

A close-up, profile view of a woman with long, dark brown hair, looking slightly downwards and to the right. The image is positioned on the left side of the slide, partially overlapping a vertical green and pink bar.

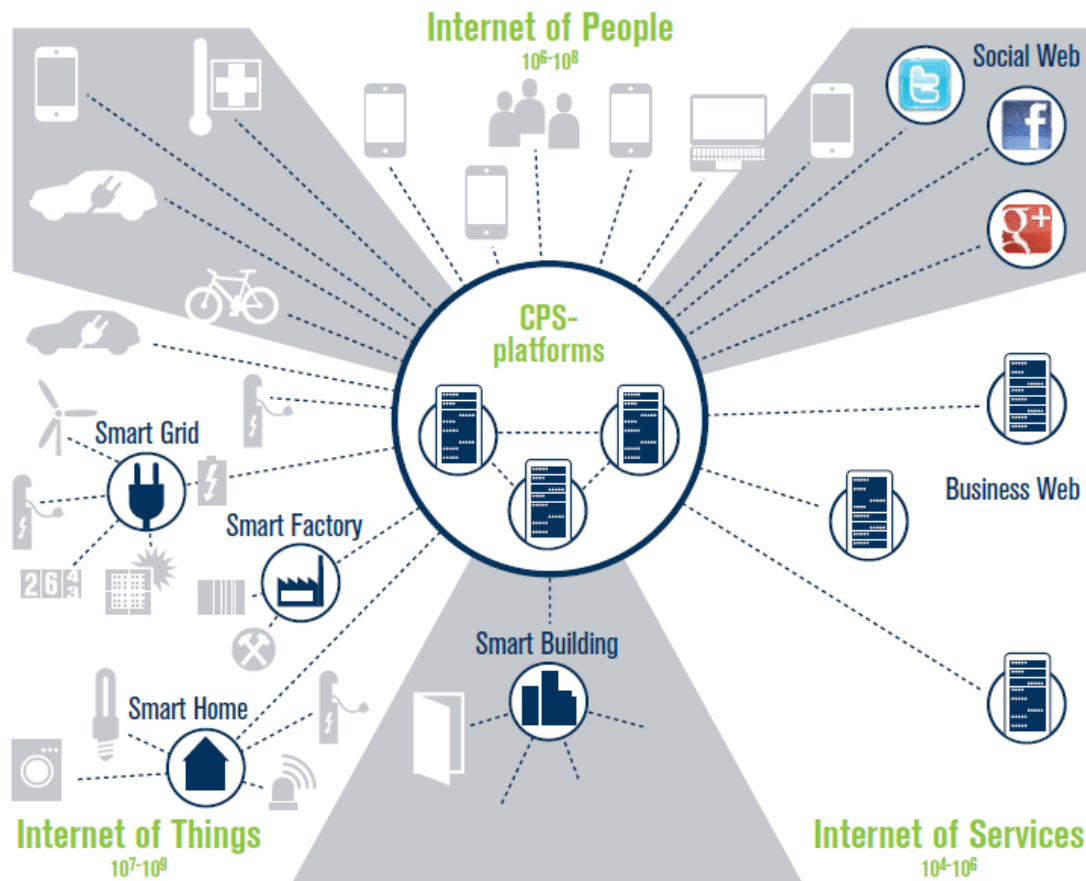
No Doubt.

