Generic methodology for a systems-approach to conformity assessment for cybersecurity as the basis for a UN CRO guidelines

David Hanlon
IEC Secretary of the Conformity Assessment Board

UNECE WP.6
27th Annual Session
International Regulatory Cooperation
November 30th 2017, Geneva

INTERNATIONAL ELECTROTECHNICAL COMMISSION

Cybersecurity environment

All at risk

- Data theft
- Corporate hacking
- Critical infrastructure
- Smart grid
- Smart manufacturing
- Smart cities
- Smart homes
- Internet of things
- Railway systems
- Air transport systems

  and so on

IEC Cybersecurity activities

ACSEC

- A standards development (SD) initiative to understand the current global situation concerning standards with cybersecurity elements.
- >650 standards found
- >50 standards development organizations

IEC Cybersecurity activities

IECEE

- Full global CA services for cybersecurity based on IEC 62443 series
- CA services for cybersecurity launched at a workshop held in Chicago in November
- Cybersecurity CA services for…
  - Industry automation
  - Critical infrastructure
  - Railways
  - Information services

    etc

IEC Cybersecurity activities

CAB WG17

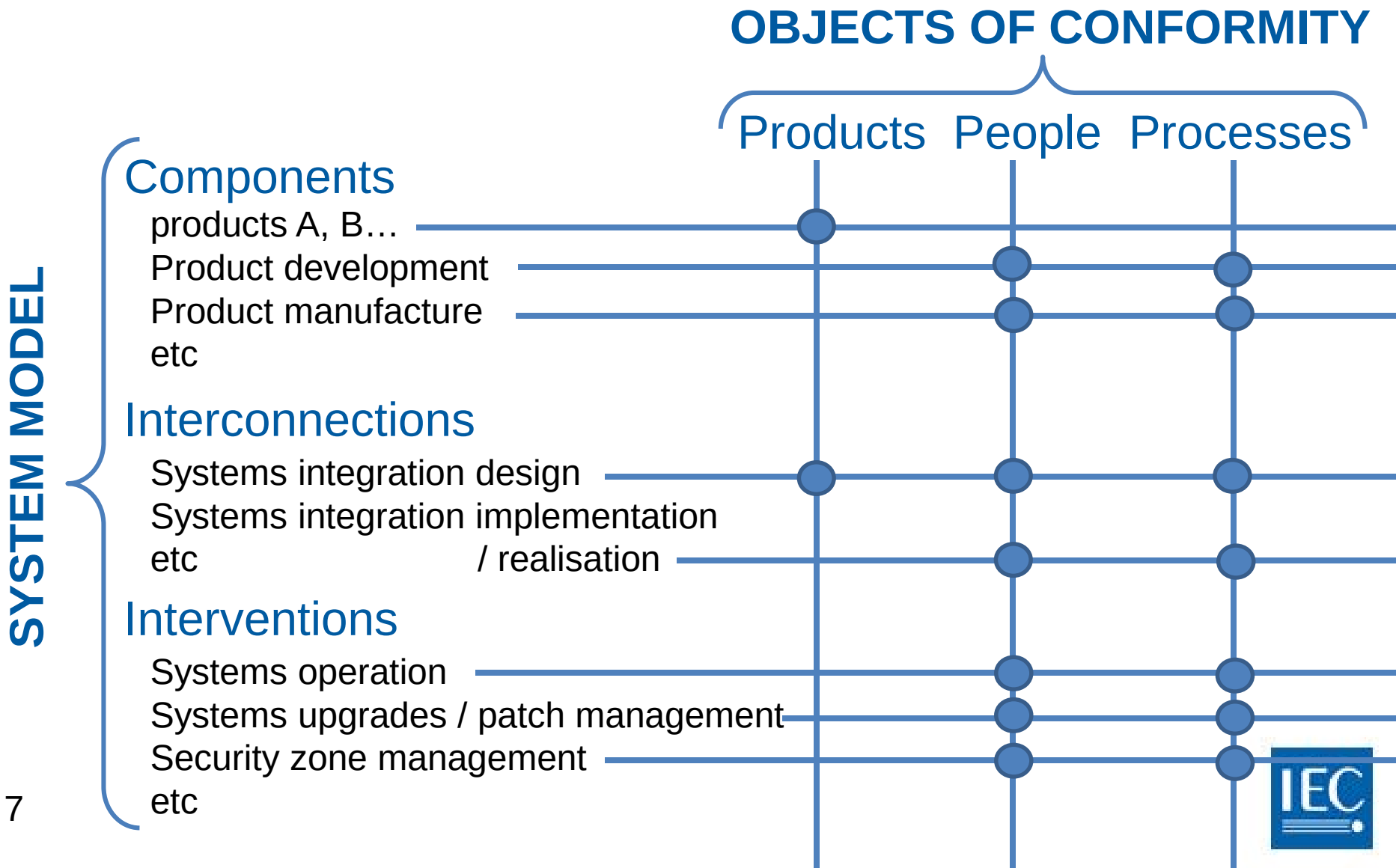
- To investigate market needs and timeframes for global CA services in cybersecurity
- To investigate national regulatory responses to the market needs for cybersecurity.
- To propose a systems-approach to CA for cybersecurity.

