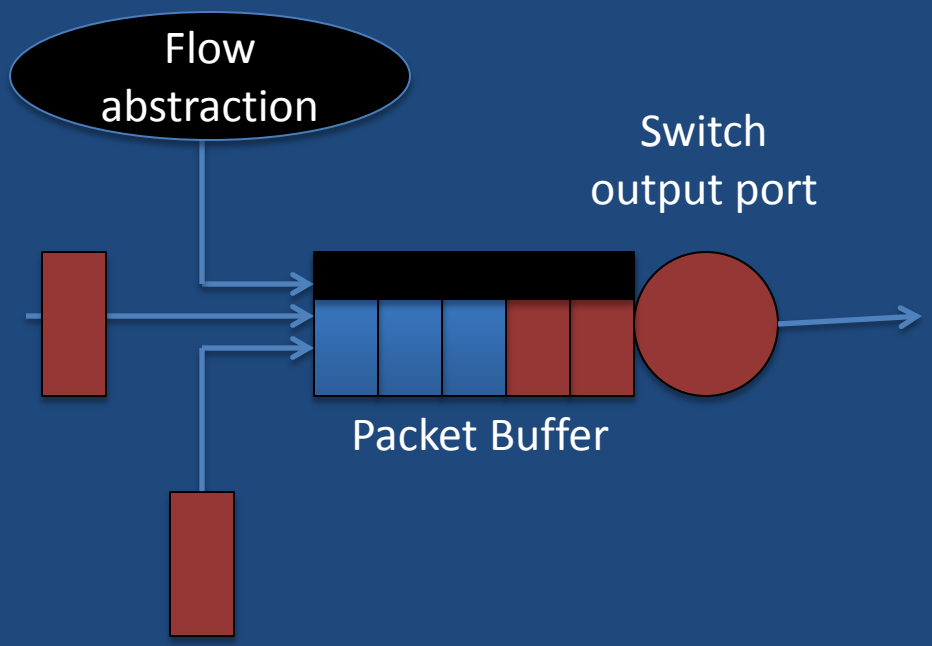
Research problems for modeling Smart Grid networks

- Ensemble MUST at times run in real-time
  - means the emulation & simulation have to "keep up"

- Wired networks – reduce computational cost
  - Structured traffic patterns create possibilities for compact and efficiently executed background traffic
    - Low cost background traffic, mixed with detailed foreground traffic
  - Co-simulate concurrent traffic, mixed abstractions

Network Simulation

Co-simulate concurrent traffic, mixed abstractions



Switch model --- combined discrete & continuous traffic
Flow abstraction --- needs to carry variance

