SIEMENS
Ingenuity for life

Driving security in an unsecure world

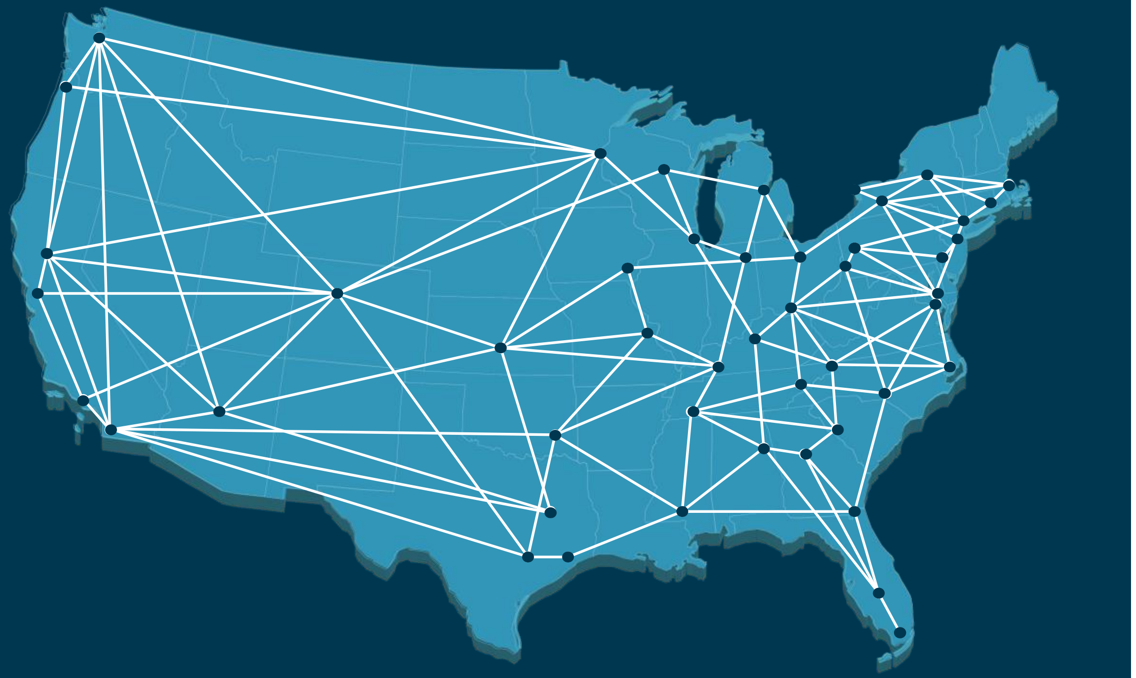
NIST Cybersecurity Risk Management Conference

Leo Simonovich | Nov. 7, 2018 | Baltimore, MD USA

charter-of-trust.com | #Charter of Trust

SIEMENS
Ingenuity for life

Siemens in the U.S. – Our company at a glance



Map shows Siemens' **major employment hubs**

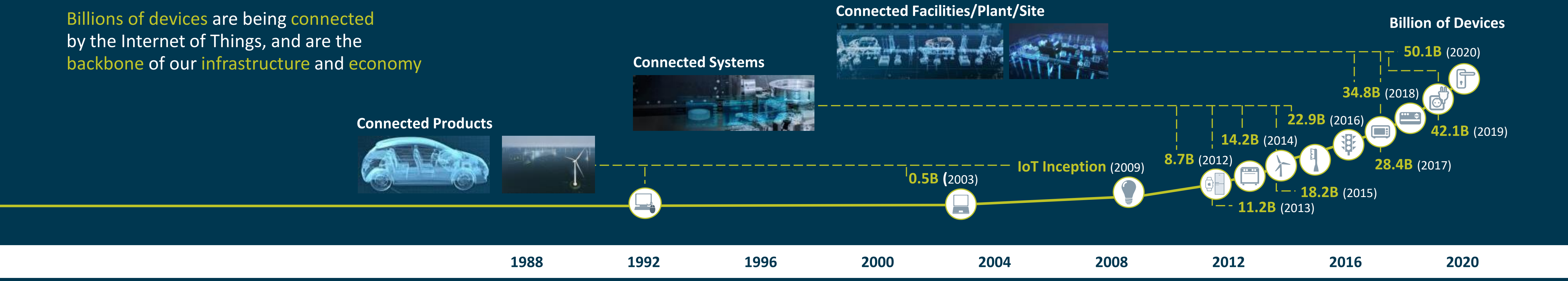
- **60+** manufacturing sites and **50,000** employees
- Over **$5 bn** in exports annually
- **~$40 bn** invested in the U.S. in last 15 years
- **$50 m** job training programs annually
- **$1 bn** annual R&D investment
- **800,000 jobs** linked to Siemens' global business operations in FY15

