



IEC's
understanding of
& activities in
cybersecurity
& how it applies to
critical
infrastructure

David Hanlon
IEC Secretary of the
Conformity Assessment
Board

IEA Digitalization and
Energy Workshop:
Digital Resilience
April 6th 2017, Paris

IEC INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

Good morning / afternoon.

My name is David Hanlon.

I am the Secretary of the IEC Conformity Assessment Board.

My presentation today is titled

IEC's understanding of and activities in cybersecurity and how it applies to critical infrastructure

Although that is rather a long title, I'll try to keep my presentation short and interesting.

IEC activities

International SD & CA



- Two pillars
 - The development of international standards in the electrotechnical sector
 - The operation of worldwide global CA Systems
 - certification schemes
 - IECEE (since the 1980s)
 - IECEQ (since the 1980s)
 - IECEX (since the late 1990s)
 - IECRE (since 2013)



Many of you may know the IEC as an international standards development organization.

And this is certainly true.

But IEC stands on two pillars, not only the development of international standards, but it also operates 4 worldwide global conformity assessment systems.

The IECEE, for certification of consumer and industrial products, IECQ, for business to business supply chain certification, IECEX, for certification of products, people and services in the explosive atmospheres sector, also known as HAZLOC areas, and our newest CA System, the IECRE, for renewable energies in the wind, marine and PV solar sectors.

Almost a million certificates have been issued through the IEC CA Systems, with more than 90'000 certificates currently being issued each year.

IEC ACSEC

Advisor Committee for Security



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

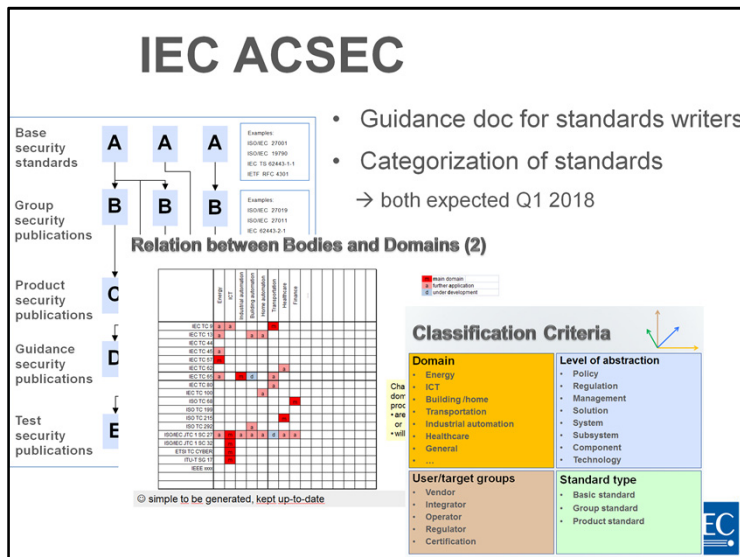


For the IEC cyber security became an important issue about 3 or 4 years ago.

On the standards development side an advisory committee on security, or ACSEC, was established to investigate the current situation of cybersecurity in international standards.

The initial investigation revealed a list of more than 650 standards containing cybersecurity elements,

developed by more than 50 standards development organizations including IEC, ISO, ITU, IEEE, CEN, CENELEC, ANSI, BSI, NIST, DIN, DKE, ETSI and about 40 more.



ACSEC was then given two tasks:

- Firstly it was to create a guidance document for IEC standards writers called IEC Guide 120 – Security aspects – Guidelines for their inclusion in publications
- And secondly it was to create a landscape view of all of the IEC standards mapped to a number of categories given in the guidance document.
The categories include the application domain, the user target group, the type of content, and so on.

Currently a draft of the guide has been written and has been through a first round of commenting.

It has yet to go through a number of editing and commenting rounds, and is expected to be completed in Q1 2018.

The mapping exercise is started, and is also hoped to be completed by Q1 2018.

IEC Conformity Assessment (CA)

2 initiatives



- **Operational Level**
 - IECEE global CA System
 - Cybersecurity scheme industrial automation
- **Helicopter Level**
 - CAB WG 17
 - understand current global situation concerning CA for cybersecurity.



On the Conformity Assessment side, two separate initiatives have been launched.

