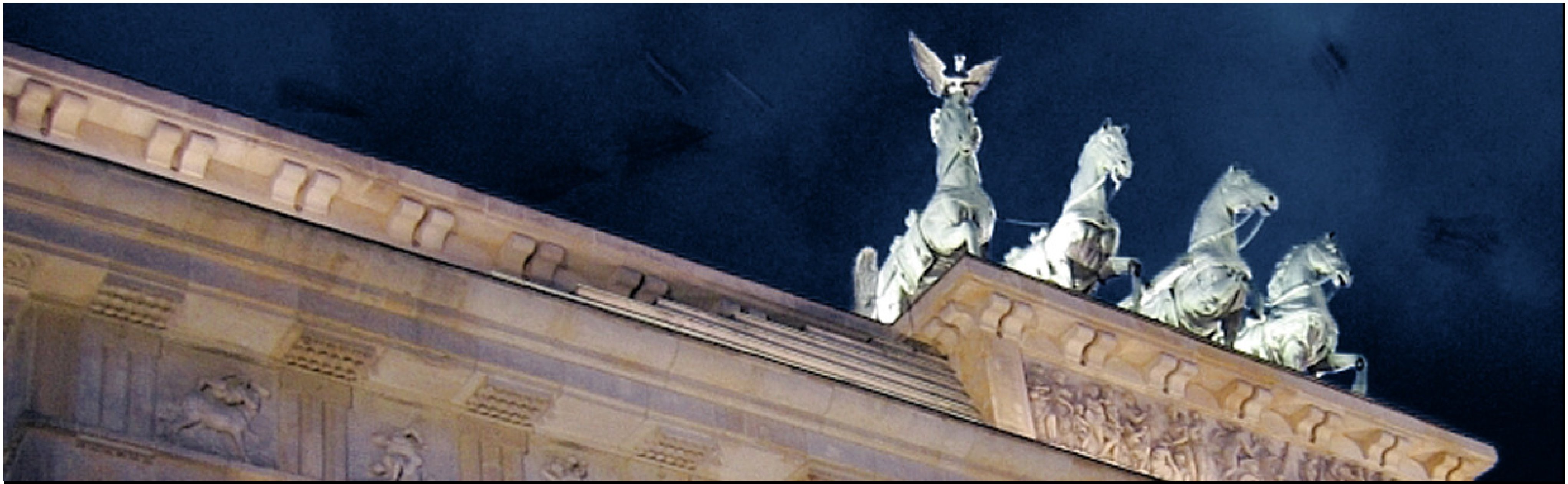


Gerhard Brandt, ABB AG , BU Power Generation

Cyber Security and Compliance in Increasingly Distributed and Aging Power Generation Infrastructures

A global leader in power and automation technologies
Leading market positions in main businesses

- 145,000 employees in about 100 countries
- $38 billion in revenue (2011)
- Formed in 1988 merger of Swiss and Swedish engineering companies
- Predecessors founded in 1883 and 1891
- Publicly owned company with head office in Switzerland

How ABB is organized
Five global divisions

Power Products	Power Systems	Discrete Automation and Motion	Low Voltage Products	Process Automation
$10.9 billion	$8.1 billion	$8.8 billion	$7.7 billion	$8.3 billion
36,000 employees	20,000 employees	29,000 employees	31,000 employees	28,000 employees

(2011 revenues, consolidated; including Thomas & Betts revenue for LP division)

- ABB's portfolio covers:
  - Electricals, automation, controls and instrumentation for power generation and industrial processes
  - Power transmission
  - Distribution solutions
  - Low-voltage products
  - Motors and drives
  - Intelligent building systems
  - Robots and robot systems
  - Services to improve customers productivity and reliability

