Cyber-security for Energy Systems

Marija Ilic

MIT IDSS, Visiting Professor* ilic@mit.edu

Governor' Summit on Energy &Infrastructure, Washington,DC 02/23/17

*CMU Professor milic@andrew.cmu.edu; Director EESG http://www.eesg.ece.cmu.edu/ (on leave);

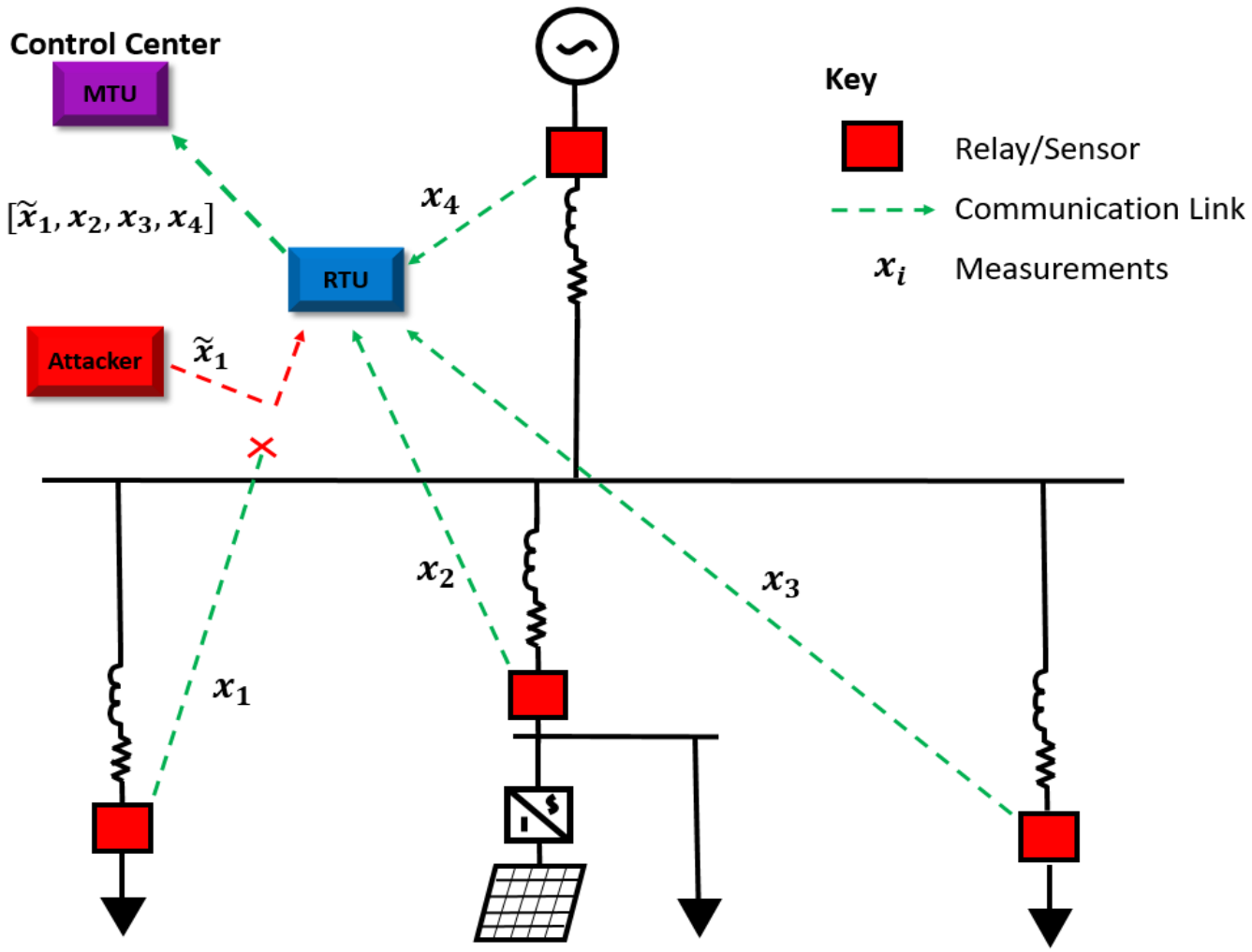
MIT LL Group 73 Senior Staff marija.ilic@ll.mit.edu