- Firstly, at an operation level, the IECEE is working to establish a cybersecurity certification scheme for the industrial automation sector.

It needs to be mentioned that all of the IEC CA services exist because the various market sectors requested those services. IEC only starts a new service if it is asked to do so.

The Industrial Automation sector asked the IECEE to create this scheme for it.

And IECEE is working with the Industrial Automation sector to fulfill their needs.

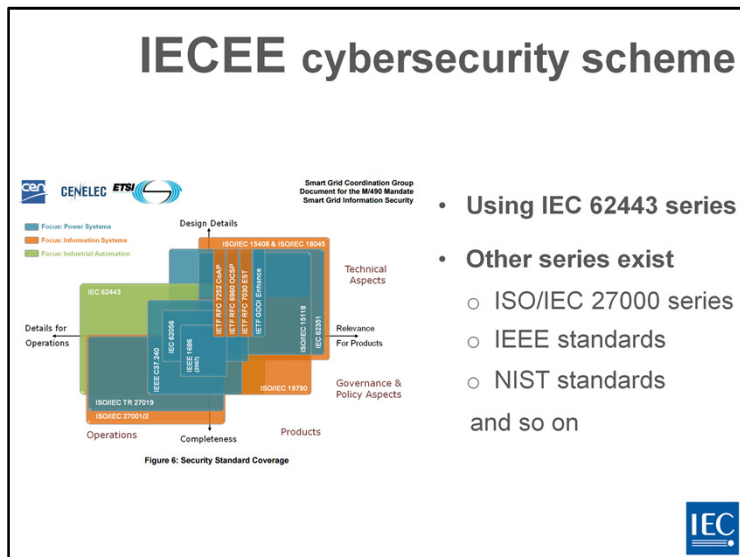
- Then the second initiative, at a helicopter level, a working group was established to try to understand the needs of cybersecurity on a global level across sectors. This is CAB WG 17.

IECEE cybersecurity scheme			
General	Policy & procedures	System provider / integrator	Component / Application (software) provider
✓ 62443-1-1 Terminology concepts and models	✓ 62443-2-1 IACS security management system - Requirements	✓ 62443-3-1 Security technologies for IACS	P 62443-4-1 Product Development Requirements
TR62443-1-2 Master glossary of terms and abbreviations	62443-2-2 IACS security management system - Implementation	P 62443-3-2 Security assurance levels for zones and conduits	P 62443-4-2 Technical security requirements for IACS components
62443-1-3 System security compliance metrics	✓ 62443-2-3 Patch management in the IACS environment	✓ 62443-3-3 System security requirements & security assurance levels	
62443-1-4 IACS security and lifecycle use cases	✓ 62443-2-4 Requirements for IACS solution suppliers	13 Total Deliverables ✓ - 6 Available Today P - Priority development	

To put in place a global cybersecurity certification system for the Industry Automation sector, the IECEE is working with the IEC 62443 series of standards.

This is a series of standards that covers security requirements for providers of integration and maintenance services for Industrial Automation and Control Systems (IACS).

The entire series is expected to contain 13 standards, of which 6 are available today, while three others are being developed in priority.



The IECEE is using the IEC 62443 series for its global cybersecurity conformity assessment system.

But the IEC 62443 series is not, of course, the only series of standards that covers a full range of cybersecurity issues.

The ISO/IEC 27000 series also cover cybersecurity, but they are more focused on information technology infrastructures. Then there are IEEE standards and NIST standards, and so on.

It's also true that there is much overlap between all of these standards series.

And this is perhaps the most important understanding to come out of the other IEC conformity assessment initiative.

Helicopter view

Systems = Systems



- **A system**
 - Elements
 - interacting, interacting, interdependent
 - physical and/or virtual
 - Confined or dispersed
 - Need occasional repair, replacement update, upgrade
 - many transmit & receive information
 - Forming purposeful whole
 - Periodic or constant modification
 - by virtual, automated or human intervention



The second conformity assessment initiative for cybersecurity was a helicopter view of cybersecurity needs across application and market sectors.

What this group found, across applications and sectors, was that the needs are very similar.

It also realized that the root cause of this was simply because all technical systems are very similar.

