



Software Defined Networking for Smart Grid Resilience

Hui Lin¹, Xinshu Dong², Rui Tan^{2,3}, Ravishankar K. Iyer^{1,2}, Zbigniew Kalbarczyk^{1,2}

¹ Coordinated Science Laboratory, University of Illinois at Urbana Champaign, IL, USA;

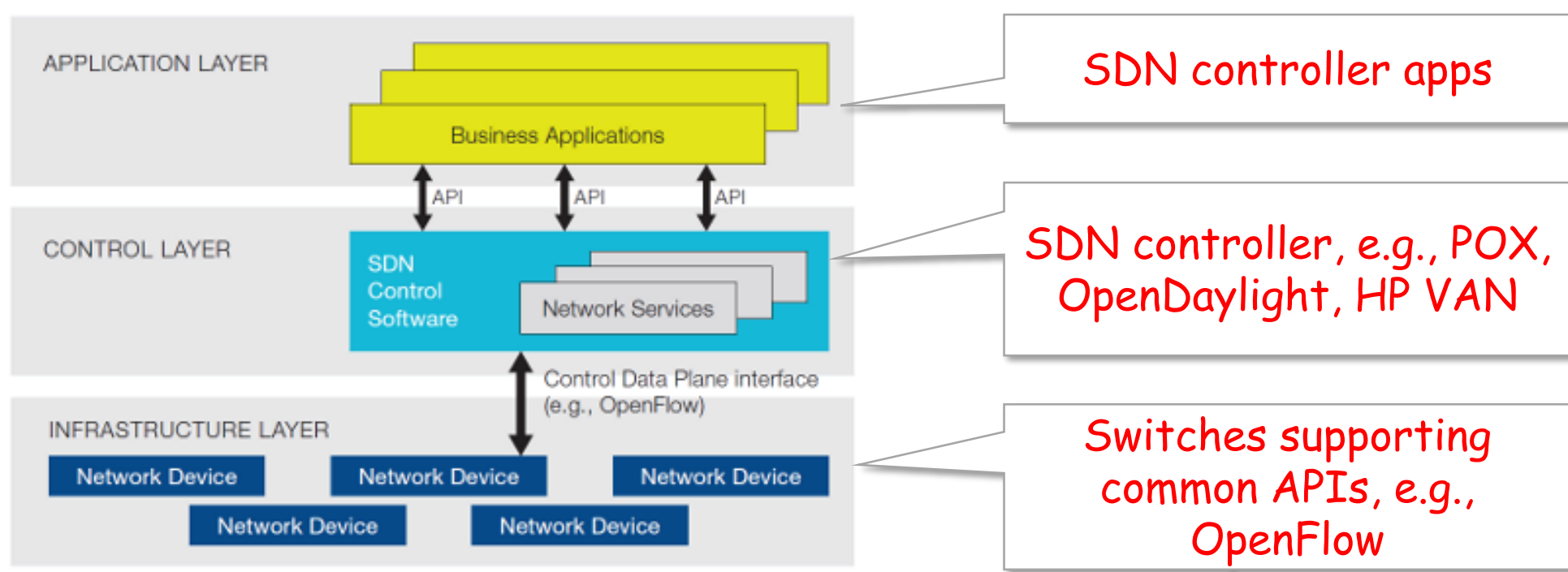
² Advanced Digital Sciences Center, Illinois at Singapore;

³ School of Computer Science and Engineering, Nanyang Technological University, Singapore

Software Defined Networking

Software Defined Networking (SDN)

- Unprecedented flexibility, visibility, and QoS compared to “vertically-integrated black boxes” of old networking devices
- Enables various applications, e.g., optimize QoS, enhance network resilience, etc.