Massachusetts Institute of Technology

Outline

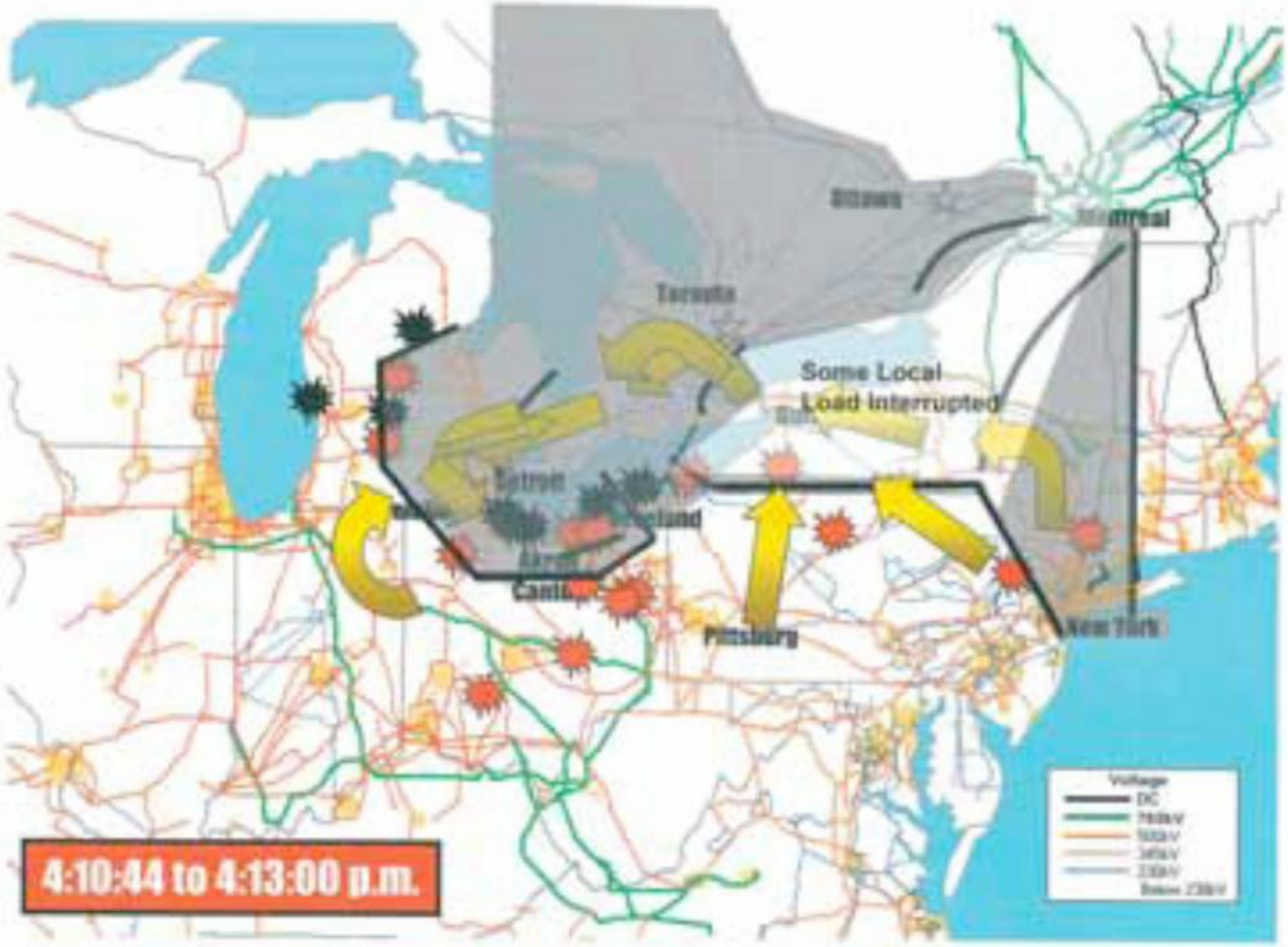
- **Reliable and secure (resilient) energy services.**
- **Challenges and opportunities.**
- **Technical challenge—design and implement next generation operating technology (OT) enabled by information technology (IT).**
- **Proposed approach to making it work.**
- **Getting there from here..**
- **Conclusions and recommendations**

Hidden IT and physical failures



Could lead to wide-spread blackouts…

- Relia



Reliable energy services

- Reliable service-- Energy system infrastructure in place to survive unplanned physical equipment failures and hidden IT failures and continue serving customers.
- Resilient (cyber-secure) services--- Have energy system infrastructure in place to survive targeted, well-planned cyber-attacks on energy system IT.
- Common problem: Can not be solved solely by building new hardware. Need for next generation integrated OT/IT.