Network Simulation

Research problems for modeling Smart Grid networks

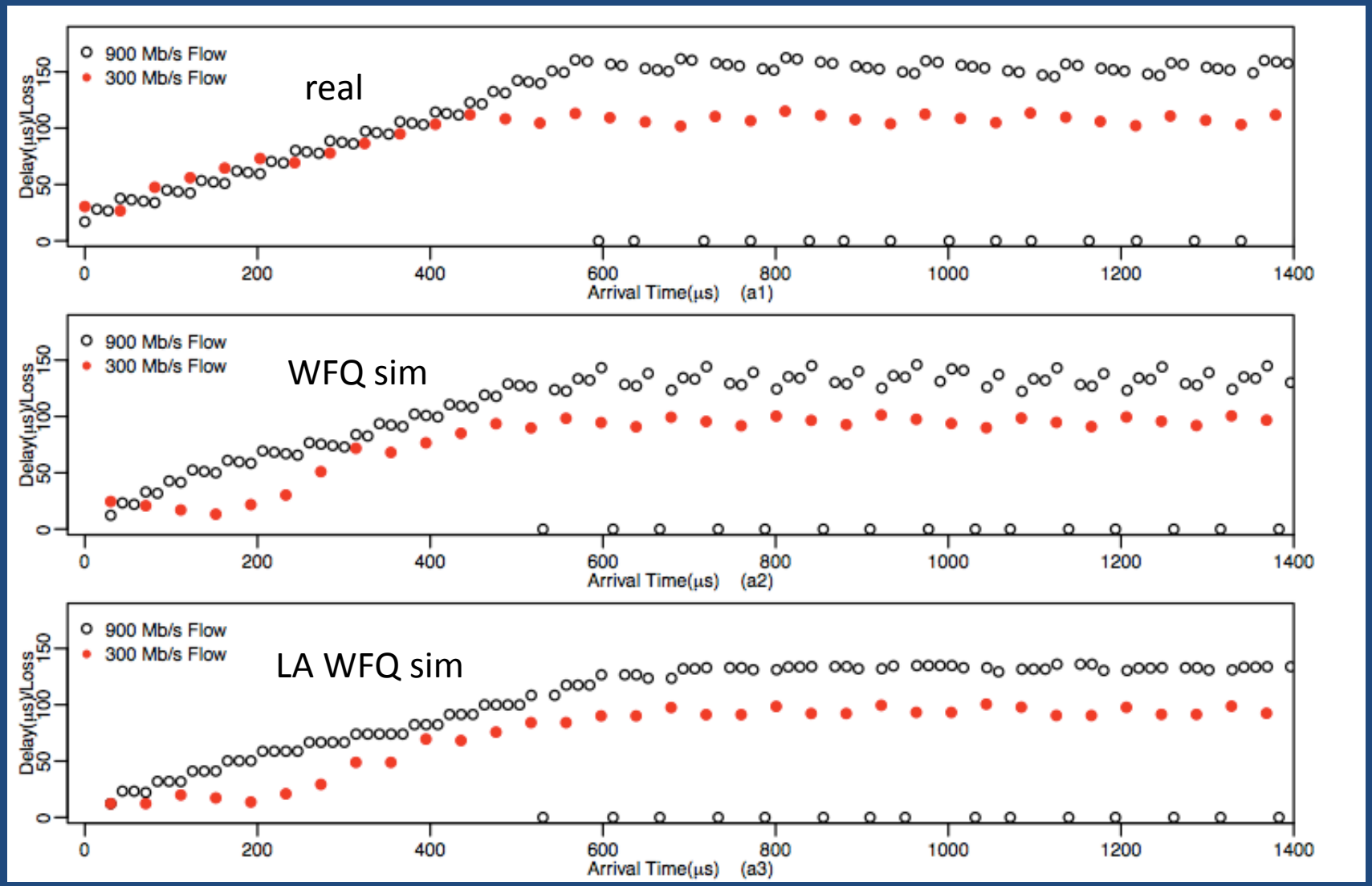
- Wired networks – reduce computational cost at switch

OBSERVATION --- time-scale difference between apps and switch suggests *exact* latency not so key as *average* latency

BUT a packet loss under TCP impacts app behavior

We developed latency-approximate scheduling for weighted fair queuing discipline ---- reduced cost as small loss of fidelity

Latency Approximate Scheduling

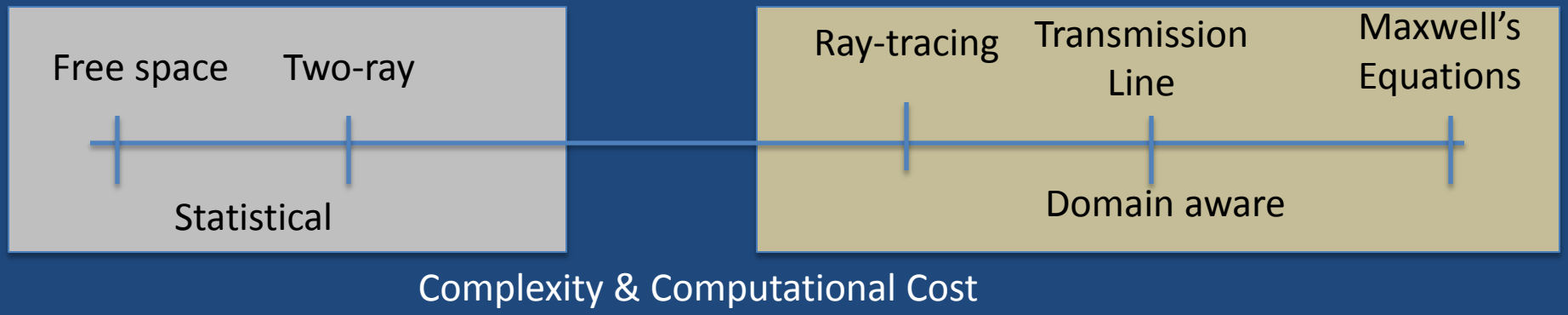


Network Simulation

Research problems for modeling Smart Grid networks

- Wireless networks – computationally efficient model of physical layer
  - Complicated interference geometries in substation
  - Behavior depends on quality of signal