UNECE & IEC

Collaboration

- To develop a proposal for a sectorial initiative on cybersecurity
- To propose a tool for use by governments, regulators, asset-owners and industry
- A systematic methodology of systems modelling, risk & requirements gap analysis, determination of system-wide CA needs and then implementation and review.

Systems-approach to CA



Generic Matrix Model (GMM)

		Objects of conformity					
Activities	**Who**	**Products**		**People**	**Processes**		
Components							
Systems components development	Component producers Asset Owners	IEC 62443-4-2	Technical security requirments for IACS components		IEC 62443-4-1	Product Development Requirements
Systems components manufacture	Component producers Asset Owners (?)	??			??	
Interconnections							
System intergration design	Systems designers Asset Owners				IEC 62443-2-4	Requirments for IACS solution suppliers
System intergration implementation / realisation	Systems builders Asset Owners				??	
Interventions							
Systems operation	Asset Owner Service provider				IEC 62443-2-1 IEC 62443-2-2	IACS security management system - Requirments IACS security managemnt system - Implementation
Patch management	Asset Owner Service provider				IEC 62443-2-3	Patch management in the IACS environment
Security solutions implementation/realisation	Asset Owner Service provider				IEC 62443-3-1	Security technologies for IACS
Zones	Asset Owner Service provider				IEC 62443-3-2	Security assurance levels for zones and controls
Security auditing	Asset Owner Service provider				IEC 62443-3-3	Systemsecurity requirements & security assurance levels

Systematic Methodology

periodic

1) Map sector application to generic matrix model
2) Risk analysis of sector application map
   - o Identify and rate risk points
3) Determine appropriate level of CA for each risk point according to risk level rating
4) Identify requirements documents (standards)
   - o Determine what is available/appropriate
     → standards gap analysis
   - o Determine how to fill the gaps – SD
5) Apply appropriate CA to appropriate standards at each risk point

Revue, revise, renew (R3)

Next Steps

1) Validate the Generic Matrix Model (GMM) approach

2) Obtain sector-specific GMM
   - Critical infrastructure (Oil/gas, Nuclear, Electric grids, etc)
   - Railways
   - Cloud computing
   - Smart energy
   - Smart factory
   - Smart buildings

3) Develop risk analysis and ranking methods

4) TBD

Thank you

David Hanlon
IEC Secretary of the Conformity Assessment Board

UNECE WP.6
27th Annual Session
International Regulatory Cooperation
November 30th 2017, Geneva

INTERNATIONAL ELECTROTECHNICAL COMMISSION