* Chart courtesy of <http://twings.com/networkcomputing/2012/5/sdn-arch.png>

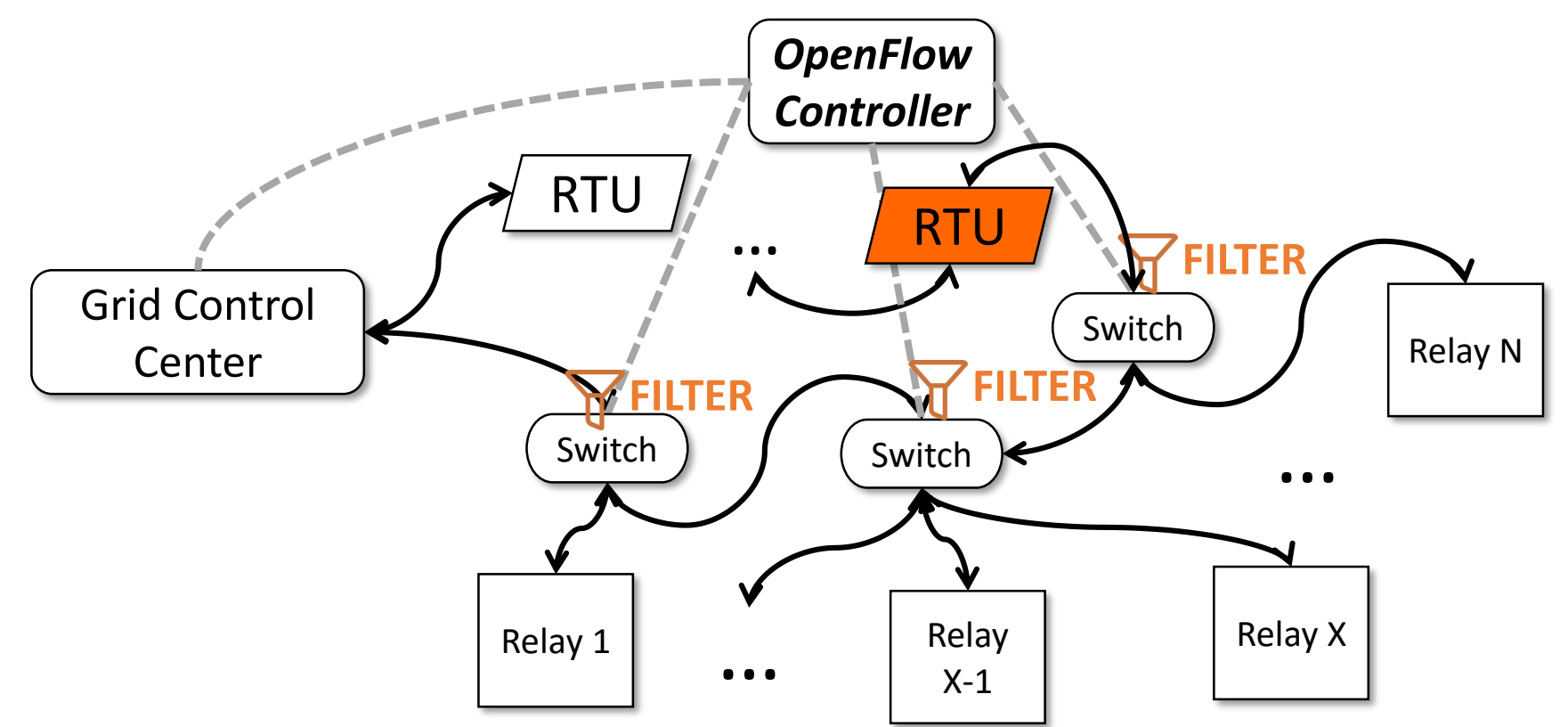
Applying SDN to strengthen smart grid operations

- Smart grid: critical infrastructure leveraging information and communications technology
- Initial industrial effort towards SDN-enabled smart grid
 - SEL-2740S switch

SDN for the Grid: Opportunities & Risks

SDN for greater resilience in smart grid [1]