Power and automation are all around us
You will find ABB technology…

orbiting the earth and working beneath it,

crossing oceans and on the sea bed,

in the fields that grow our crops and packing the food we eat,

on the trains we ride and in the facilities that process our water,

in the plants that generate our power and in our homes, offices and factories

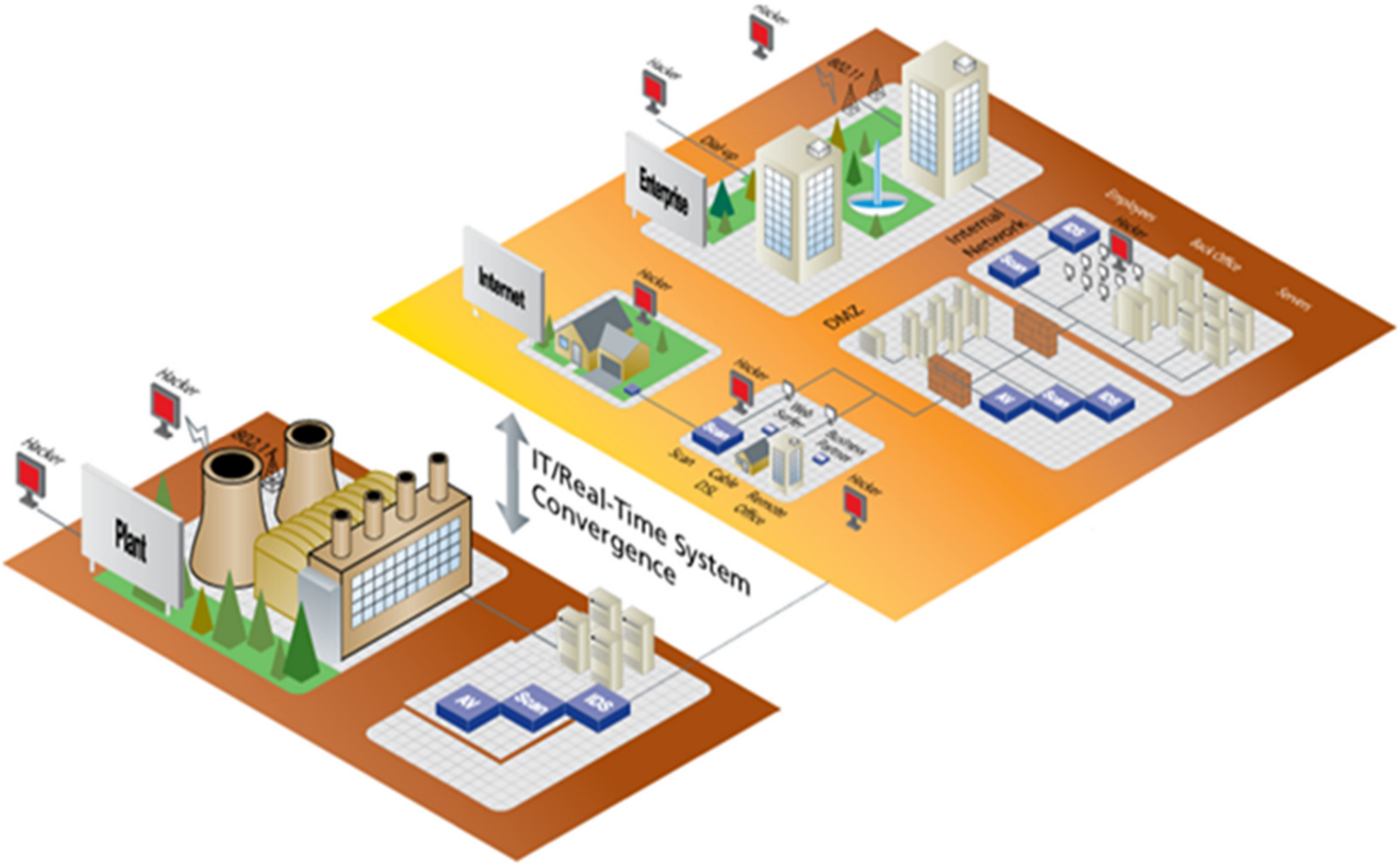
Situation of today

- The potential threat for IACS during the years 2010 and 2011 has increased significantly and today authorities like the German BSI (Bundesamt für Sicherheit in der Informationstechnik) note, that professional attacks from organized crime and intelligence agencies on industries, authorities and private individuals are a common fact. The methods and techniques involved get increasingly complex and sophisticated, resulting in growing effort and cost for the defense. Trojans like Stuxnet demonstrate, that IACS and SCADA systems are in the focus of such activities. The most effective means still being prevention.
- The legal status throughout Europe is still heterogeneous, as no common binding guidelines exist. However existing regulations resulting from various laws (e.g. in Germany SOX, HGB, AktG, KonTraG) indirectly demand corporations and individuals to take adequate organizational and technical precautions (obligation to exercise due care, risk management, liability for premises) as neglect may cause indemnification claims.
- IACS = Industrial Automation and Control System

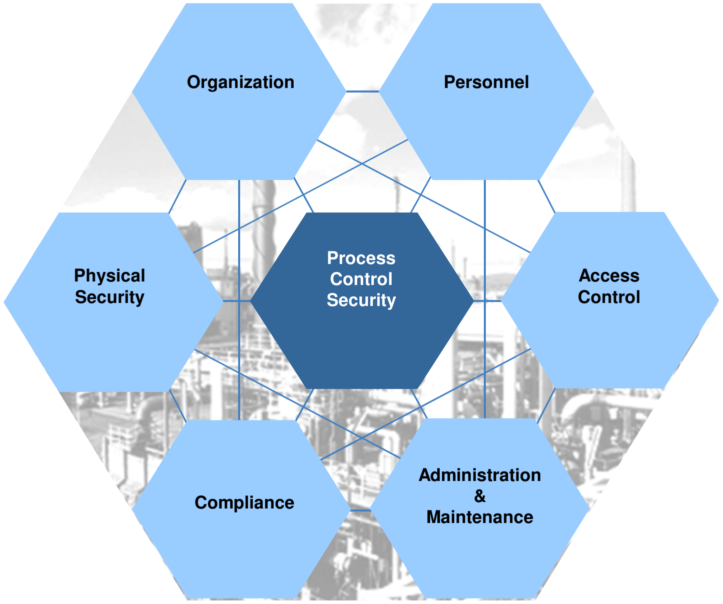
Anticipated development (1)

- International, European and national standardization activities converge and a set of binding guidelines for suppliers, service providers as well as operators in Europe is on the horizon. On global scale the standards SO/IEC 27001 and 27002 are getting established and specifically for industrial automation ISA99 / IEC62443.