Digitalization creates opportunities and risks

Digitalization creates …

Opportunities

Billions of devices are being connected by the Internet of Things, and are the backbone of our infrastructure and economy



Connected Products

Connected Systems

Connected Facilities/Plant/Site

Billion of Devices

0.5B (2003)

IoT Inception (2009)

8.7B (2012)

11.2B (2013)

14.2B (2014)

18.2B (2015)

22.9B (2016)

28.4B (2017)

34.8B (2018)

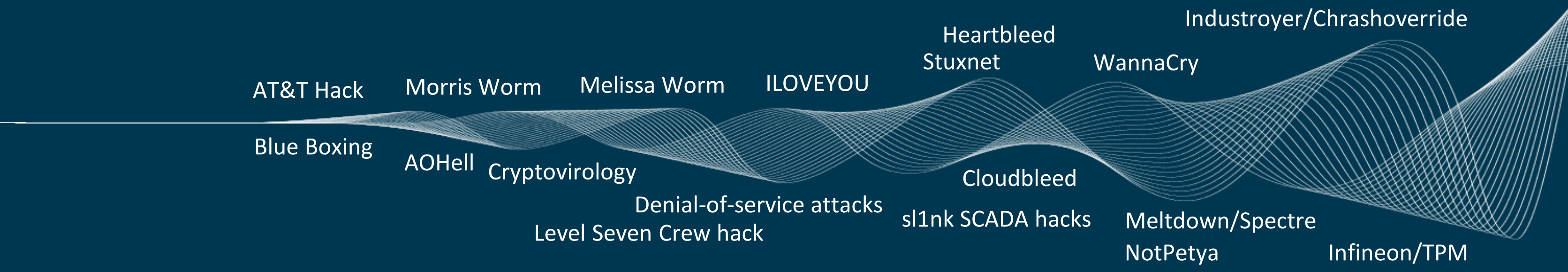
42.1B (2019)

50.1B (2020)

1988 | 1992 | 1996 | 2000 | 2004 | 2008 | 2012 | 2016 | 2020

… and risks

Exposure to malicious cyber attacks is also growing dramatically, putting our lives the stability of our society at risk



