資料6-3

Standards : key for digital security of critical infrastructure

*

Richard Schomberg
IEC Ambassador & Chair
IEC System Committee for Smart Energy
Past Chair IEC Nuclear Instrumentation

METI Workshop
Digital Security
29 August, 2019
Tokyo

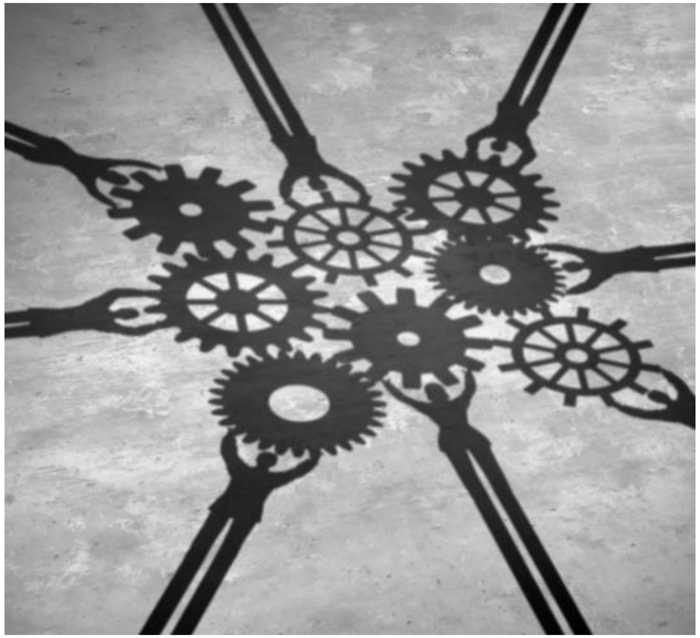
International
Electrotechnical
Commission

Questions to be addressed

- What are the greatest digital risks to energy systems?
- What can be done to enhance digital resilience?
- What is the most reasonable approach for using standards and their Certification Schemes?

Energy: complexity is increasing

+ More interconnection
+ More information exchange
+ Higher reliability, increased control
+ Better interoperability
- Increased cyber vulnerabilities



Roles and challenges

Regulators:

- Raise cyber security awareness, assign accountability, provide clear requirements

Utilities:

- Accept responsibility, update infrastructure, commit necessary investment

Global risks, global approach

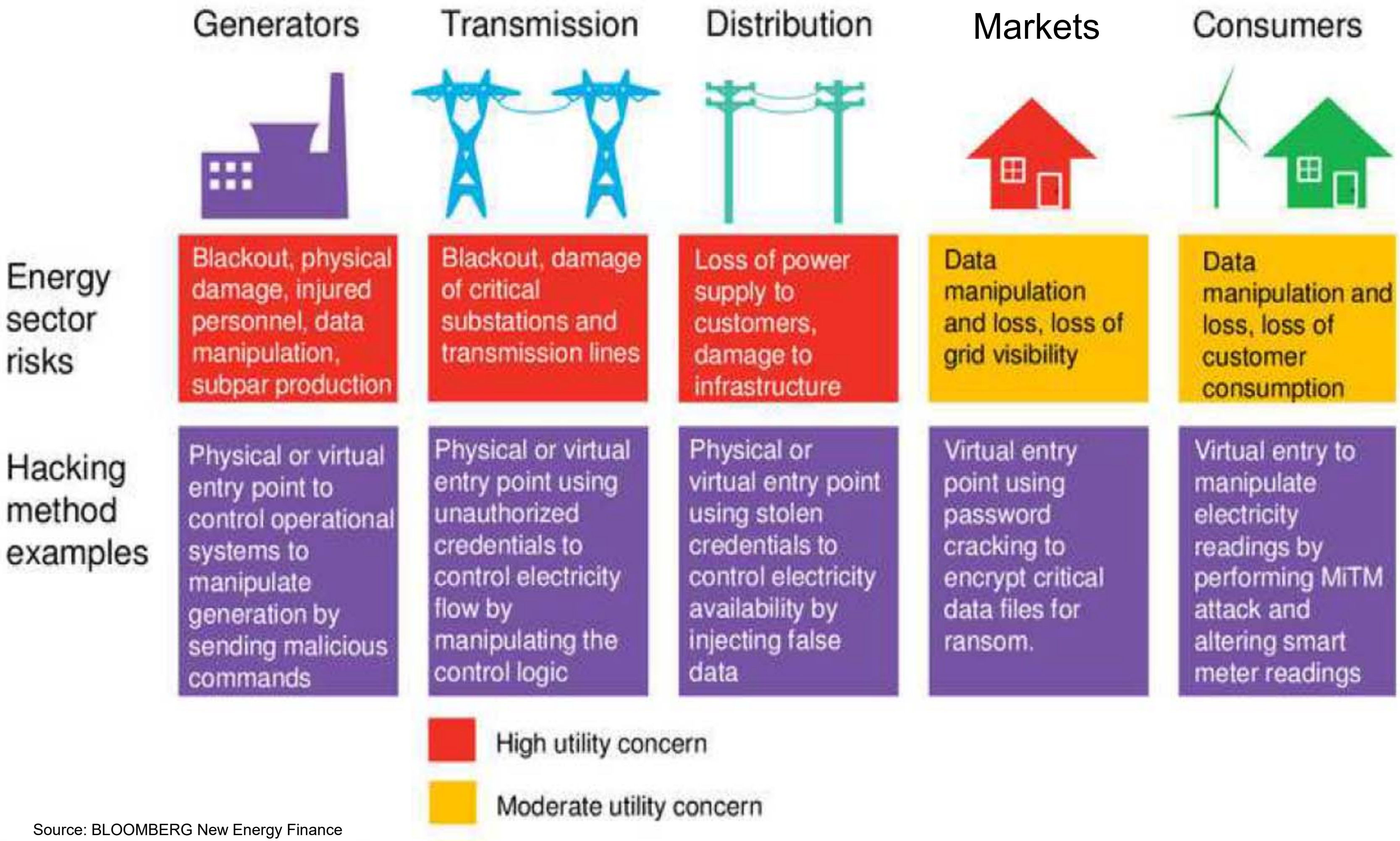
Prefer common platforms that encourage cooperation and avoid island solutions.

IEC Standards:

- Global reach – 171 countries
- Members = countries
  not companies
- Built-in high consensus value
- Neutral, independent

Provide input to standardization.

Five "ecosystems" requiring adapted cybersecurity Certification Schemes



	Generators	Transmission	Distribution	Markets	Consumers
Energy sector risks	🟥 Blackout, physical damage, injured personnel, data manipulation, subpar production	🟥 Blackout, damage of critical substations and transmission lines	🟥 Loss of power supply to customers, damage to infrastructure	🟨 Data manipulation and loss, loss of grid visibility	🟨 Data manipulation and loss, loss of customer consumption
Hacking method examples	Physical or virtual entry point to control operational systems to manipulate generation by sending malicious commands	Physical or virtual entry point using unauthorized credentials to control electricity flow by manipulating the control logic	Physical or virtual entry point using stolen credentials to control electricity availability by injecting false data	Virtual entry point using password cracking to encrypt critical data files for ransom.	Virtual entry to manipulate electricity readings by performing MiTM attack and altering smart meter readings

🟥 High utility concern

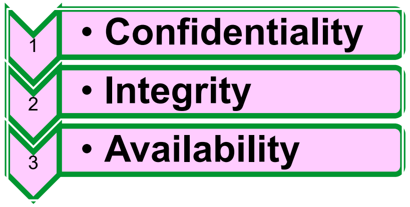
🟨 Moderate utility concern

Source: BLOOMBERG New Energy Finance

IT Security is different from OT Security

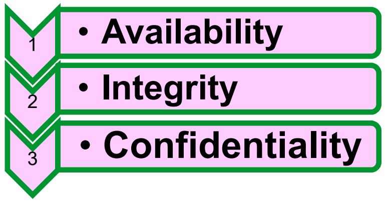
- The power system is a **cyber-physical system**, which combines the physical and electrical properties of the power system operational equipment with cyber-based control of that equipment.
- The **requirements for cybersecurity of cyber-physical systems are very different from those for typical IT** systems.
- Cyber-physical systems must not only protect the information in cyber assets but also ensure the **resilience** necessary for the physical system to remain operational.