Challenges and opportunities*

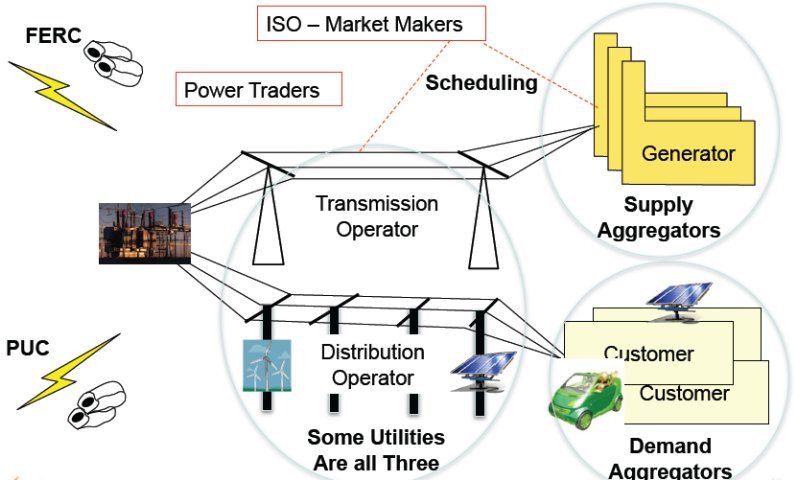
- ***Technical challenges:*** Design high tech operating technology (OT) and integrate it with information technology (IT) to enable energy services during extreme events (disasters, cyber-attacks).
- ***Business challenges***: No legal, political nor economic incentives for investment in OT/IT for secure and reliable energy services.
- ***Technical opportunities*:** Major innovation, high tech jobs.
- ***Business opportunities:*** ***a) for utilities*** *(high tech energy services business at value);* ***b) for vendors*** *(massive development and deployment of OT/IT infrastructures;* ***c) for electric energy users*** *(energy services at value).*

**Ilic, Marija, Toward a Unified Modeling and Control for Sustainable and Resilient Electric Energy Systems,* Foundations and Trends in Electric Energy Systems,Vol. 1, No. 1 (2016) 1–14, DOI 10.1561/3100000002

Today's OT/IT in energy systems

- Vertical "seams" within a BA
- Horizontal "seams" between BAs

Contextual complexity



Observations:

O1: Worst-case-based standards—do not work
O2: Highly inefficient (preventive)
O3: Do not apply local grid small users
O4:No incentives for flexible OT/IT deployment*
(yet functioning IT/OT critical!)

Industry reacting to mandates!

Exhausted, cant rethink new problems.

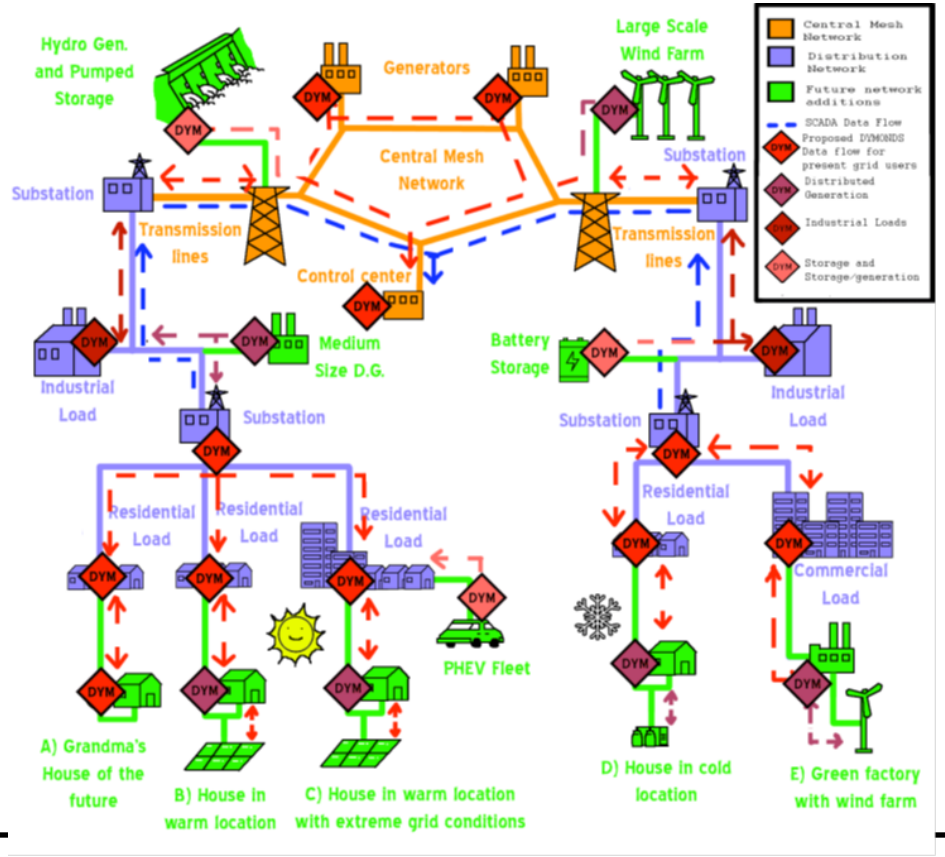
** Ilic, M., Invited testimony on reliability, FERC 2016*

