STARGRID WORKSHOP

Recommendation R4 “Security and Privacy”

Emilio Rodríguez (TECNALIA)

Brussels, 23 January 2015

1. Security and privacy: the problem

- **ICT technologies** will allow the Smart Grid paradigm, improving efficiency, reliability and sustainability of the power system, allowing new functionalities, etc. but increasing the **potential threats and attacks**. Reasons:
    - Deregulation leads to an increase of actors (consumers, DG producers, aggregators,…) and data communications (interfaces) → vulnerabilities-gateways for attacks to the overall system-
    - Massive deployment of IT-based components. Increasing connectivity and software-based solutions.
    - Lots of different domain requirements, preventing the application of standard security measures (example, antivirus software)
    - Increase of communications over public networks (Internet)
- Growing **complexity** of the Smart Grid increases exposure to potential attackers who can exploit vulnerabilities and penetrate the power network.
- Smart meter and smart appliances will provoke a data tsunami of **private details** of daily life (showing consumer behaviour and characteristics). It is not clear who is the owner and who can make use of this data.

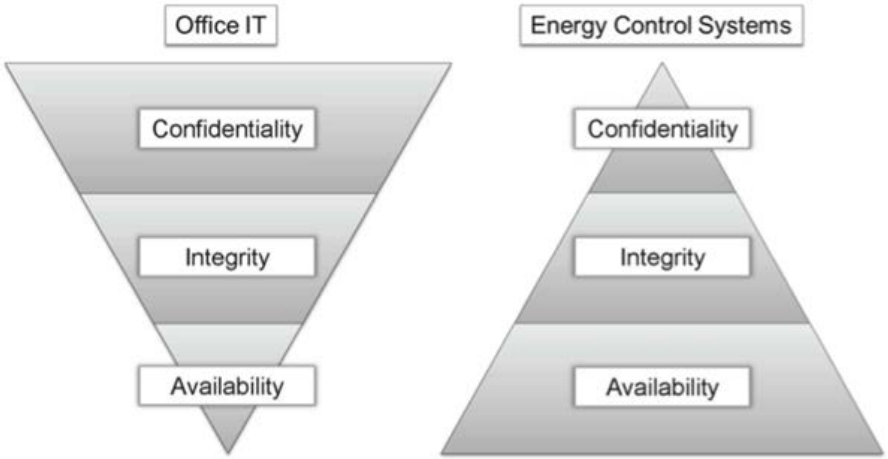
1. Security and privacy: the problem

- **Some examples of attacks** already detected and published:
  - Theft of CO2 certificates at emission trading (bad identity control)
  - Viruses and worms attacking energy companies: *Flame*, *Shamoon*,…
  - Worm *Stuxnet* manipulated industrial facilities and sabotaged the Iranian uranium enrichment.
  - Attacks to SCADA systems
  - Hacking of smart meters
  - …

2. Security and privacy: some basic concepts

"Cyber-Security":
Branch of computer and network technology also known as **Information Security**. The objective of information security is the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional (while allowing the information to remain accessible and productive to its intended users).

- **It includes also "privacy"** (protection of the misuse of personal data)
- **Holistic approach** (security is a global issue and measures are necessary in every layer of the architecture)
- **"Security-by-design"**(security analysis to identify relevant security processes and measures at the beginning of the development)
- **Different prioritization of the main protection goals** (pyramid of IT security requirements)



3. Critical issues from the STARGRID survey

- **Relevance and Future Impact of Standards**:
  High score Core IEC Standard on Security (IEC 62351, "Power systems management and associated information exchange – Data and communications security")
- **Highest priority gap for the *smart metering* topic**: strong security mechanisms (encryption & authentication) mandatory for the WAN communication of the smart meter gateway
- **Some hints from the "industry"**:
  - ✓ *"Security and security standards is the challenge due to the complexity of the Smart Grid system"*
  - ✓ ***"Security aspects are not sufficiently guaranteed by the existing standards"***
  - ✓ ***"Traditional security systems are ineffective against aimed attacks"***
  - ✓ *"The complexity of the system highly increases the risk of aimed attacks and makes ineffective the old security scheme"*
  - ✓ ***"Requirements on security/privacy and information models are not clear and agreed enough"***