- The German government (BMI, ministry of interior) intensifies its activities with focus on “critical infrastructures” (kritische Infrastrukturen, KRITIS). These are defined as infrastructures whose failure would have a sustained impact on the security of supplies with considerable effect on public safety and other dramatic impacts.

Focus on Cyber Security solutions



Aspects of information security (1)



- **Organisation (ISMS)**
  - Proesses, responsibilities, security concepts, awareness and training of staff,
- **Physical safety**
  - Security zones, access control, safety of
- **System security**
  - System documentation (like project manual, maintenance manual, backup manual)
  - System architecture, security zones
  - Redundancy, availability, system hardening (DMZ)
- **Network security**
  - Network interfaces, firewalls, local and remote address management, Remote Access
  - WLAN, Mobile Computing, Intranet/Internet

Aspects of information security (2)

- **Operations and communications management**
  - Protections from malware and trojans, vulneraribility management (e. g. closing of USB ports), user and rights management, handling of storage media
  - Access to network, operating system and applications (local and remote access)
  - Monitoring and diagnosis
- **Safeguarding of business operations**
  - Data security and integrity (backup / restore)
  - disaster recovery
  - Handling of information security cases
- **Compliance**
  - Manual and automated logging and protocols of conformity with rules and guidelines as audit preparation (audit trail)
  - audits