**Toward more secure network environment in critical sector, IPRI, MIT Report, 2017, contact<joel@joelbrenner.com>*

Recommendations for enhancing OT/IT

- ***Rec. 1*** Move beyond worst case mandatory standards
- ***Rec. 2*** Systematic methods for benchmarking
- ***Rec. 3*** Enhance today's SCADA
- ***Rec. 4*** Create a dynamic interactive IT/OT environment
- ***Rec. 5*** Evolve today's Balancing Authorities (BAs) into intelligent Balancing Authorities (iBAs)
- R&D under way for such solutions; industry should work closely with academia toward next generation IT/OT

Next generation SCADA-Dynamic Monitoring and Decision Systems(DyMonDS)*

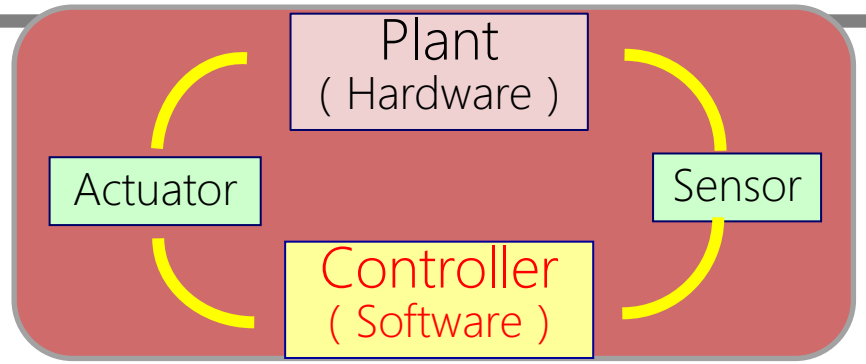


Basics for a working IT/OT:

O1: Multi-directional info flow
O2: Basis for on-line resource management
O3: End-to-end participation in supply/demand/delivery
O4: Possible to set simple specifications for ranges of power and energy characterizing different components
O5: Multi-layered –
--Detailed information local to components, iBAs
--Granular (aggregate) information exchange between iBAs

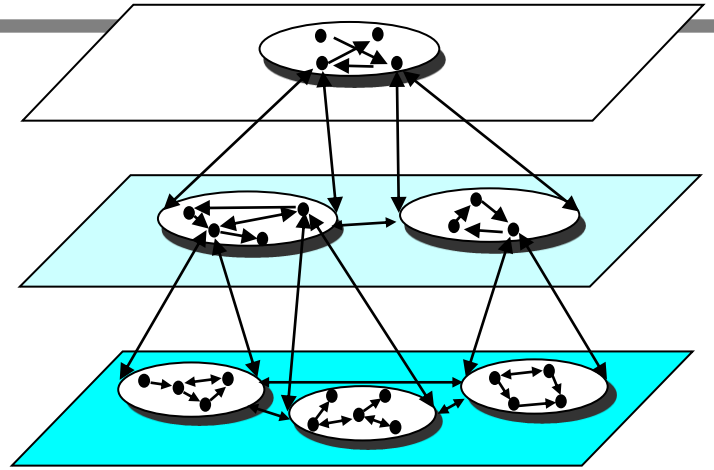
Next generation IT/OT for energy systems(Japan)