3. Critical issues from the STARGRID survey

- **Some hints from the "industry"**:
  - ✓ *"A new scheme is necessary based on the anti-intrusion rules i.e. the same approach as for critical infrastructures should be adopted (including asset identification, security control, perimeters security, physical security, personnel & training, recovery management models adapted to the energy chain"*
  - ✓ ***"The problem is that requirements for security are not agreed and clear enough. Once that is solved, the implementation should not be a problem: the technology already exists in other areas (cryptography)"***
  - ✓ ***"Measures for smart meters personal data protection should be harmonized. Standards for use of sensible energy data are still missing in EU"***
  - ✓ *"Customer is the owner of the data. Data which is not required for billing or statutory purposes should only be provided with the express consent of the consumer"*
  - ✓ ***"Consumer/customer data protection is the pre-requisite for his participation in the business and the realisation of forecast benefits"***
  - ✓ *"Failure to adequately address consumer concerns about privacy will limit active consumer involvement and make it difficult to realise forecast benefits"*
  - ✓ *"Perform local processing at the meter level (data minimization and less exposure)"*

4. STARGRID Main Recommendations

R4: *Develop a standards framework for security against physical and information attacks and data protection encompassing the requirements of Smart Grids with a coordinated and systemic approach*

- Develop a harmonised legal framework across Europe, ensuring security of the energy system and data protection
- Approach the security standardisation through a "security-by-design" concept based on Use Cases definition and associated risk analysis. Standardise the approach methodology
- "Privacy-by-design-and-default": no supplementary customer actions are needed to keep privacy and explicit consent must be obtained before disclosing personal information to third parties. Transparency: customer must be informed about collection and use of personal data
- Enhance awareness and provide clear instructions on information privacy and protection to utilities and consumers using Smart Grid services. Implement policies at EU and National level

4. STARGRID Main Recommendations

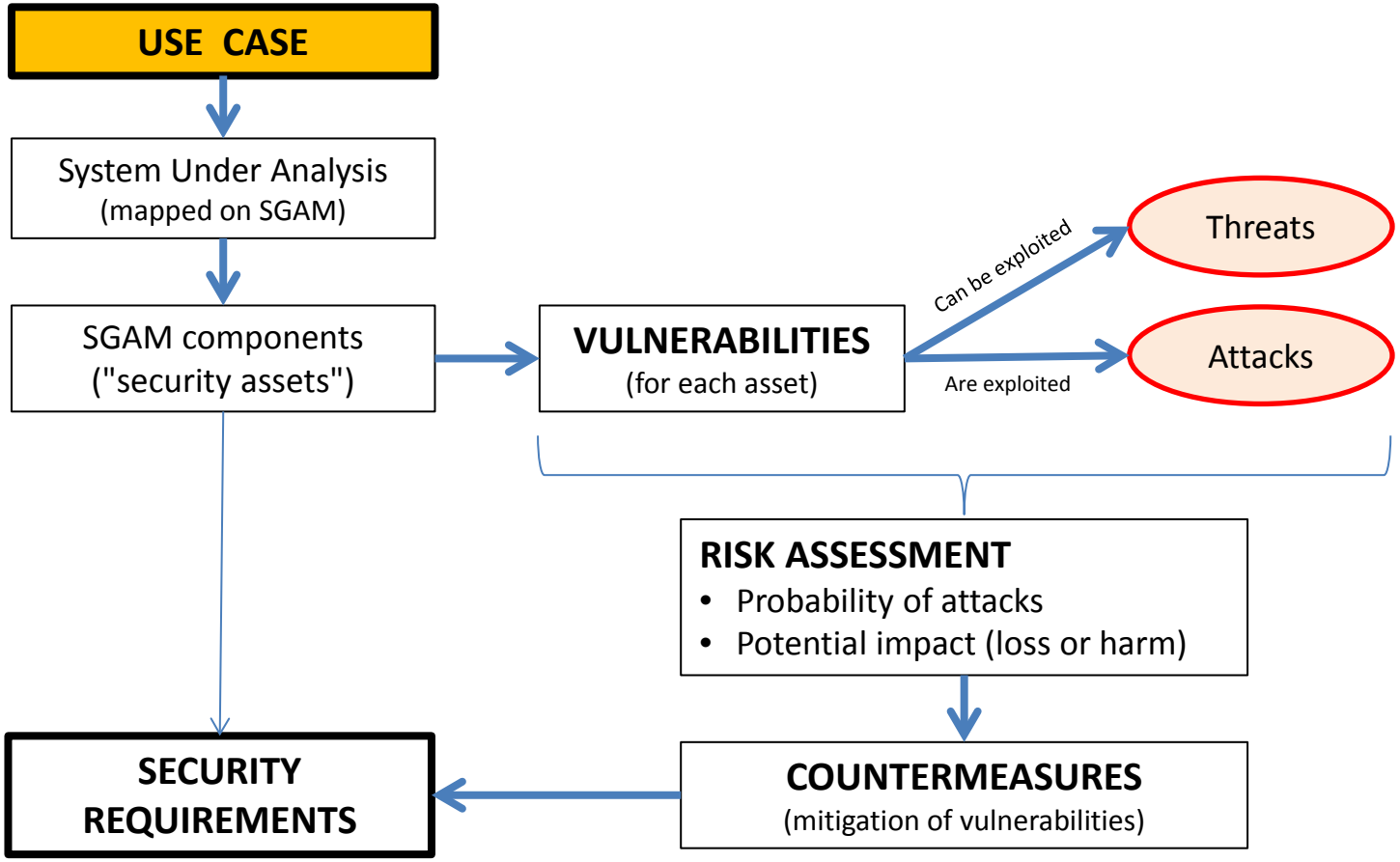
R4: *Develop a standards framework for security against physical and information attacks and data protection encompassing the requirements of Smart Grids with a coordinated and systemic approach*