Technical challenges
Meeting a unique set of requirements

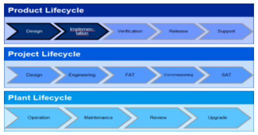
	Enterprise IT	Industrial Control Systems
Object under protection	Information	Physical process
Risk impact	Information disclosure, financial loss	Safety, health, environment, financial
Main security objective	Confidentiality, Privacy	Availability, Integrity, Privacy (SmartGrid)
Security focus	Central Servers (fast CPU, lots of memory, …)	Distributed System (possibly limited resources)
Availability requirements	95 – 99% (accept. downtime/year: 18.25 - 3.65 days)	99.9 – 99.999% (accept. downtime/year: 8.76 hrs – **5.25 minutes**)
System Lifetime	3 – 10 Years	5 – 25 Years

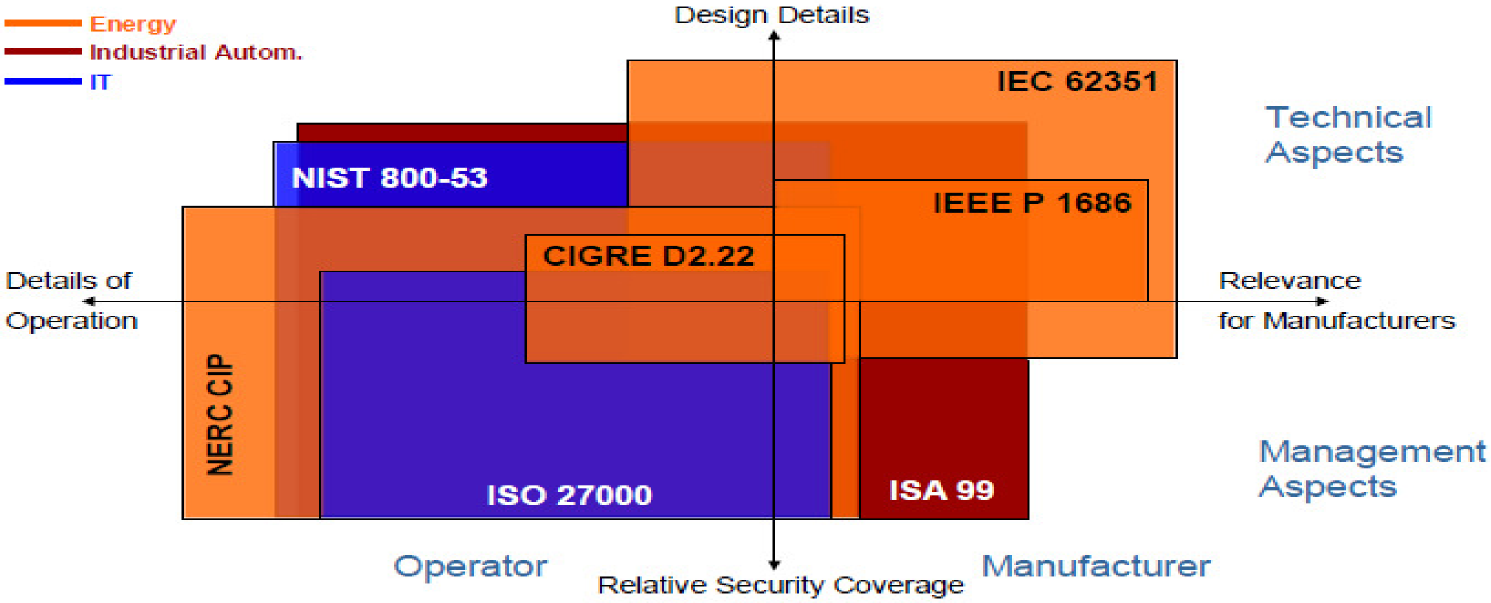
Anticipated development (2)

Standard	**Main focus**
NERC CIP	Cyber security regulation for North American power utilities
IEC 62351	Data and communications security
IEEE PSRC/H13& SUB/C10	Cyber security requirements for substation automation, protection and control systems
IEEE 1686	IEEE standard for substation intelligent electronic devices (IED´s)
IEC 62443	Industrial communication networks – Network and system security (DRAFT)
ISO-IEC ISO/IEC 27000-series (27001, 27002 / 17799)	Information technology - Security techniques - Code of practice for information security management.
ISA-99	Security for Industrial Automation and Control Systems