Cyber Security is essential

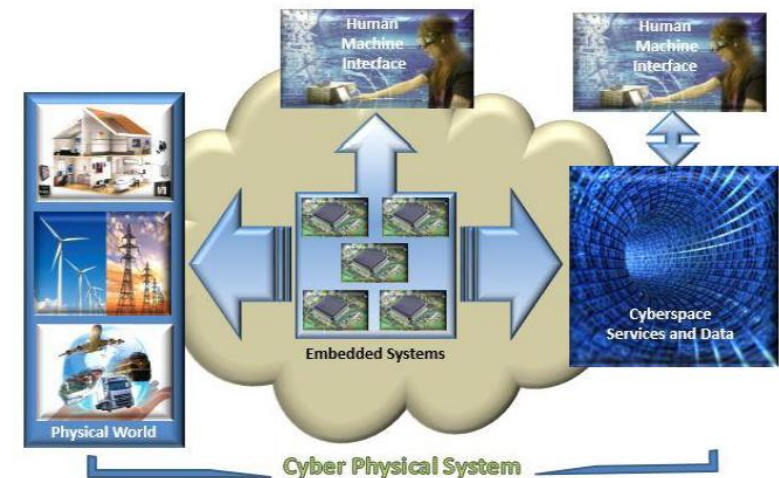
DEKRA Certification Group

Beat.Kreuter@dekra.com

Industry 4.0 and Internet of Things

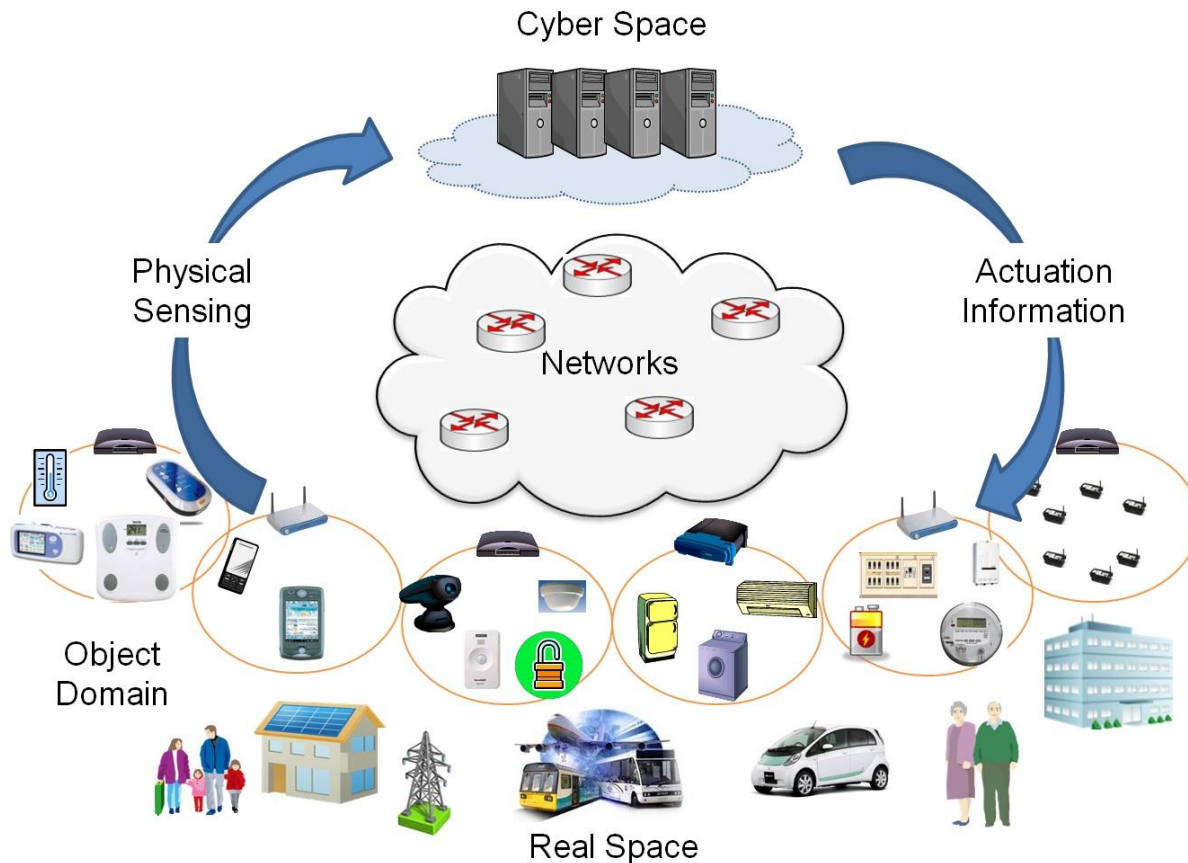


- Link sensors, actuators, wireless technologies, the internet, and merge the physical things with the virtual things to create a cyber physical system



Source: report Cyber-Physical Systems: Uplifting Europe's Innovation Capacity

Industry 4.0 and Internet of Things



Essential success factors

- Safety
- Interoperability
- Security

Customer Experience !!!!