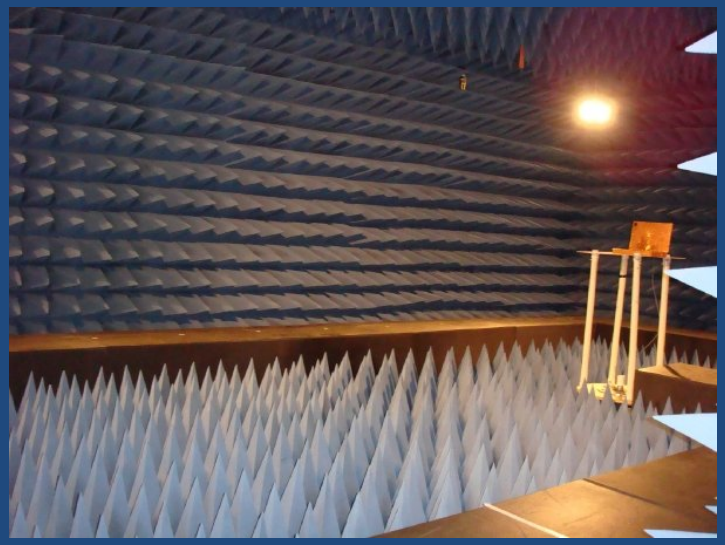
Range of models that vary in computational cost and fidelity



Network Simulation

Research problems for modeling Smart Grid networks

- Wireless networks – computationally efficient model of physical layer
- Studies in an anechoic chamber suggest



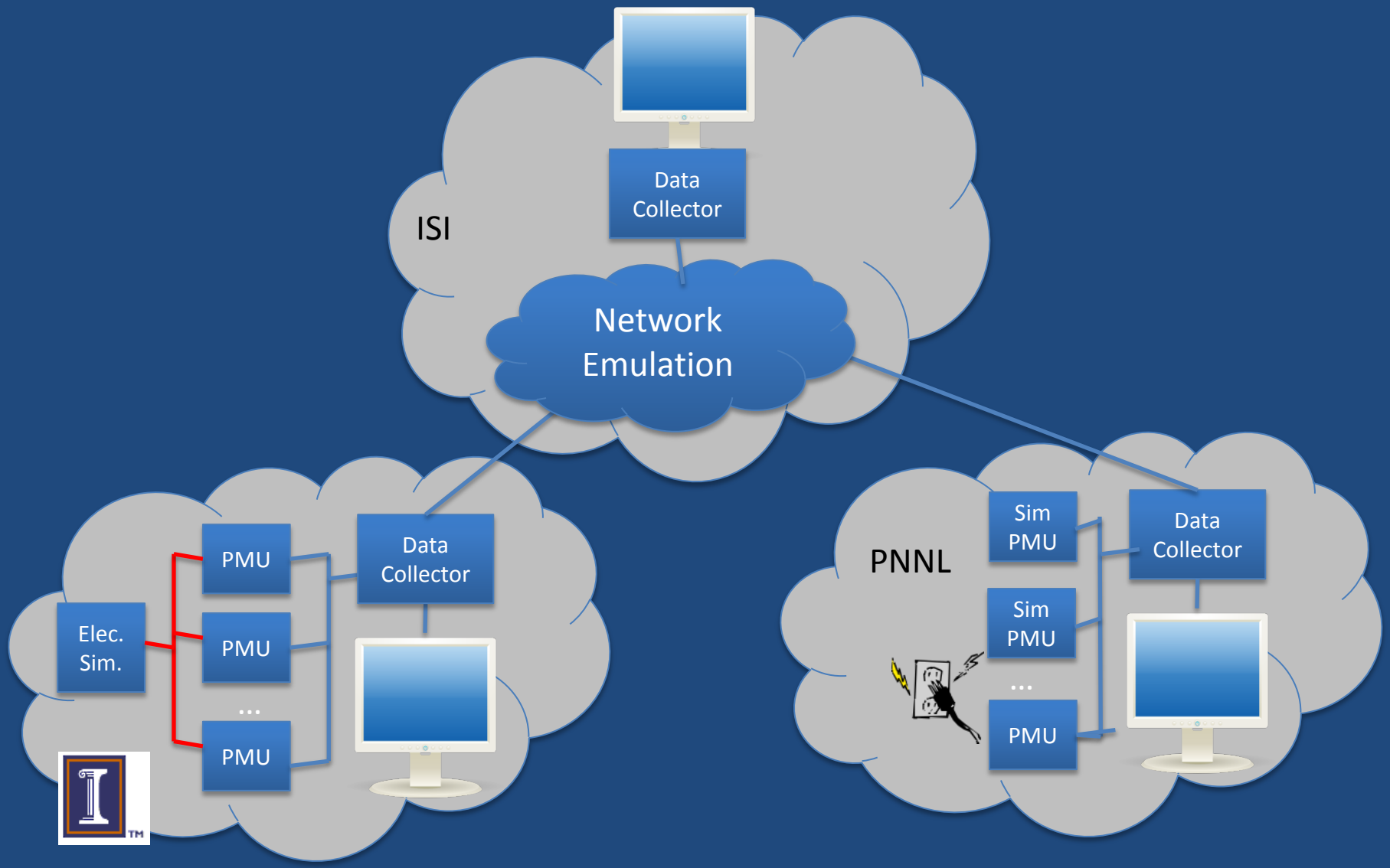
  - Ray tracing may needs phase information
  - Uncertainty in model parameters