- Selected international standards and initiatives in the German market some de-facto standards establish themselves amongst involved parties

Product Lifecycle - Design & Implementation
Standards and their scope





- Graphical representation of scope and completeness of selected standards

*) source DTS IEC 62351-10 10: Security architecture guidelines

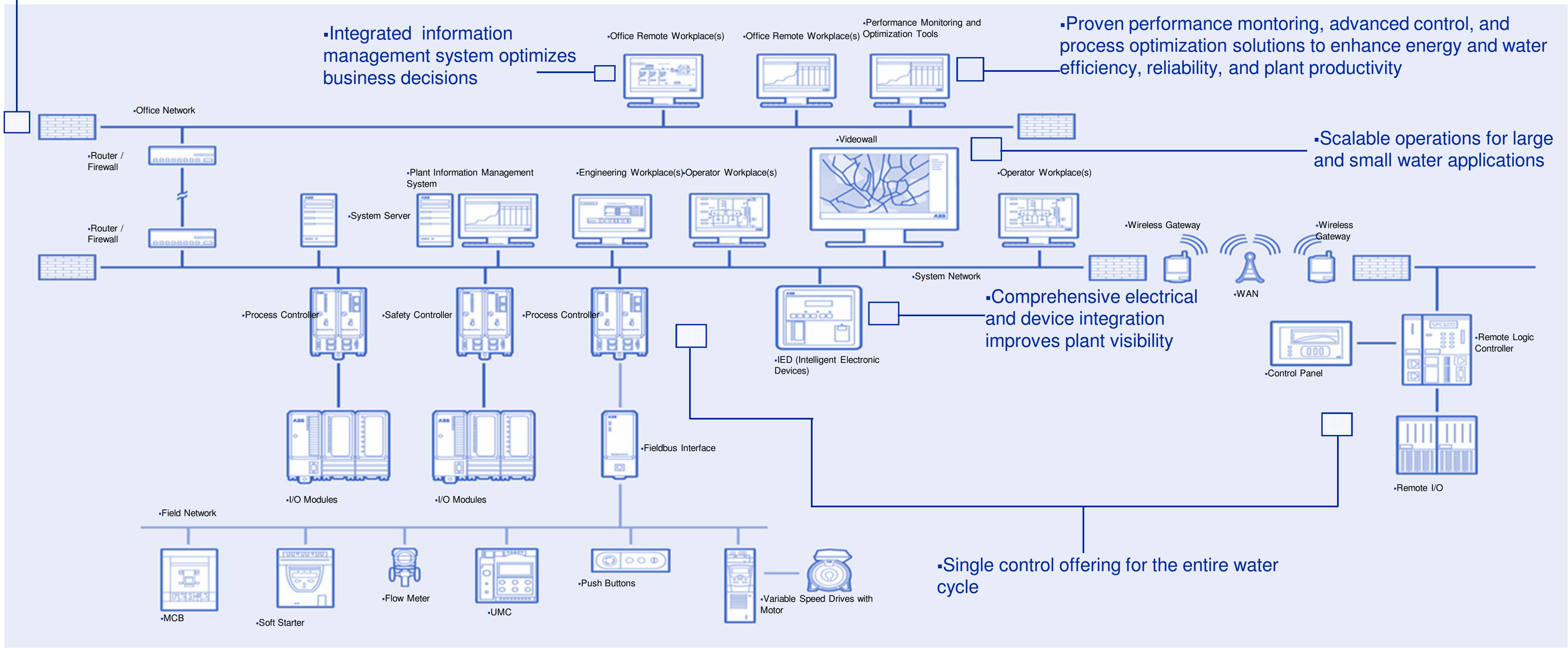
Anticipated development (3)

Standard	Main focus
BDEW Whitepaper (bdew, Vattenfall, e.on, EnBW, itecPlus)	”Anforderungen an sichere Steuerungs- und Telekommunikationssysteme” (requirements on safe control and communications systems)
VDI/VDE guideline 2182	„Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell" (information security in industrial automation – general process model)
VGB Powertech technical guideline R175	„IT-Sicherheit in Erzeugungsanlagen“ (IT security in power generation plants)

- Selected German guidelines and initiatives
- Once a binding set of standards is established, operators and suppliers of products and solutions may strive or be forced for a certification of information security. In the German markets such a direction from BSI as well as TÜV can be noticed.