IT



1. Confidentiality
2. Integrity
3. Availability

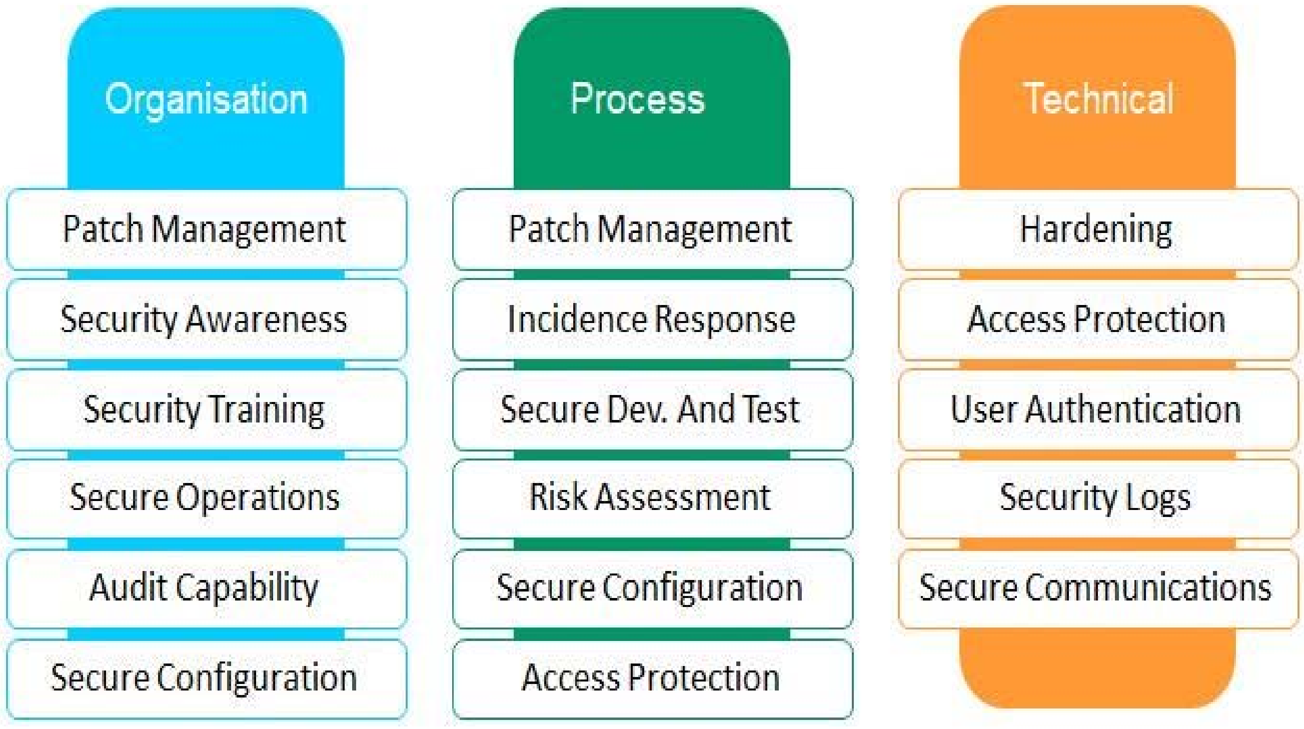
OT



1. Availability
2. Integrity
3. Confidentiality

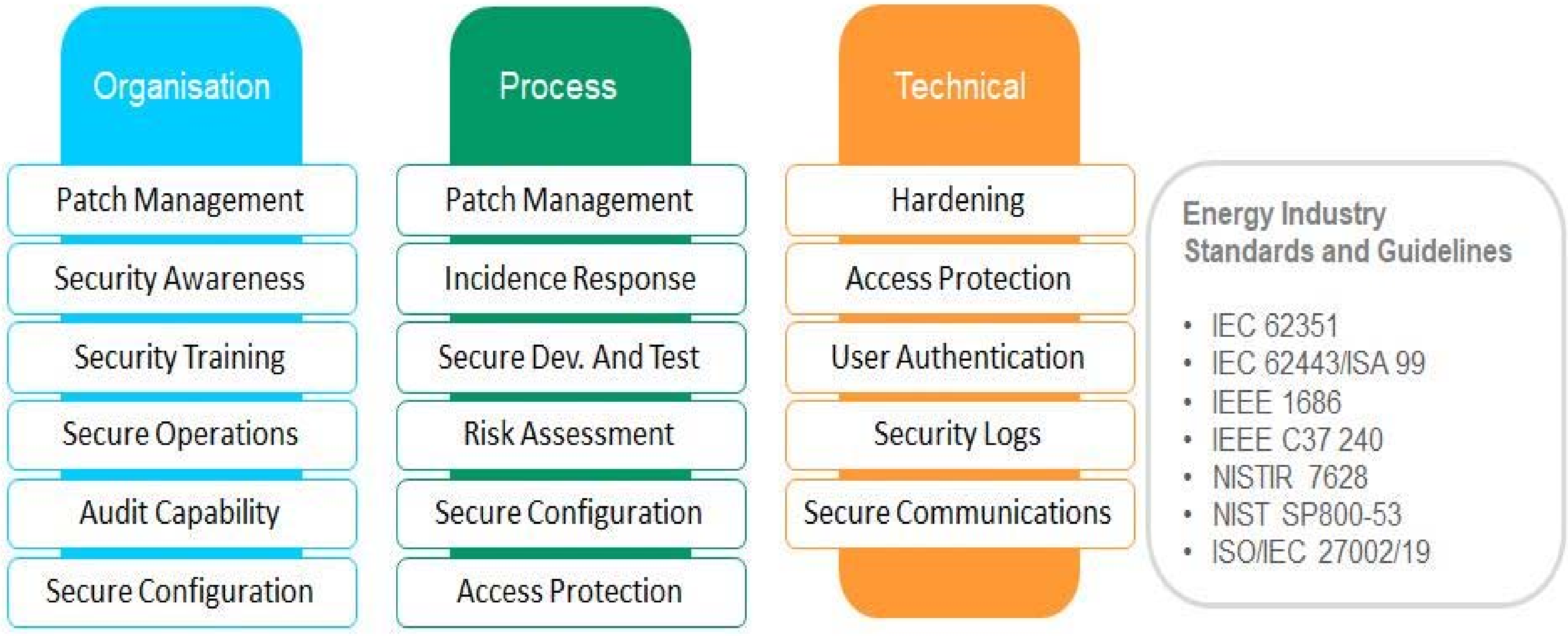
- *Cannot just shut down the power system if attacked*
- *Must protect physical equipment, not just protecting information*

Not just about installing secure technology !



Organisation	Process	Technical
Patch Management	Patch Management	Hardening
Security Awareness	Incidence Response	Access Protection
Security Training	Secure Dev. And Test	User Authentication
Secure Operations	Risk Assessment	Security Logs
Audit Capability	Secure Configuration	Secure Communications
Secure Configuration	Access Protection	

Build to International Standards



Organisation	Process	Technical
Patch Management	Patch Management	Hardening
Security Awareness	Incidence Response	Access Protection
Security Training	Secure Dev. And Test	User Authentication
Secure Operations	Risk Assessment	Security Logs
Audit Capability	Secure Configuration	Secure Communications
Secure Configuration	Access Protection	