AT&T Hack

Blue Boxing

Morris Worm

AOHell

Cryptovirology

Melissa Worm

Level Seven Crew hack

Denial-of-service attacks

ILOVEYOU

Heartbleed

Stuxnet

sl1nk SCADA hacks

Cloudbleed

WannaCry

Meltdown/Spectre

NotPetya

Industroyer/Chrashoverride

Infineon/TPM

Charter of Trust

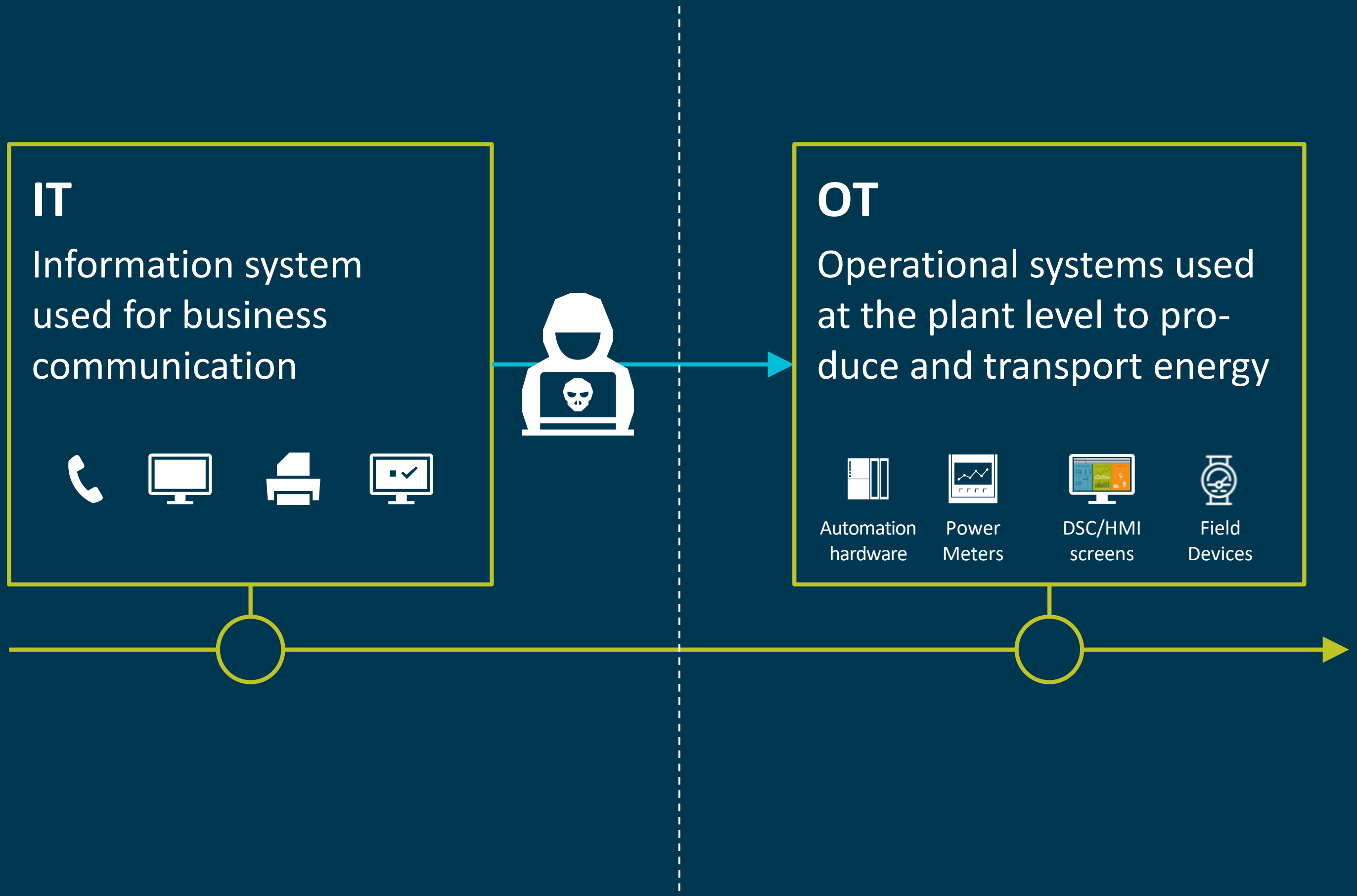
Cybersecurity is getting to be a critical factor for the success of the digital economy

Industrial safety is of particular importance

It's all about the protection of…

… industrial installations, resources, utilities, and materials essential to operations from a cyber attack

Industrial security is uniquely different



IT

Information system used for business communication

OT

Operational systems used at the plant level to produce and transport energy

IT Information Technology		OT Operational Technology
3 – 5 years	**Component Lifetime**	10 – 20 years and legacy systems
Mature stages and advanced cyber knowledge	**Cyber market maturity**	Early stages and limited awareness
Loss of data	**Key Concerns**	Impact to production, health, safety and environment
Recover by reboot	**Recovery Ability**	Fault tolerance essential
Continuous	**Connectivity**	Intermittent
Straightforward upgrades, automated changes	**Ability to update**	Typically difficult to patch, changes made by vendors

Organizations cannot protect what they cannot see

Core operational challenges move to the center stage

- Don’t know what OT Cyber Assets exist or need to protect
- Limited understanding in what way OT systems are vulnerable
- Too many vendors! Lack of integrated solution sets
- Inability to monitor and respond rapidly to threats
- Human errors and insider threats
- Lack of OT cyber manpower
- Lack of real-time information
- Too many legacy, proprietary and outdated systems

And for a common truth

We can’t expect people to actively support the digital transformation if we cannot **TRUST** in the security of data and networked systems.

That’s why together with strong partners we have signed a “Charter of Trust” – aiming at three important objectives

1. **Protect the data** of individuals and companies
2. **Prevent damage** to people, companies and infrastructures
3. **Create a reliable foundation** on which confidence in a networked, digital world can take root and grow

enel | IBM | Munich Security Conference MSC Münchner Sicherheitskonferenz | NXP

SIEMENS | AES | AIRBUS | Allianz

AtoS | CISCO | DAIMLER | DELL Technologies

SGS | T · · | TOTAL | TÜV SÜD

We came up with ten key principles

01 **Ownership of cyber and IT security**

02 **Responsibility throughout the digital supply chain**

03 **Security by default**

04 **User-centricity**

05 **Innovation and co-creation**

Charter of Trust

For a secure digital world

06 **Education**

07 **Certification for critical infrastructure and solutions**

08 **Transparency and response**

09 **Regulatory framework**

10 **Joint initiatives**

And we bring them to life as

Principle 1 — Ownership of cyber and IT security

The Siemens approach for a new **Cybersecurity organization**

Our Vision

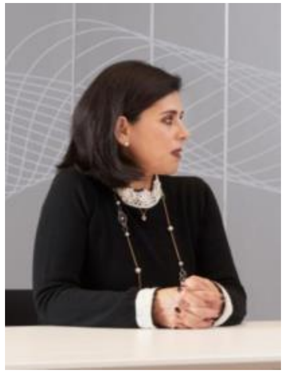
For our society, customers and Siemens, we are
the trusted partner in the digital world
by providing industry leading cybersecurity
Together we make cybersecurity real – because it matters