① Feedback



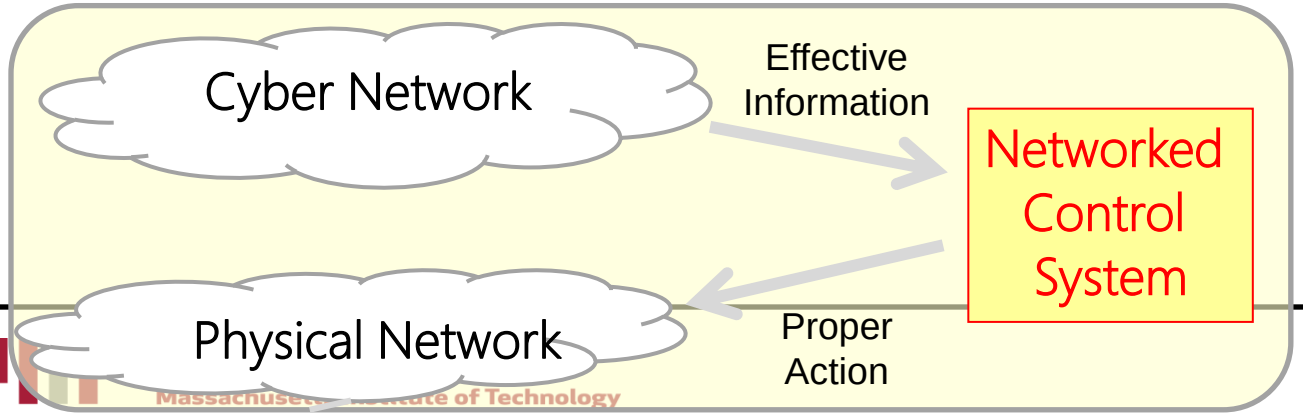
Feedback System

③ Hierarchy (SoS)



Interactive iBAs

② Hybrid (CPNS)



Cyber Physical Network System

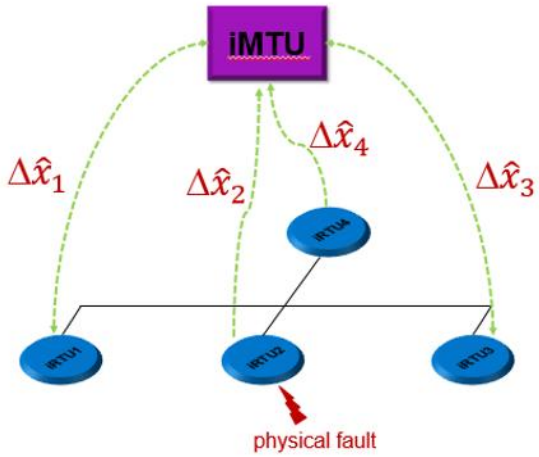
S. Hara & S. Honda, "System Science and Technology for Super Smart Society", Keisoku to Seigyo (Measurement and Control), Vol. 55, no. 4, pp. 284-287, 2016 , (in Japanese)

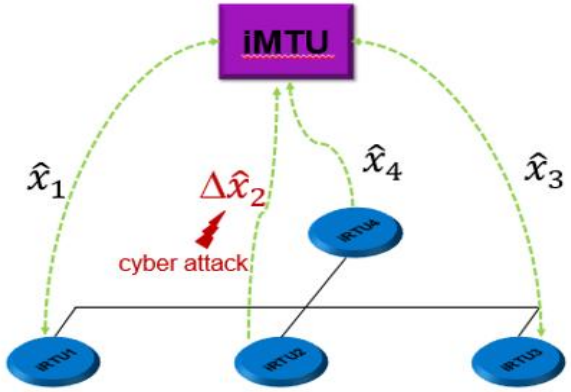
Cyber-security integral part of IT/OT system

- Aggregate variables representing iBAs for interacting with the rest of the system encrypted (by design!); could have IT/OT to dynamically aggregate and exchange information so that attacker never knows how is aggregation done
- Transparent multi-layered, not too complex. Could have lots of software for computing/and comparing with measurements to detect IT attacks.
- SEEDS project on iBA-based method for detection and protection against cyber attacks in energy systems

iBA-based method for differentiating between physical and IT failures*

Consequence / Attack	Cyber	Physical
Cyber	Acquisition of private information	Replay attack
Physical	Meter bypassing	Physical equipment destruction/failure





**Ilic, M., Jevtic, A., Aggregation approach to IT/OT for cyber-secure energy systems, IEEE CDC paper 2017 (under preparation)*

Recommendations

- Next generation IT/OT systems for secure, reliable, cost-effective and clean energy service needed
- Not sufficient to follow today's NERC reliability and CIP standards
- Could build on the existing IT/OT by focusing on what must be fixed (O1-O4)
- Probably the most straightforward way is to evolve today's balancing authorities into intelligent Balancing Authorities (lots of autonomy, could be at States level).
- Naturally lend themselves to dynamic encryption and manageable information processing

Getting there from here…

- Build on the on-going R&D in academia.
- Academia should work closely with industry and government to understand options prior to engaging into expensive and lengthy implementations; industry needs proactive help with next steps.
- Carefully designed simulators for purposes of emulating causes and effects during major disasters and cyber-attacks could help.
- The same simulators should be used to assess potential benefits from the proposed IT/OT solutions.