- Stakeholders should clarify and agree the requirements on information security and data privacy
- Stakeholders should use standardised formats, language and models for the specification of requirements on security/privacy
- Take advantage of EU funded projects to develop security Use Cases and specifications
- Coordinate security and interoperability analysis approaches

5. Implementation: Use Cases development

- Identify and define **critical Use Cases**, where security is paramount. Whenever necessary for these critical situations, **develop missing Use Cases**.
- **Similar approach** to the one proposed for **interoperability** test specification and validation (STARGRID Recommendation R3): selection and definition of use cases (actors, interfaces, information exchanged, etc.)
- Interoperability is a **pre-requisite** for security (harmonised/standardized protocols and information models)

5. Implementation: Basic approach for security analysis



5. Implementation: standards

- There are **well-established security standards** for different targets groups and topics
- Diverse security standards exist **to establish the base of SG security** but still existing and new use cases, technologies, policies, best practices must be considered and incorporated
- **Standards objectives**: (1) unification and simplification of the design process of IT security and (2) achieve a dedicated security level on technical, organizational, or procedural level

MAIN STANDARDIZATION ACTIVITIES ON SECURITY:

- **CEN/CENELEC/ETSI SGCG Working Group SGIS** (Smart Grid Information Security):
  - Response to M/490 Mandate
  - Provision of a high level guidance on the use of standards for IT security in SG
  - Selection of security standards mapped on SGAM
  - Analysis of several use cases to show applicability of standards
  - Provision of the "SGIS Framework" ("SGIS Toolbox") for risk analysis and election and implementation of security measures for the use cases

5. Implementation: standards

MAIN STANDARDIZATION ACTIVITIES ON SECURITY:

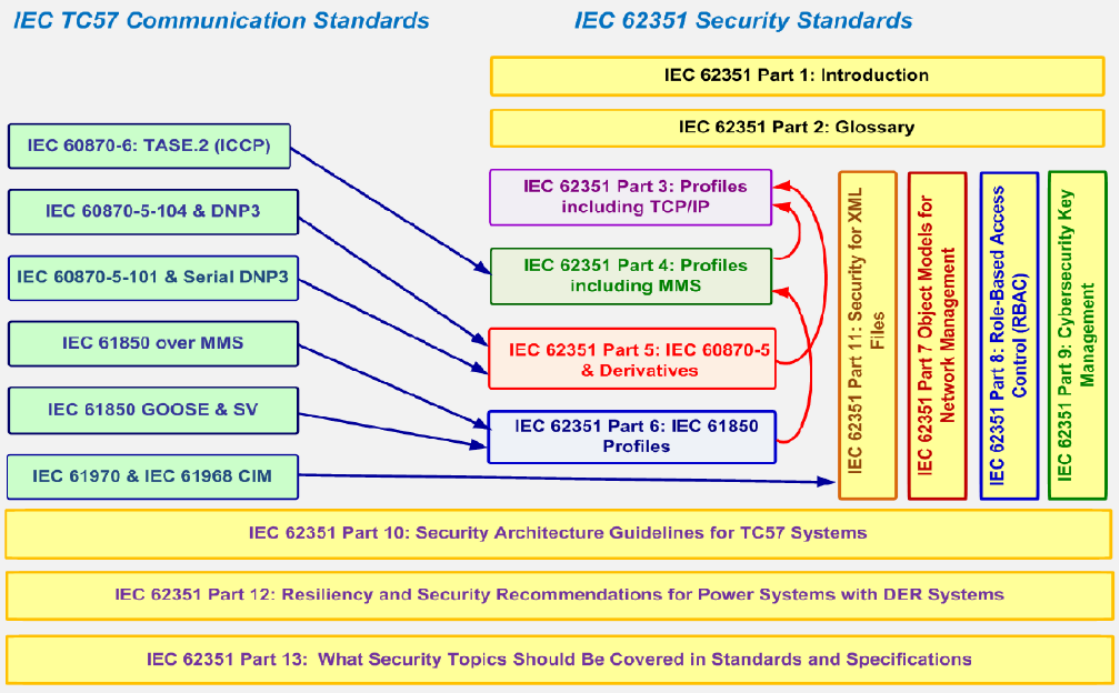
- **ISO/IEC 27000 series**: general approach for information security management systems (governance aspects: risk assessment, policies,...)
  - Specially relevant: **ISO/IEC TR 27019** (information security management for process control systems specific to the energy utility industry)

- **IEC 62443 (ISA 99)**: industrial communication networks – network and system security

5. Implementation: standards

MAIN STANDARDIZATION ACTIVITIES ON SECURITY:

- **IEC 62351**: power systems management and associated information exchange – data and communication security ("core IEC standard for Smart Grids")
  - End-to-end security specification for the reference architecture (IEC/TR 62357-1)
  - Covering most of the IEC TC57 communication protocols (IEC 60870, IEC 61850, IEC 61970, and IEC 61968 series)
  - Not covering information security management issues
  - 11 parts (mostly Technical Specifications) + 2 new Technical Reports



5. Implementation: standards

MAIN STANDARDIZATION ACTIVITIES ON SECURITY:

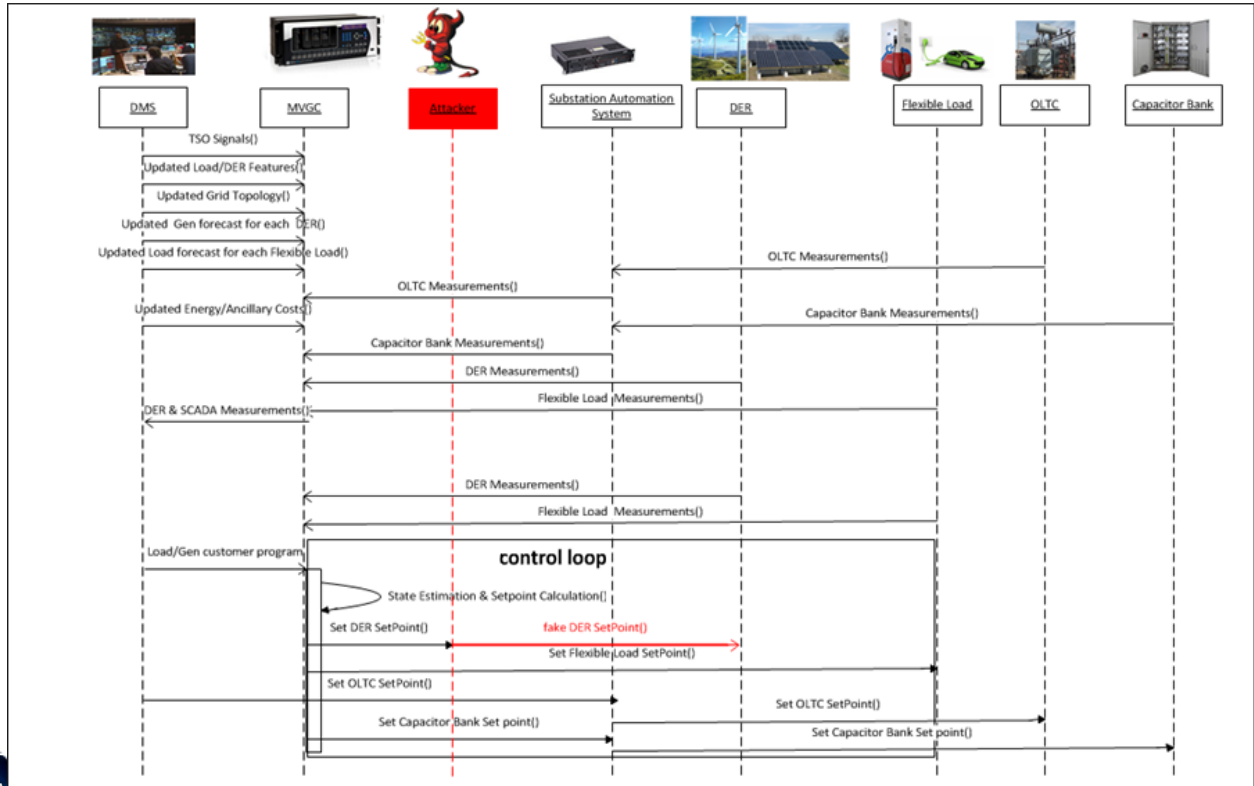
- **ENTSO-E Network Code on Operational Security**: focused on common operational security principles at pan-European level, coordination of system operation, etc.
- **ENISA** (European Union Agency for Network and Information Security): security and resilience of critical infrastructures
- **NISTIR 7628**: reference in USA
  - Vol. 1: overall approach, risk assessment process, high level security requirements
  - Vol. 2: recommendations for privacy
  - Vol. 3: supporting analyses and references
- **NERC CIP standards family** (USA, Canada, Mexico): mandatory cyber-security framework
  - Identification of criticalities and vulnerabilities of network assets
  - Personnel training
  - Physical security; electronic security perimeter
  - Incident reporting
  - System security management
  - Recovery plans,...

5. Implementation: EU funded projects

- **EU funded projects** are a proper context to develop an effective security framework with a systemic approach:
  - Definition of use cases and associated security requirements
  - Production of tools and guidelines
  - Identification of best practices,...

- Examples:
  SoES project,
  SmartC2Net project,
  Crutial project

- Specific actions should be addressed by **targeted calls** (in H2020)



Use Case example:
Intrusion of DER fake set points in a voltage control system

5. Implementation: privacy

- A **wider sensitivity** on data protection and privacy should be strongly fostered at EU level
- Upcoming **European Commission data protection regulation** (GDPR, "General Data Protection Regulation") applied to the Smart Grid ecosystem.
- Standards must **translate the generic privacy requirements** from the legal framework into the technical details.
- **"Privacy-by-design-and-default"**: privacy protection measures must be embedded in the design of Smart Grid systems, with no supplementary actions by the customer to guarantee privacy of personal data.
- This will generate the needed **confidence for customer** participation in the Smart Grid (ex. Demand Response programmes)
- **Privacy protection technologies** must be **adapted and applied to the Use Cases** requiring personal information (smart metering, smart appliances, electrical vehicle), leading to standardized mechanisms and requirements.