Symphony Plus
Typical system architecture

Inherent system security ensures plant integrity and confidentiality



▪Integrated information management system optimizes business decisions

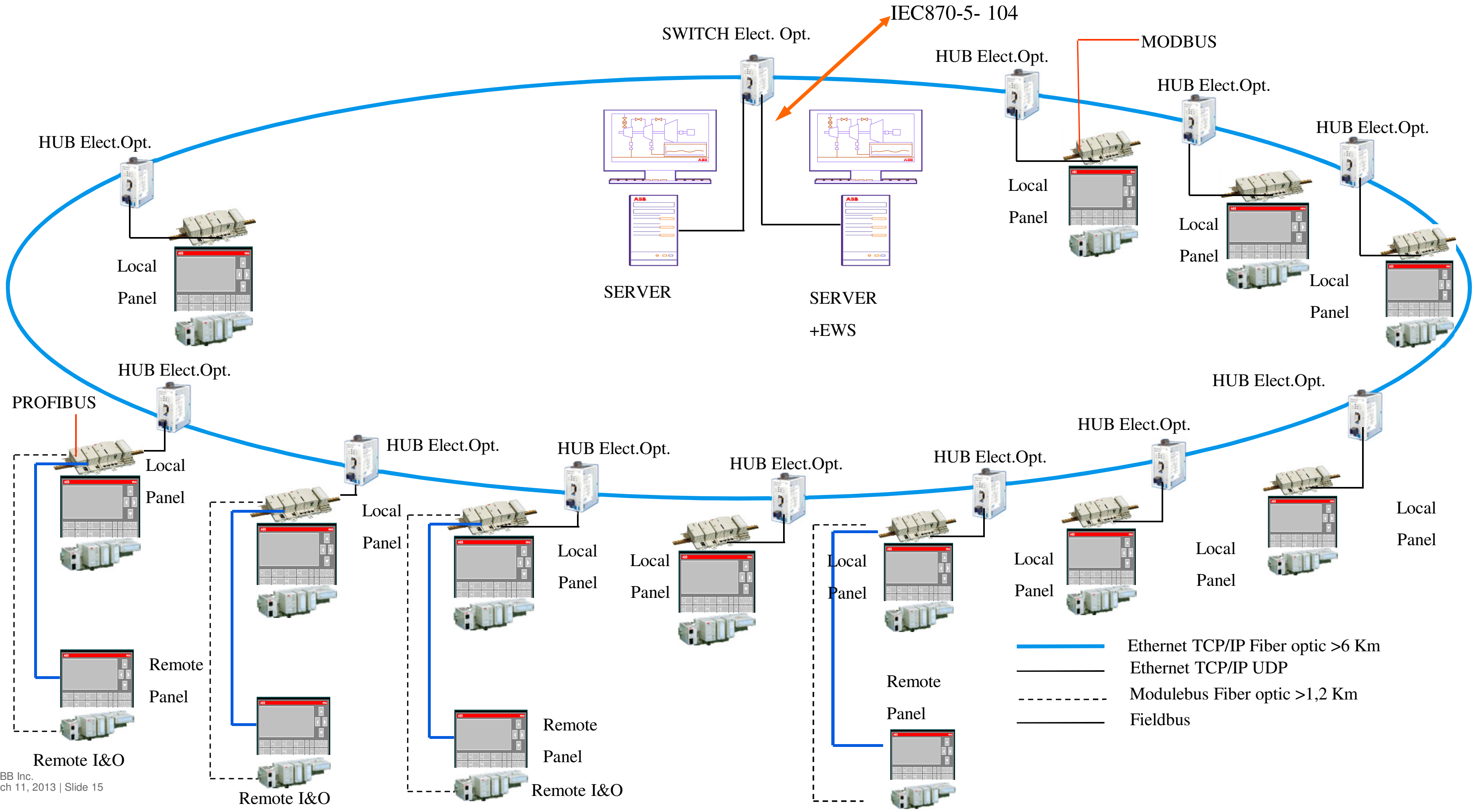
▪Proven performance montoring, advanced control, and process optimization solutions to enhance energy and water efficiency, reliability, and plant productivity