ICS Cyber Security regulations United States

- The presidential Executive Order 13636 from February 2013, called for the development of a Cybersecurity Framework to enhance the security and resilience of the Nation's critical infrastructure



Source: securityaffairs.co/wordpress/29977/cyber-warfare-2/russia-hacked-us-critical-infrastructure.html



Chemical



Financial service



Commercial facilities



Food and agriculture



Communication



Government facility



Critical manufacturing



Healthcare and public health



Dams



Information technology



Defense industry



Nuclear reactors, materials and waste



Emergency service



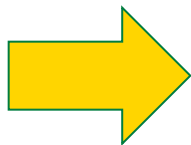
Transportation



Energy



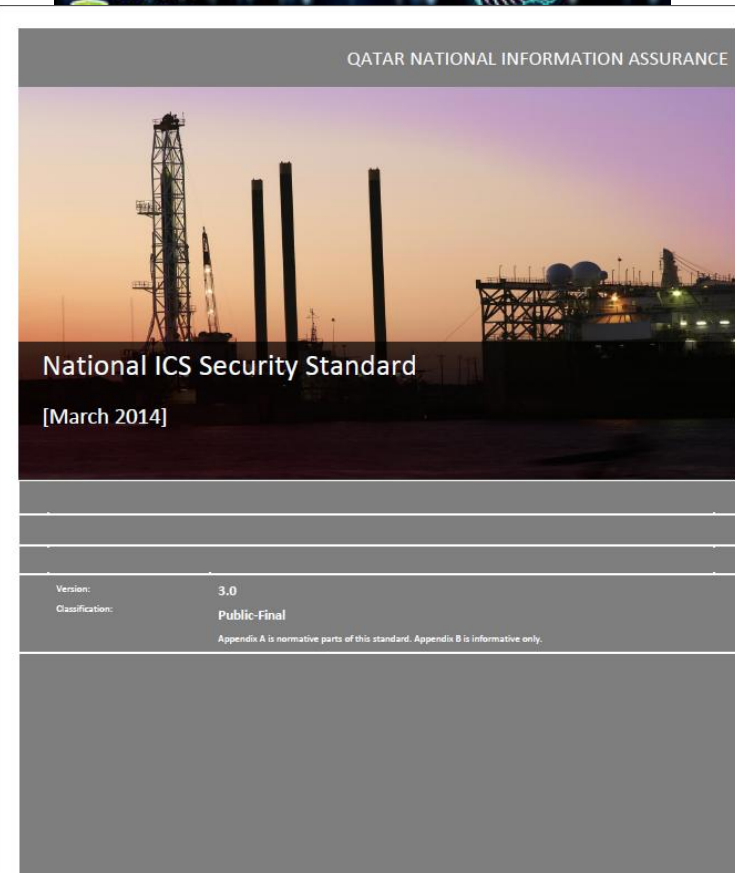
Water and waste water systems



- National Framework for Improving Critical Infrastructure Cybersecurity 1.0 has been release on Feb. 2014. and maps security requirements to various available national and international standards

ICS Cyber Security regulation in Qatar

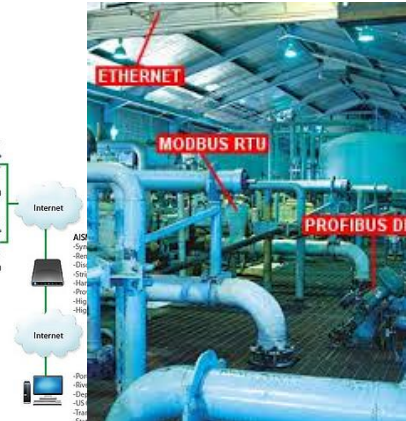
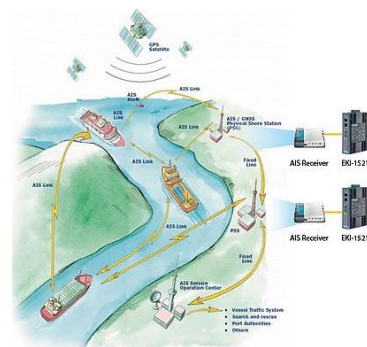
- On March 2014, Qatar has published its National Standard ICS security standard – the standard defines management of cyber security and provides for specific technical requirements for ICS network architecture and devices connected to those networks.
- E.g. Wireless devices should be avoided in critical ICS systems – and if wireless devices are being used then ISA100a, IEC 62591 (wireless HART) are to be used.
- ICS related protocols such as MODBUS, Ethernet/IP and DNP3 shall only be allowed within ICS networks and not allowed to cross into corporate networks