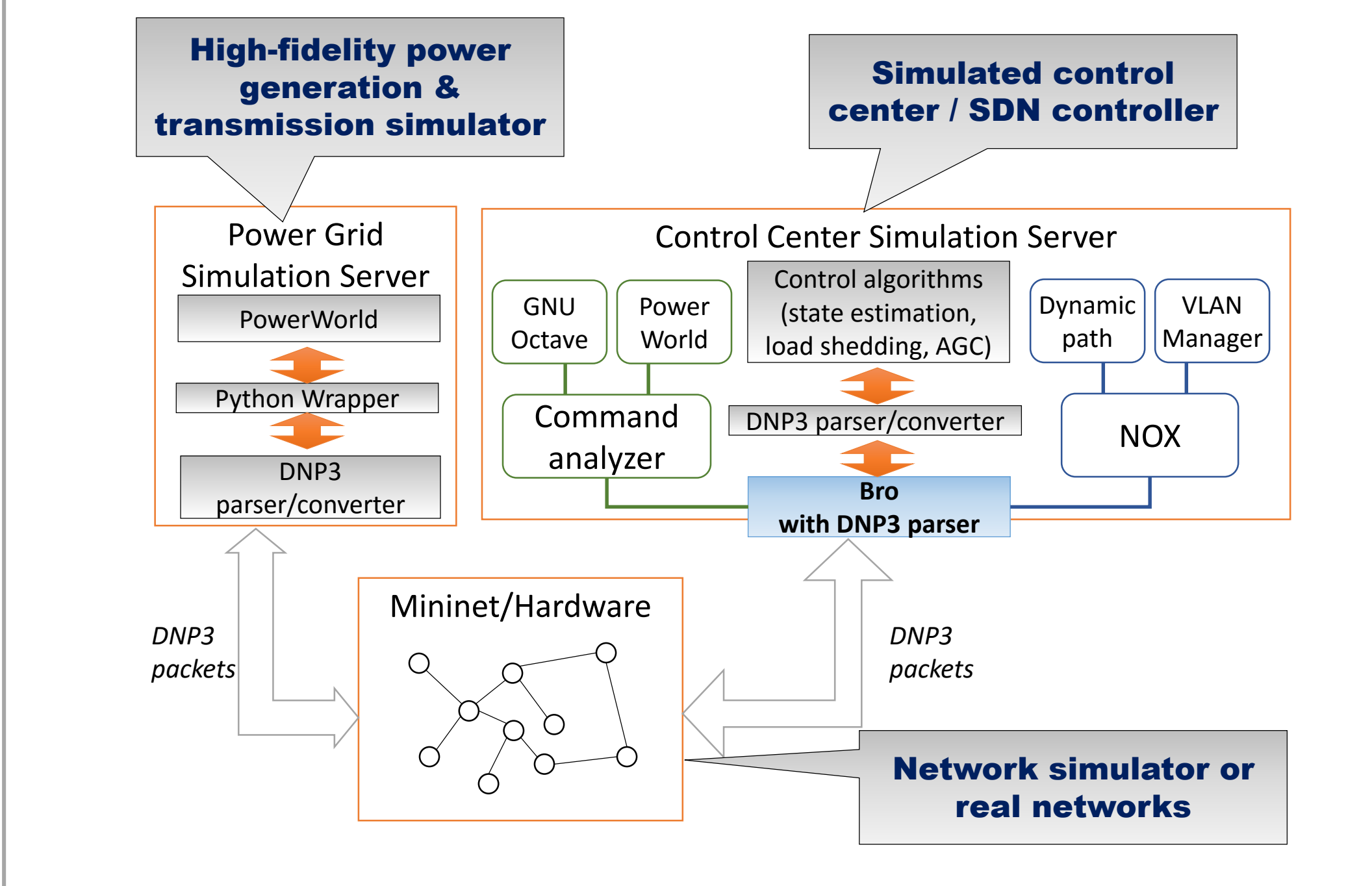
- Example 1: detecting malicious command forwarding behaviors
- Example 2: filtering out flooded responses from control and field devices caused by spoofed requests



