Cyber Security Standards for Critical Energy Infrastructures

Session 2, February/2/2018

Wilhelm Wimmreuter
InCharge Systems, Inc.
February 2018

Cyber Security Standards in Critical Energy Infrastructure

- **Overcome the Race between different Standards**

  Can standards bodies overcome the different goals of centralised-legacy and distributed-network standards?

Standard Organizations on the Move:

State Regulators:	FERC, FTC, ...	deregulated markets
Standard Bodies:	ITU, IETF, ...	adopted regulation & new technology.
Industry Forums:	ATIS, ...	try to fill the missing link(s)

David Isenberg's **"The Rise of the Stupid Network"** 1997, is reality and must be considered by all business operations using the Cyber-Space.

Challenges

- Transition from Human-Control through Closed-Central-Control towards Open-Distributed-Network-Control and Operation
- From Trust-by-Wire to Trust-by-Authentication
- Standards, Policy, Production and Operations have different goals and likely stick to their legacy practises

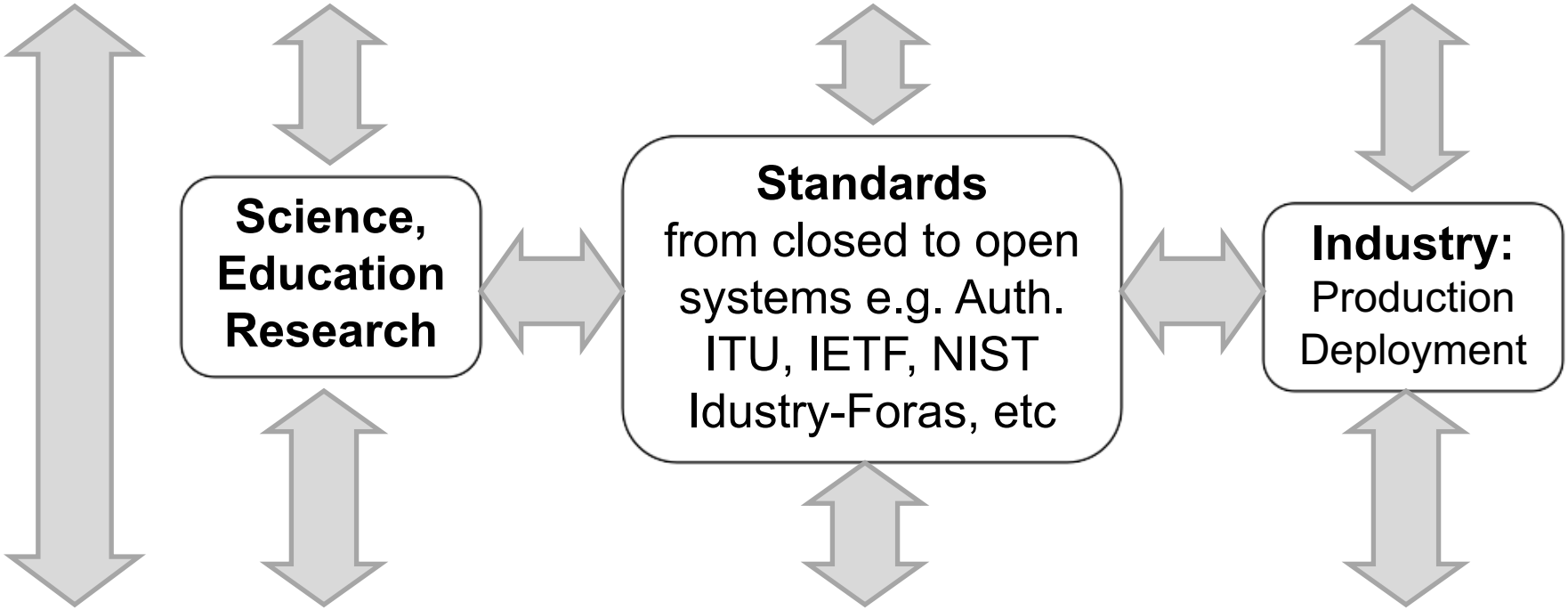
Opportunities

- Overcome the difference between centralised, closed and distributed open network standards
- Network-independent authentication migrates life-time-responsibility and cost to the principal - user/employee
- Increase Security by simplifying policies and operations e.g.: Re-use secure credentials of principals PKI tokens

Stakeholders their Interactions / Influences for the Transition of Standards

State Regulators

- Federal Energy Regulatory Commissions, Government, etc.
- They Deregulated but execution & policies are still on the move.



Critical Energy Infrastructure Providers

Energy, Water, Transport, Communication, etc.