European Union – ICS Cyber security



- In 2013 the EC published COM(2013) 48 - Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union
- This directive called NIS (Network and Information Security) but frequently referred to as Cybersecurity Directive essentially establishes security requirements for market operators



Cyber Security in different industries

- Many economies prepare regulations
- Many industry sectors work on sector specific standardization and guides (e.g. IHE - Medical Device Cyber Security – Best Practice Guide – SAE - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems SAE J-3061, etc.)
- Few international standards addressing industrial control systems e.g. IEC 62443 series of standards
- Few international standards addresses ICT (ISO 15408 or CC)
- Few testing and certification schemes mostly regional or by country

Cyber Security Certification Schemes

- **Name: Achilles**
- **Scope: Industrial Controls System**
- **Participants: Global**
- **Achilles Communications Certification (industrial control products)**
- **Achilles Practices Certification (solutions, people and process)**
- **Certification by: Wurldtech, DEKRA**



wurldtech
A GE Company



- **Name: CSPN (Certification de Securite de Premier Niveau)**
- **Scope: IT products, ICS (PLC, firewall, VPN gateway, switch)**
- **Participants: France**
- **Derived from Common Criteria but more time and cost optimized**
- **Certificates issued by: Agence nationale de la sécurité des systèmes d'information (ANSSI)**



Cyber Security Certification Schemes

- **Name: Common Criteria**
- **Scope: IT equipment, smart cards, network devices , access control devices etc.**
- **Participating countries: 26**
- **Issuing and accepting certificates**
- **Accepting certificates only**



- **Name: ISA secure**
- **Scope: Embedded devices**
- **Participants: US, Japan**
- **On the basis of IEC 62443**
- **Certification : ISASecure**

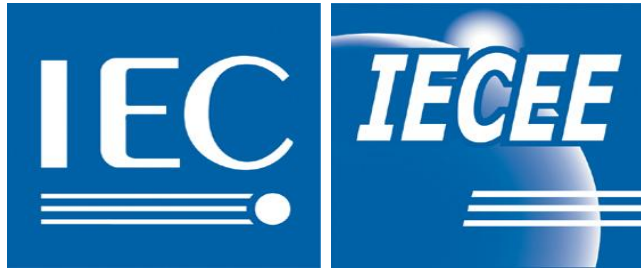


The role of standardization in global trade

Standards play an essential part in global trade, standards in particular do;

- **harmonize terminologies,**
- **harmonized flow of information,**
- **address particular risks of processes, products and raw materials**
- **promote research and innovation,**
- **promote best practises**
- **promote self-regulation of actors**
- **guarantee that products comply for minimum safety und quality requirements (if applied)**
- **provide for compliance means against regulatory requirements**
- **provide and harmonize methods for testing**
- **eliminate technical barriers**

Cyber Security Certification of Products, Processes, and People



- The International Electrotechnical Committee – Conformity Assessment Board (IEC CAB) is working on a global Cyber Security Assessment/Testing and Certification scheme for products, supplier/integrators and operators/asset owners using the well accepted IECEE Testing & Certification platform. The Cyber Security program is based on IEC 62443 series of standards.
- The IECEE CB Conformity Assessment Program is a globally accepted assessment/testing/certification scheme with presently 58 countries participating
- The program provides for 3rd party evidence that devices, systems and procedures conform to industry proposed technical requirements which have been reached through mutual and international consent and laid down in a international standard -