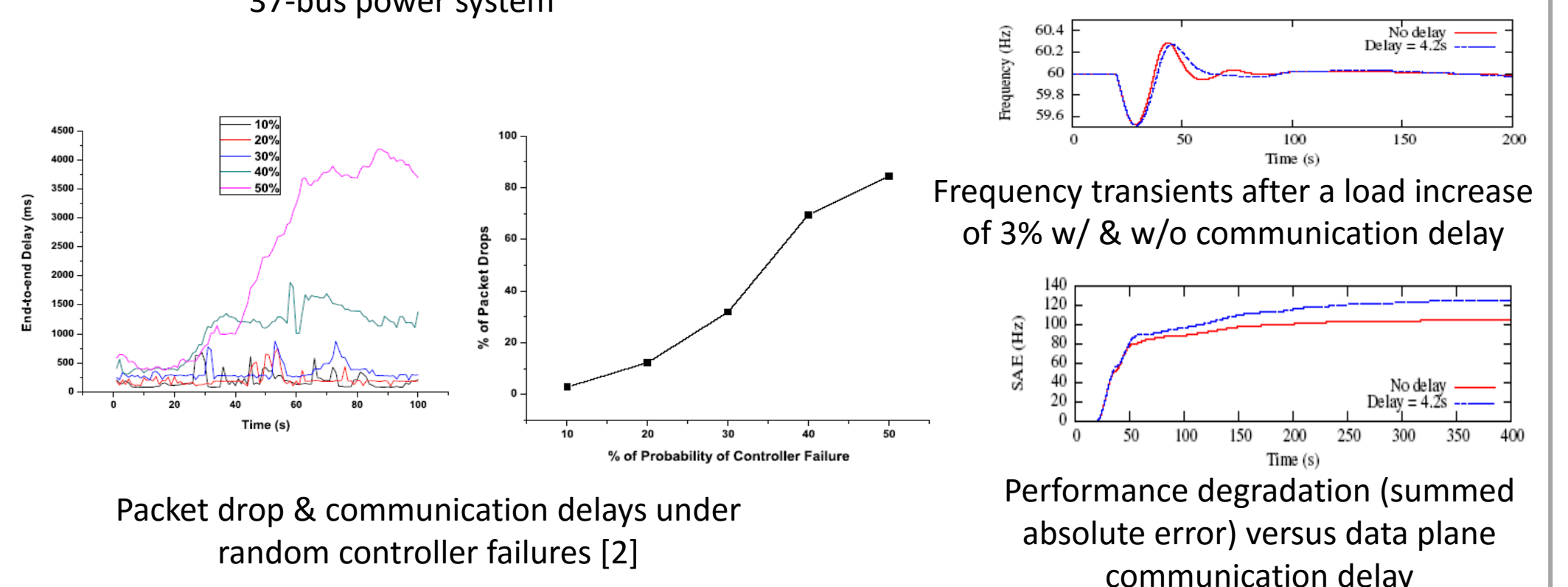
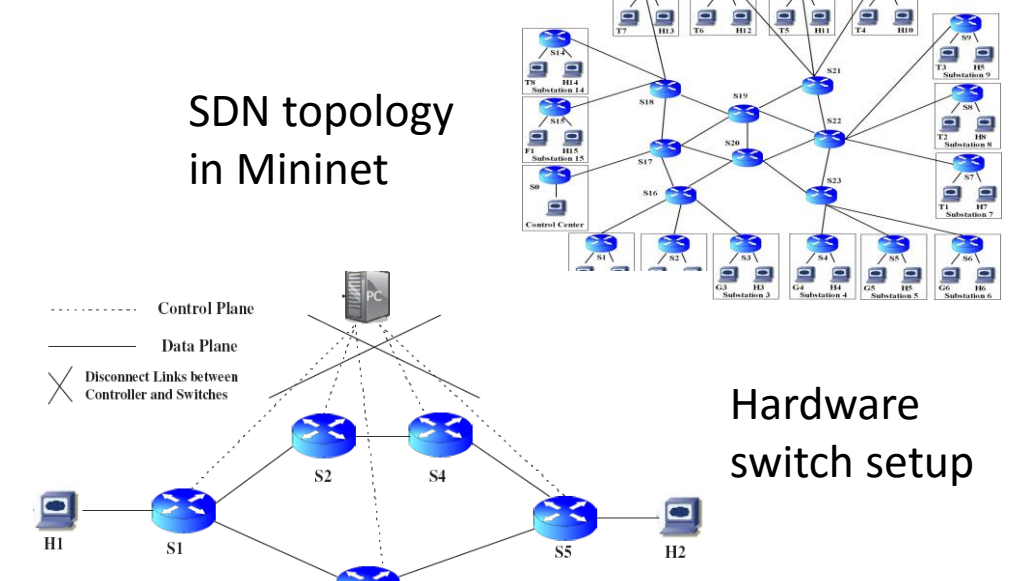
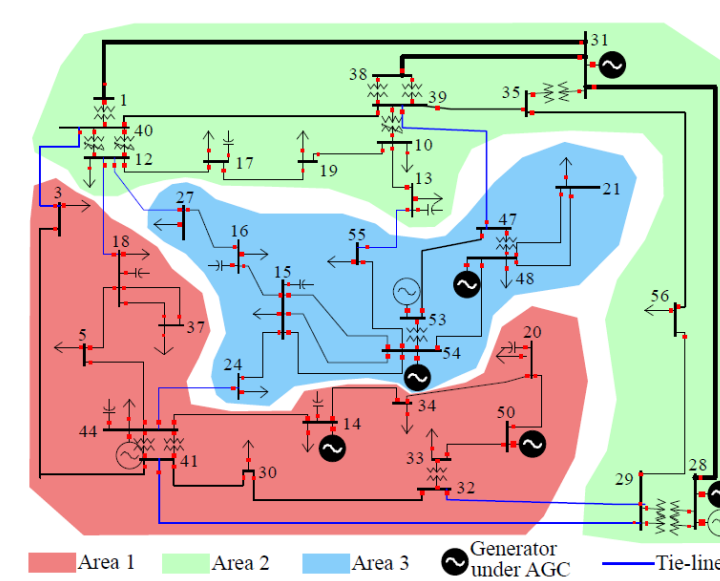
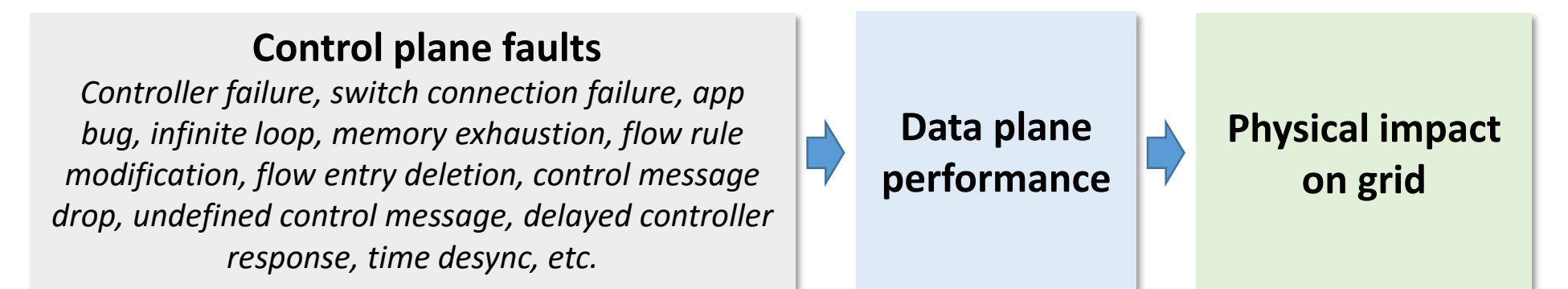
Nevertheless, SDN may also bring in additional risks to smart grid