If we consider a system to be a group of interacting, interrelated, or interdependent elements forming a purposeful whole, and that those elements can be physical and/or virtual, and that they can be confined to a limited physical location, or spread out over a large physical distribution, and that they need periodically to be repaired, replaced, updated or upgraded, and that many of those elements transmit and receive information between themselves and are, or could be, in some way connected to the internet, and that the whole system itself is periodically or constantly undergoing modification and development through interventions that could be virtual, automated or human, then, the needs for cybersecurity protection of systems become pretty generic.

Helicopter view

Systems = Systems



- **Cybersecurity Systems**
 - Components
→ physical or virtual
 - Interconnections
→ systems integration
 - Information flows
 - Interventions
→ human, virtual or automatic
- **Best cybersecurity**
= **best practices at all levels**
→ CA at all levels

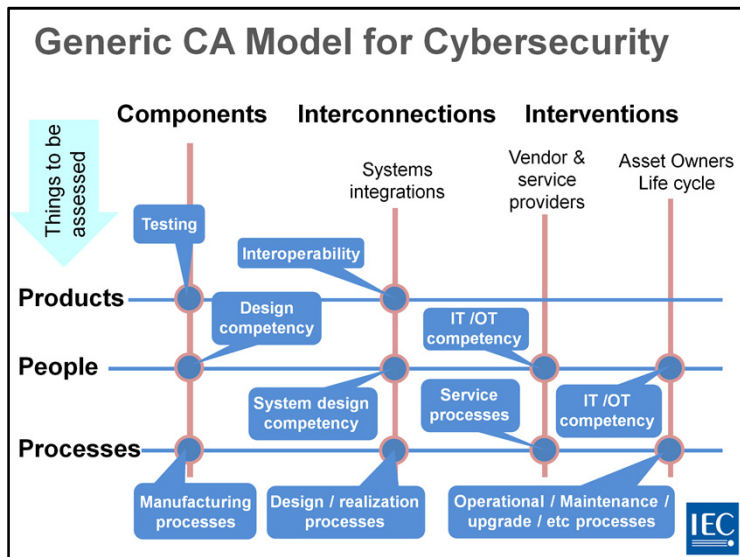


Generically speaking, the systems that concern us for the issue of cybersecurity are made up of components (which can be physical or virtual), interconnections (the systems integration), information flows, and interventions (which can be human, virtual or automatic).

To ensure best cybersecurity coverage for the system as a whole, best practices need to be applied for each of these elements.

The way to ensure the application of best practices is through the assessment of the conformity to those best practices.

For this reason the group developed a generic conformity assessment model for systems.



All technical systems consist of components, interconnections (also known as systems integration), and interventions (which can be human, virtual or automatic).

Interventions can be such things as building the system, or operating the system, maintaining the system, or providing services for the system, and so on.

Conformity assessment simply means assessing the conformity of something, to some agreed requirements.

The something, which is referred to as the object of conformity, can be components or products, or can be people, or can be processes.

Conformity assessment, occurs at the intersections, of the horizontal and vertical perspectives.

And systems conformity assessment is the overall matrix of CA activities.

For example, in the case of components, they can be tested against a standard, but so can the manufacturing process, to ensure that the components are always built to be conformant.

And even before this, the design process for the component can be assessed and approved as can the competencies of those doing the designing.

At the systems integration level, design and implementation processes need to be followed correctly by people with the appropriate competencies.

And at the Asset Owners level, correct operating procedures, maintenance procedures, enhancement procedures, and so on, by qualified persons, need to be ensured.

This is how conformity assessment of an entire system is done.

