



Concluding Remarks

Tutorial – On behalf of Cigré **JWG D2/B3/C2-01**
*“Security for Information Systems and Intranets
in Electric Power Systems”*

presented by
Giovanna Dondossola
CESI - Italy



Agenda Tutorial

- 1 Introduction - Cyber Security Considerations in Power System Operations
- 2 Framework for Managing Information and Control Systems Security in an Electric Utility
- 3 Cyber Risk Assessment in the Electrical Power Industry
- 4 Concluding Remarks



Agenda Part 4

- 1 Summary of the Tutorial
- 2 Research challenges



Summary: Part 1 - 1

Part1: Cyber security considerations for the Electric Power Industry

- ✉ **Awareness** about the consequence criticality / relevance of cyber risks in the power industry needs to be increased
- ✉ Agreement on a **security terminology** shared within the electric community has to be reached



Summary: Part 1 - 2

Part1: Cyber security considerations for the Electric Power Industry

- ✉ Experienced black-outs, although not influenced by malicious acts, demonstrated that catastrophic situations are caused by **concurrent multiple faults**, electric contingencies are compounded by malfunctions of monitoring, protection, control systems or by insufficient coordinated response



Summary: Part 1 - 3

Part1: Cyber security considerations for the Electric Power Industry

- ✉ Security needs to be treated by identifying different information system **domains** and by managing their inter and intra domain interactions

- ✉ Suggested actions need to be taken while comprehensive measures are developed

- ✉ Many activities are active in standard working bodies (IEC, NERC, ISA, AGA, ...)



Summary: Part 2

Part2: Information and Control Systems Security Framework in an Electric Utility

- ✉ Standards, Guidelines, Best Practice for Cyber Security Management comes from three domains: general IT, SCADA/Control Systems, Electric Industry

- ✉ The security management is based on a multi-domain model

- ✉ Need of a comprehensive framework



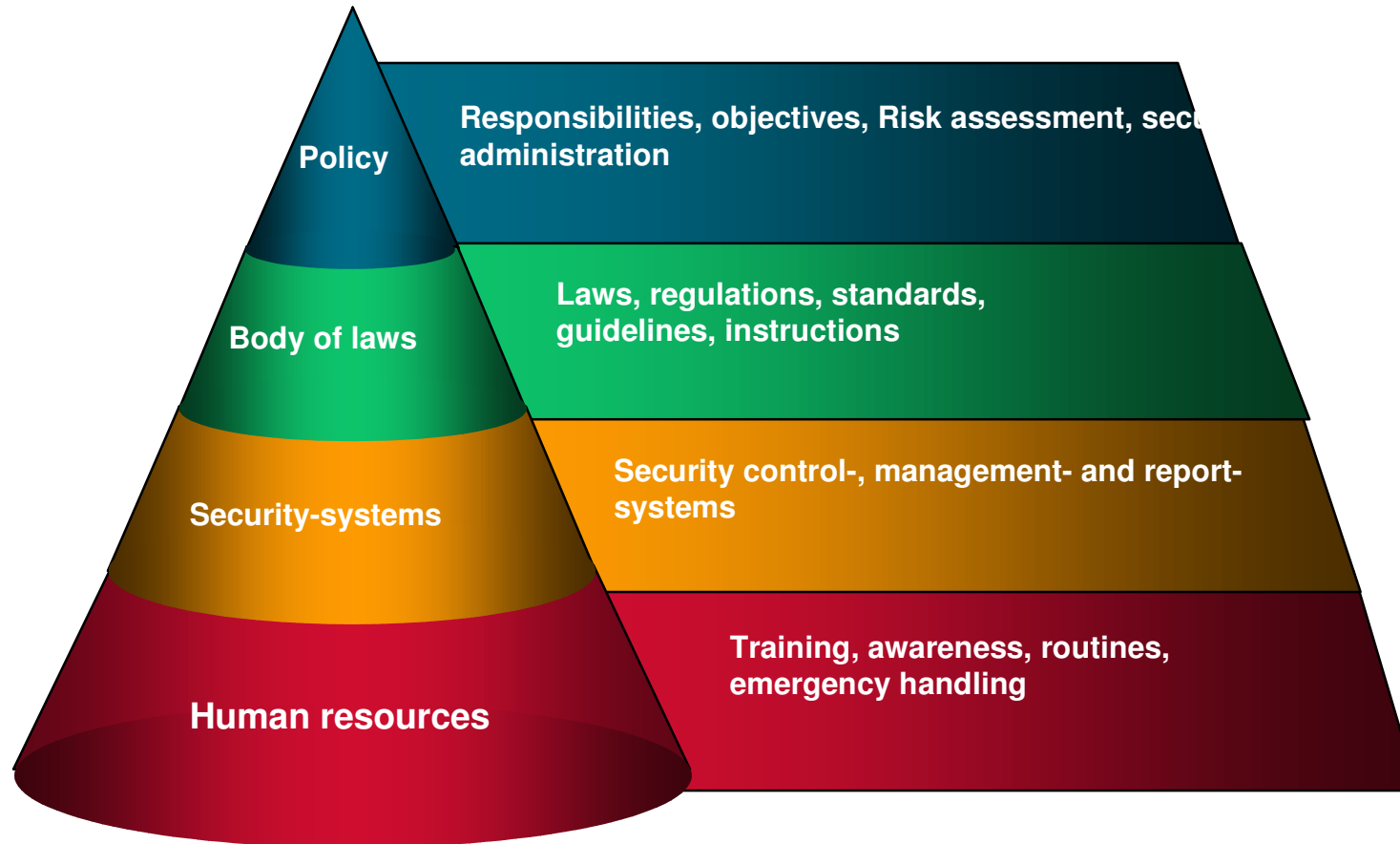
Summary: Part 3

Part3: Cyber Risk Assessment

- ✉ need of automatic tool support the security analysis of power control systems
- ✉ need of a risk assessment approach integrating electric power and control system security



The need for a complete handling of ICT security in the Electric Power Industry





Research challenges - 1

- ✓ Security assurance and management
 - ✓ review of ISO 17799 for industrial systems
 - ✓ security policies for integrated administrative and industrial systems

- ✓ Common vulnerabilities, threats and attack models

Shared models that facilitate the exchange of information across industry and with regulators/authorities, and the consistent application of standards (e.g. Common Criteria)

- ✓ Risk-based security assessment

Compatible with the sector and generic standards, and suitable to the evaluation of the security of large industrial systems connected to open networks that include **real-time components**



Research challenges - 2

- ✓ Support to certification and third party verification of infrastructural systems
 - Assurance cases for certification and mutual demonstration of security statements, and support to trust networks among stakeholders

- ✓ Support to operational security
 - ✓ security technologies for industrial systems
 - ✓ security of industrial systems including real time control networks