- Example 1: “darknets” created by SDN rootkits
- Example 2: denial-of-service attacks from weakness with the SDN controller

Cyber-Physical Simulation & Testbed



Fault Injection on SDN-Enabled Grid



SDN with Synchronized Clock

[Ongoing work] Investigating the practical benefits of having time-synchronized network updates

- Preventing varying degrees of packet loss
- Eliminating ambiguous states when access control policy is integrated into SDN switches
- Requiring less changes compared to packet versioning

References

- [1] Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges. Xinshu Dong, Hui Lin, Rui Tan, Ravishankar K. Iyer, Zbigniew Kalbarczyk. In Proceedings of The 1st Cyber-Physical System Security Workshop (CPSS), April 14-17, 2015, Singapore.
- [2] A Simulation Study on Smart Grid Resilience under Software-Defined Networking Controller Failures. Uttam Ghosh, Xinshu Dong, Rui Tan, Zbigniew Kalbarczyk, David K. Y. Yau, Ravishankar K. Iyer. The 2nd Cyber-Physical System Security Workshop (CPSS 2016), co-located with AsiaCSS, May 30, 2016, Xi'an, China.

This work was supported by the research grant for the Human-Centered Cyber-physical Systems Programme at the Advanced Digital Sciences Center from Singapore's Agency for Science, Technology and Research (A*STAR). Zbigniew Kalbarczyk and Ravishankar Iyer are supported in part by the grant Cyber Resilient Energy Delivery Consortium (CREDC) DOE DE-0E0000780 (NETL) from Department of Energy, USA, and another grant Semantic Security Monitoring for Industrial Control Systems, NSF CNS 13-14891, from National Science Foundation, USA.