Case Study : Wide Area Situational Awareness

DEFT Consortium (DETER Enabled Federated Test-bed) demo

- Federates test-beds at Illinois, ISI, PNNL
- Demonstration of how situational awareness is maintained in networked regional control

Case Study : Wide Area Situational Awareness



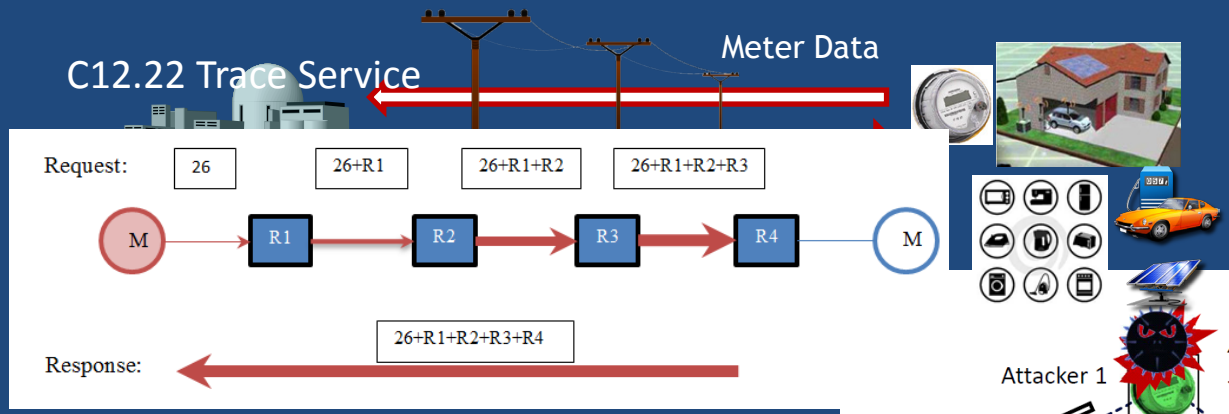
Case Study

Impact of DDoS attack using c12.22 TRACE service

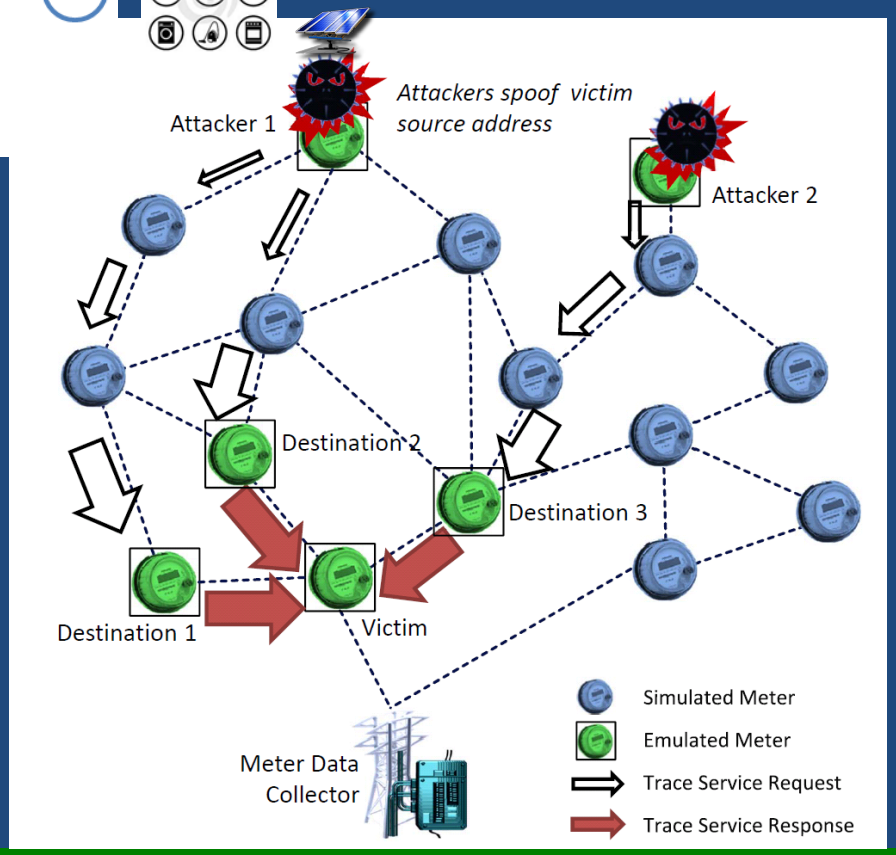
Mixed emulation + simulation

- C12.22 protocol stacks running in emulation
- Many routers and meters simulated
- Wireless network simulated
  - Zigbee protocol