6. Conclusions

- **Smart Grids requirements** engineering must focused not only on functional aspects but also on **non-functional** aspects like **information security and privacy**.
- In general, the **legal framework supporting security standardization** is feeble across Europe and is not harmonised.
- **"Security and privacy-by-design"** is an import paradigm for the development of the Smart Grid as a critical infrastructure.
- IT security is already covered by several groups of **security requirement** but **harmonization** is needed.
- Diverse security standards exist to **establish the base of SG security** but still existing and new use cases, technologies, policies, best practices must be **considered and incorporated**. **Guidance and tools** must be provided for the security ecosystem.
- Security relevant for the **operation of the Smart Grid** as a critical infrastructure but also very important for **user acceptance** (example, smart metering and privacy)
- **STARGRID Recommendations** as possible master lines to be followed

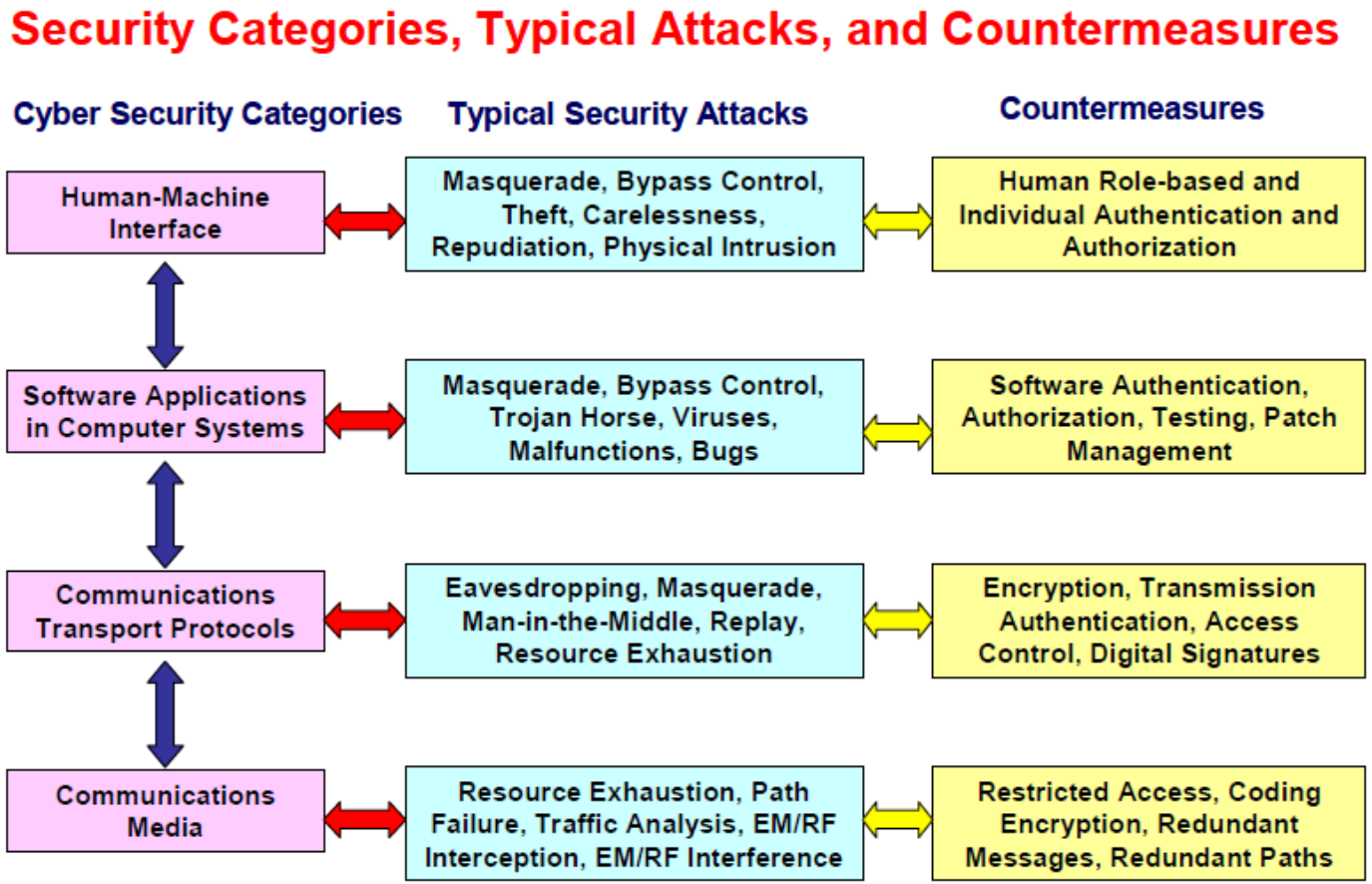
QUESTIONS, COMMENTS, DISCUSSION

THANK YOU

Emilio Rodríguez
TECNALIA

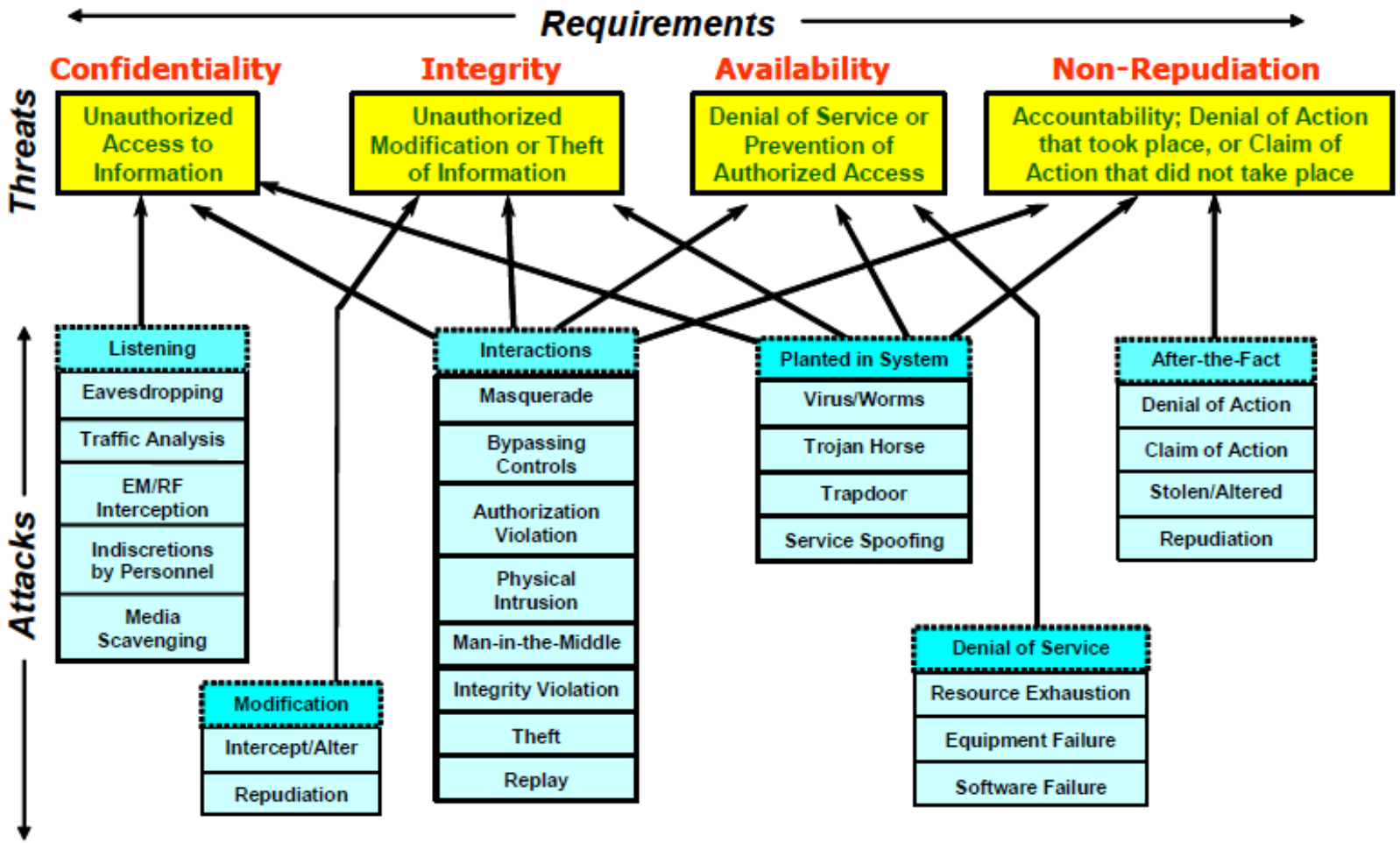
jemilio.rodriguez@tecnalia.com

COMPLEMENTARY SLIDE
Security and privacy: concepts



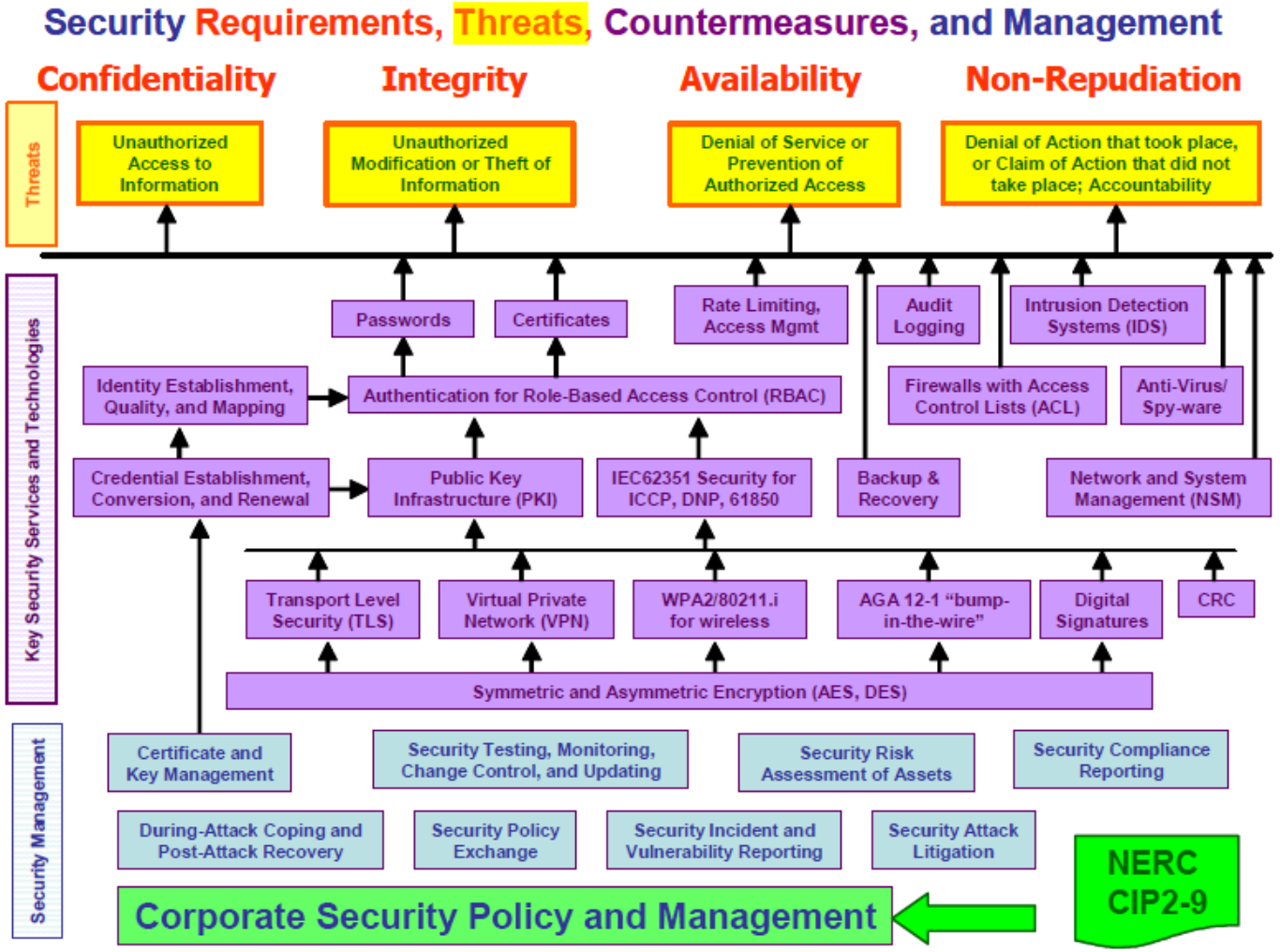
Source: IEC 62351

COMPLEMENTARY SLIDE
Security and privacy: concepts



Source: IEC 62351

COMPLEMENTARY SLIDE
Security and privacy: concepts



Source:
IEC 62351