▪Scalable operations for large and small water applications

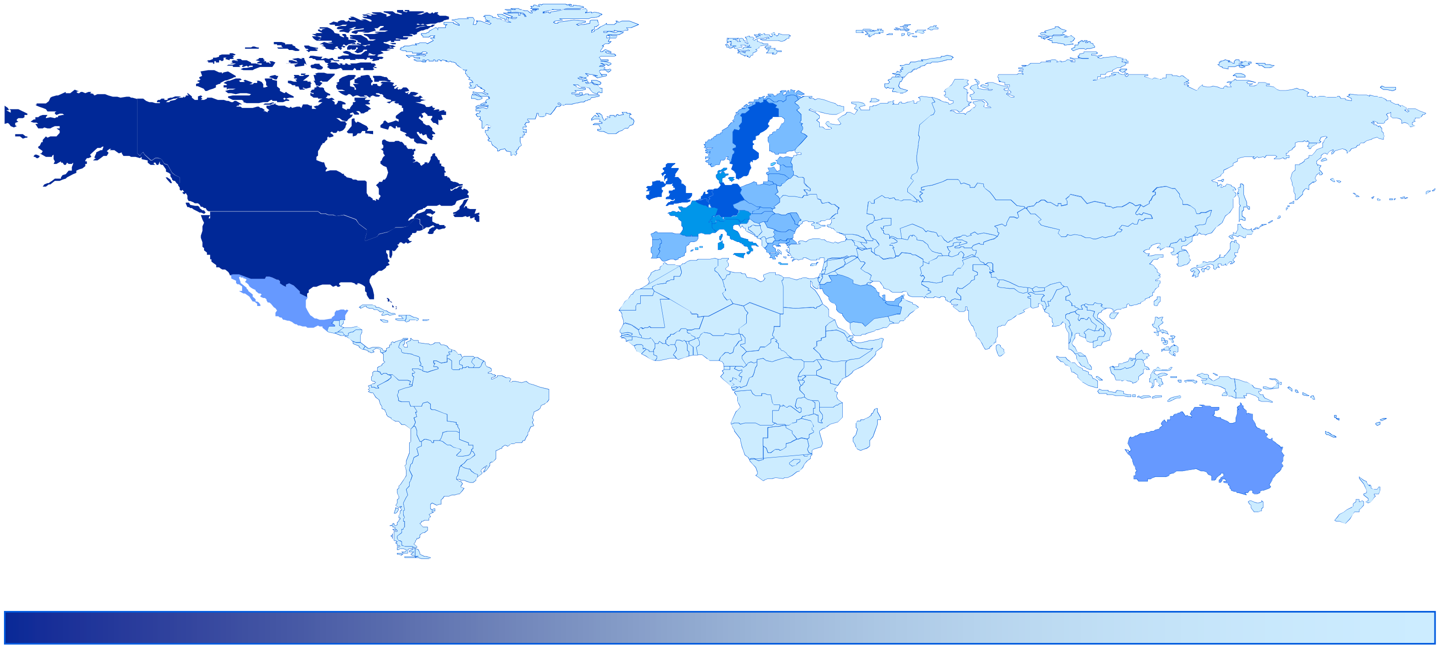
▪Comprehensive electrical and device integration improves plant visibility