Generic CA Model for Cybersecurity				
	A Component	B System integration	C Vendor	D Life cycle
1	Product hardware software/ firmware information This cell: CA requirements for the products themselves (may depend on the application of the component, eg. use in household office may have lower requirements than use in a nuclear power plant – ie: sector specific), including: • SDLC • Simple type-testing • Type 5 certification • Known threat testing/protection • Confirmation of SDLC requirements • Other	This cell: Any systems requirements on products (HW, SW, FW information), including: • Component interoperability testing • Identity management • Information security • Confirmation of SDLC requirements • Other		
2	People (personal competency) This cell: People competencies covering the cybersecurity aspects of component design and manufacture, including: • Design competencies (HW, SW, FW + ITT) • Manufacturing competencies • Other	This cell: People competencies covering the cybersecurity aspects of system design and system build, including: • System design competencies • System build competencies • IT security competencies • OT security competencies	This cell: People competencies in cybersecurity required for outsourced vendor services, including: • IT security competencies • OT security competencies	This cell: People competencies covering the cybersecurity aspects during system operation, including: • IT security competencies • OT security competencies
3	Process (can include services) This cell: Processes needed to ensure that a component is supplied with the required level of cybersecurity integrity, including: • Design processes • Manufacturing processes • post-manufacturing processes (ie. ensuring protection from latest known threats when coming from stock) • Other	This cell: Processes needed to ensure that a system is designed & built with the required level of cybersecurity integrity, including: • Design processes • Realisation (building) processes • Other Process(es) to assess the completed cybersecurity solution for the system, • system commissioning • other	This cell: Processes needed by vendors and service providers to ensure that system cybersecurity integrity is maintained during and after those services.	This cell: Processes needed to ensure that a system is operated in a way that maintains its cybersecurity integrity throughout its lifetime, including: • Operating processes • New threat updating processes • System maintenance processes • System evolution / expansion / decommissioning processes • Supply chain & supplier/vendor qualif • Cyber incident management processes • Other Process(es) for periodic assessment or ongoing approval or certification of the cybersecurity solution for a system. This is basically assessing all (or some) of the processes indicated above.

This is the same model but showing a little more detail.

Helicopter view

Some Systems $\neq$ Systems



- **Smart Grid**
 - No single Asset Owner
 - Every home with a PV panel & smart meter
 - Upgrade resilience for new threats ?
 - System continually changing
 - Homes & buildings being demolished
 - New homes & building being built
 - Neighbourhoods expanding & contracting
 - New equipment replacing old
 - New technology replacing old



A particular issue with electrical energy distribution systems, that will become more and more problematic, is that {click} there is no single asset owner.

For example the smart grid.

The smart grid will have many many owners.

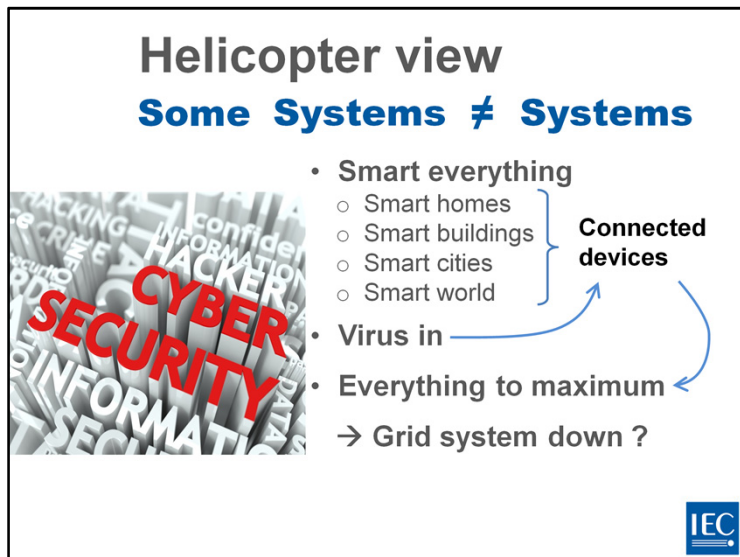
Each house with a PV panel on its roof, and a smart meter, will be one of many joint owners of the system.

How will all those smart meters be kept up to date, and resistant, to evolving cyber threats ?

Additionally, the smart grid will be a living system.

It will be continually changing as buildings get torn down, new ones are constructed and neighborhoods expand or contract.

How can the integrity of the entire system be assured ?



And as a final question to reflect on,

As our homes, building and cities all become smart, with many components, devices and equipment, including industrial and consumer products,

And all of these components and devices and equipment can all be monitored and controlled remotely,

Imagine if all of these components were to be infected by a virus and a hacker could switch everything on, or to a maximum power level, all at the same time.

Would this bring down the grid system ?

Does this mean that critical systems for electrical energy, cannot be protected unless all connected devices are cyber safe ?



Thank you

David Hanlon
IEC Secretary of the
Conformity Assessment
Board

**IEA Digitalization and
Energy Workshop:
Digital Resilience**
April 6th 2017, Paris



INTERNATIONAL
ELECTROTECHNICAL
COMMISSION