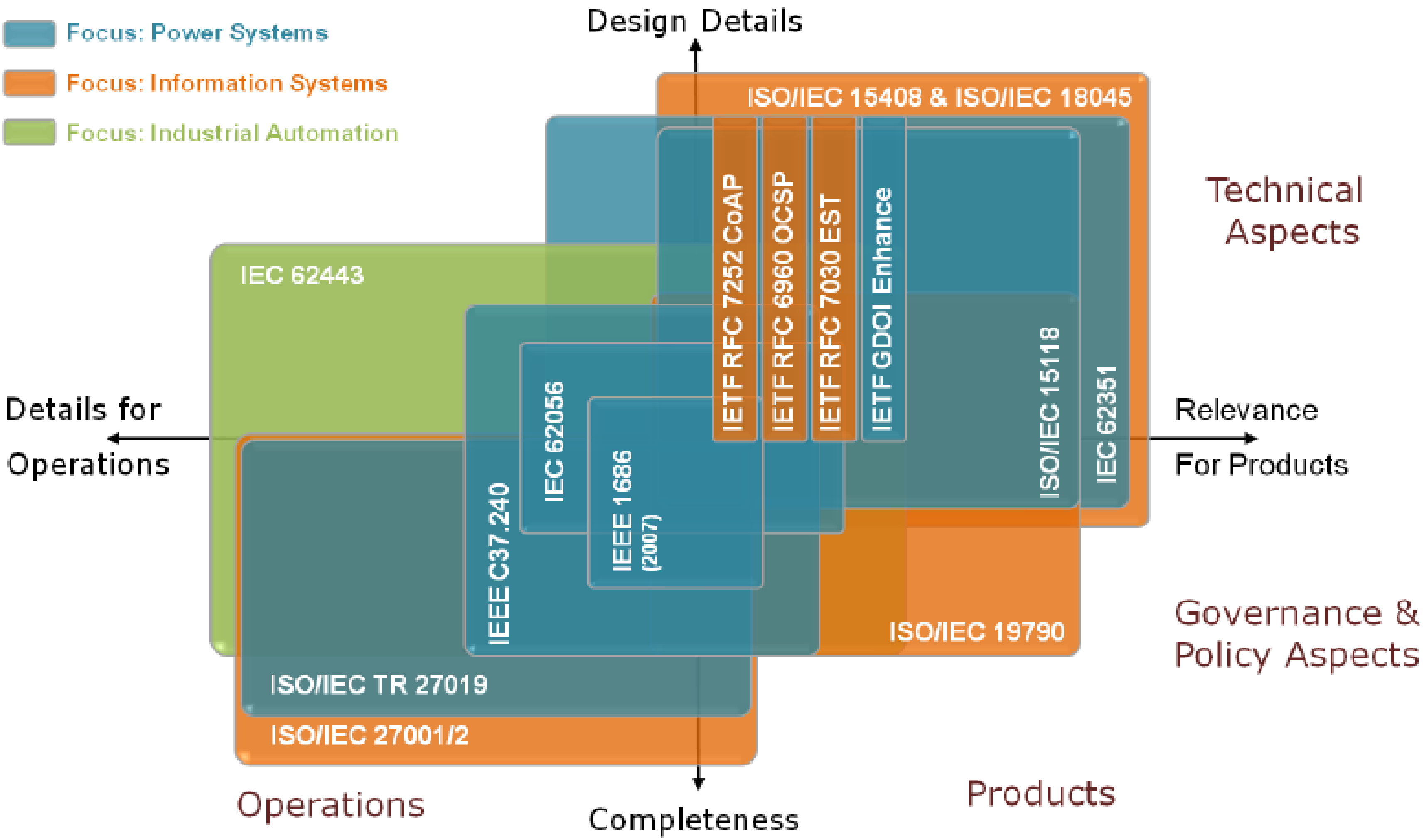
Energy Industry Standards and Guidelines

- IEC 62351
- IEC 62443/ISA 99
- IEEE 1686
- IEEE C37 240
- NISTIR 7628
- NIST SP800-53
- ISO/IEC 27002/19

IEC: 235 OT and ICT security related publications

IEC Conformity Assesment Systems in cyber security

ISO/IEC270xx & ISO/IEC15408 & IEC62443



Reality Principle: use at best what already can be put to work !

- One cybersecurity standard cannot satisfy all requirements !
- Different combinations of cybersecurity standards can more effectively address different areas or purposes
- The most effective and practical approach : A mix of cybersecurity standards and their established Certification Schemes should be used selectively for each of the 5 "ecosystems"
- Still an international effort needed to establish:
  - A consensus on the equivalence between the levels of cybersecurity assurance of different standard families
  - How to achieve a global high level of assurance by combining parts not necessarily of the same high level

3
Shanghai Transrapid

IEC

BLAUPUNKT
Internet Radio
NEW JERSEY 600i
TUNER
SOURCE
AUDIO
MENU
DIS·ESC
OK
AUX
USB