▪Single control offering for the entire water cycle

SCADA architecture examples: hydro power control



Global cyber security demand
The ABB perspective

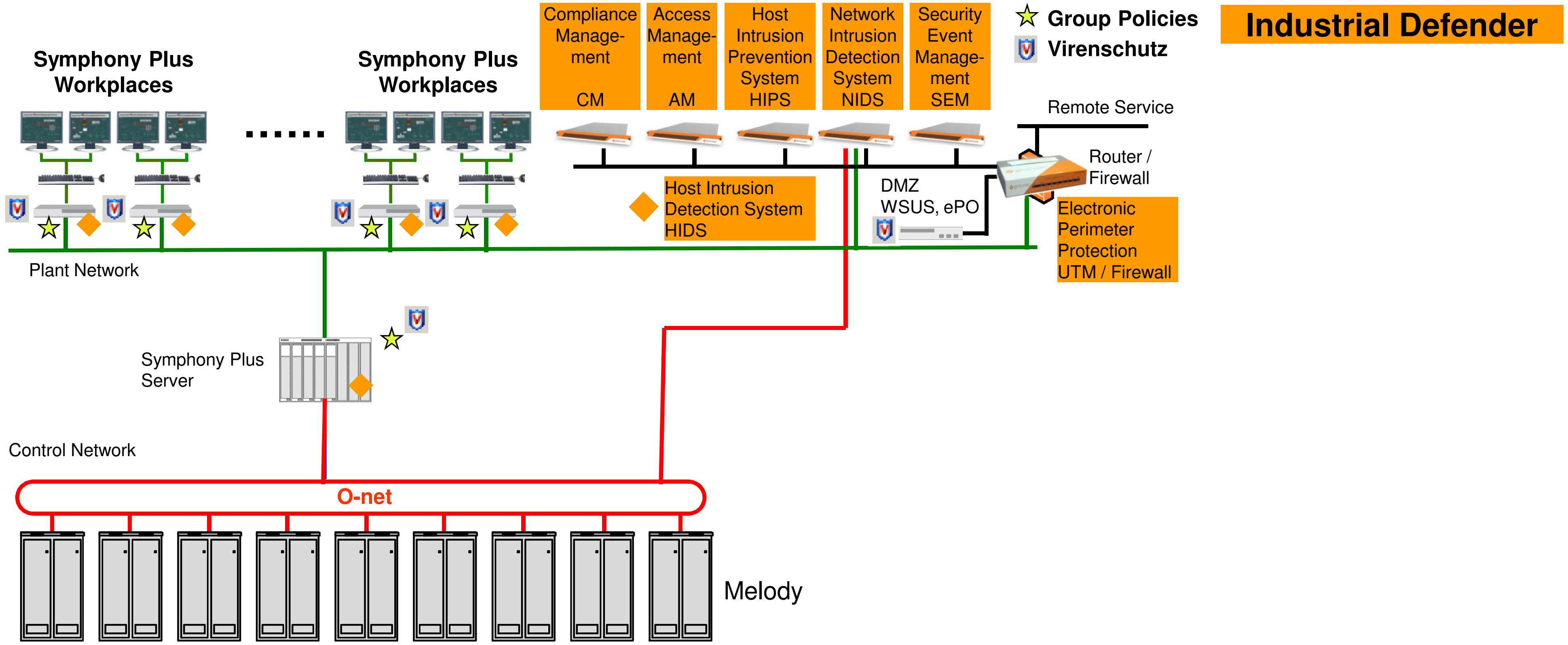


High demand seen by ABB,
requirements clear

Little demand seen by ABB,
requirements unclear-> India?

Map does not reflect global players such as BP, ExxonMobil, Shell, Daimler

Application example Symphony^{TM} Plus



Cybersecurity as example of association work

- Multiple stakeholders from utility, industry, manufacturer, government
- Multiple, competing standards
- Multiple disciplines (automation, corporate IT, operations, security, …)
- Unclear cost / benefit analysis
- Industry specific appplication guidelines useful
- Definition of minimum requirements
- Technical issues (how to handle old, installed base)
- Share best prectices
- Example: VGB 175

Cybersecurity as example of association work (deliverables)

- Guideline, recommendation, whitepaper
- Consulting and services
- Training
- Auditing and certification (technology, processes, organization, staff)
- Representation and lobbying in other institutions, assocations, governmental organization
- Collection and documentation about existing technology, use cases, etc

Power and productivity
for a better world™