DDoS Attack Using C12.22 Trace Service in AMI

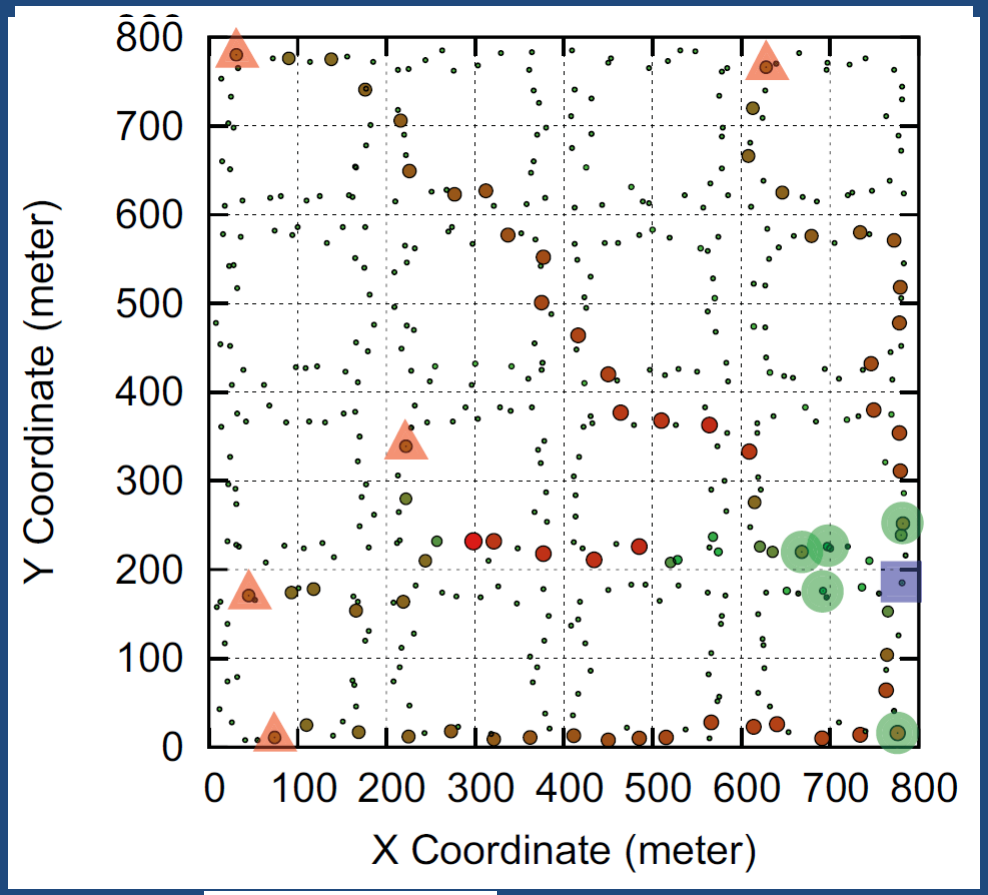


17M Smart Meters in AMI projects



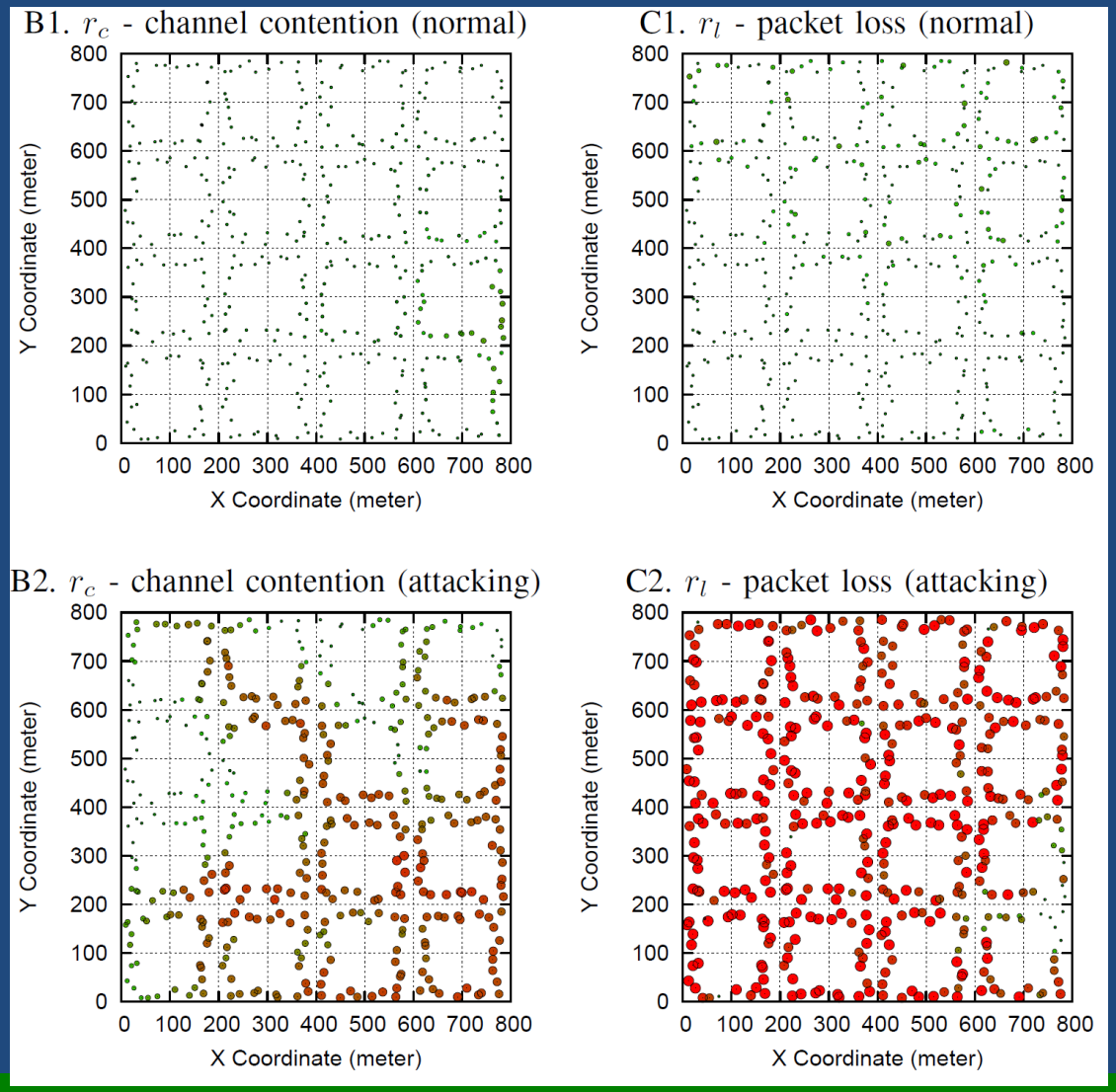
- Amplification
  - Increased volume of traffic
- Reflection
  - Spoofed source address

Attacking Experiment



- 4x4 blocks, 448 meters
- 5 attackers
- Victim: the single egress point (meter gateway)
- ZigBee wireless network, 1 Mb/s bandwidth
- Normal traffic: 100-byte packet per 10 second
- Attacking traffic: 200 times faster, 15-30 hops

Experimental Results



Summary

TCIPG is building the capability to evaluate complex Smart Grid systems

- Simulation and emulation are at the heart of it
- Good research problems follow from characteristics of Smart Grid systems