Our Holistic approach

Protection of our **IT and OT Infrastructure**	Protection of our **products, solutions and services**	Enable cyber **solutions for our business**

Concrete implementation steps at Siemens

In January 2018 we established a **new Cybersecurity unit** headed by Natalia Oropeza, our new **Chief Cybersecurity Officer** (CCSO). In this function, she reports directly to the Managing Board of Siemens AG.



“Cybersecurity is more than a challenge. It’s a huge opportunity. By setting standards with a dedicated and global team to make the digital world more secure, we are investing in the world's most valuable resource: TRUST.

Our proposals for more advanced Cybersecurity rules and standards are invaluable to our partners, stakeholders and societies around the world. That is what we call “ingenuity at work.”

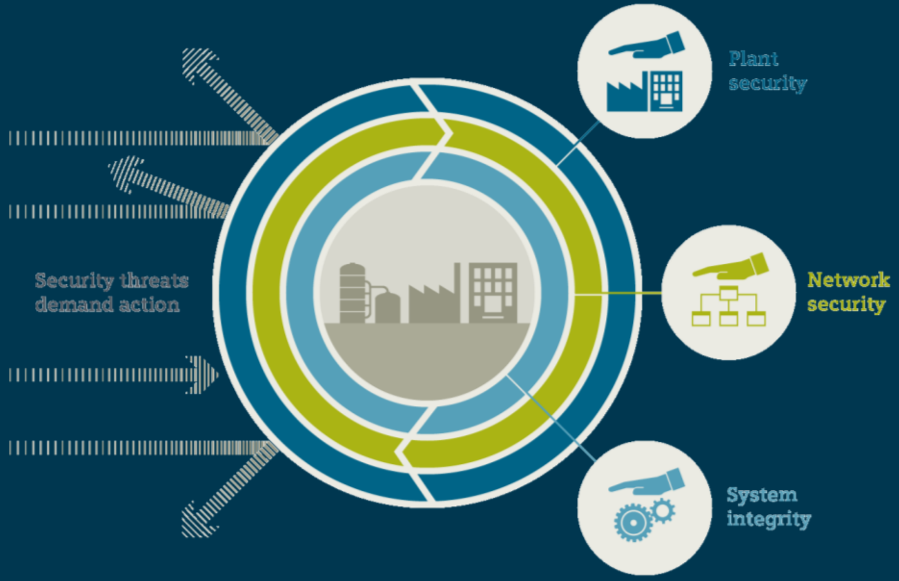
Natalia Oropeza,
Chief Cybersecurity Officer, Siemens AG

Charter of Trust

And we bring them to life as

Principle 2 — Responsibility throughout the digital supply chain

The Siemens security concept
defense-in-depth



Concrete implementation steps at Siemens

Siemens provides a **multi-layer concept** that gives plants both **all-round and in-depth protection**

- Know-how and copy protection
- Authentication and user management
- Firewall and VPN (Virtual Privat Network)
- System hardening and continuous monitoring

Concrete implementation steps with the CoT partners

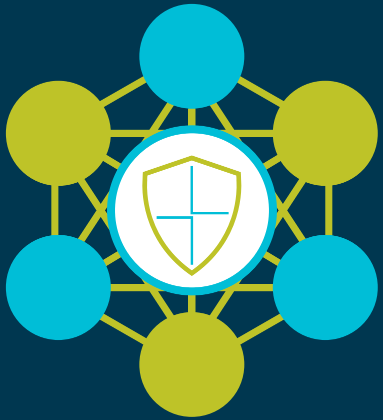
With our partners, we have defined a **list of minimum security requirements** for **all players in the supply chain**, and effective **mechanisms** that can **support their implementation**

Charter of Trust

And we bring them to life as

Principle 9 — Regulatory framework

Regulation and standardization are only successful if they are based on **multilateral cooperation**. The **World Trade Organization** is our **role model**.



Concrete implementation steps at Siemens

Siemens actively participate in a **comprehensive cybersecurity network** (relevant criminal prosecutors, ISA, FIRST, CERT Community, SAFECode). We gather threat information and disseminate it through these partnerships.

Our Government Affairs activities, which include the initiative to create a Charter of Trust, are committed to helping bring cybersecurity to the agenda and translating it into concrete regulations and standards.

Charter of Trust

Nevertheless

> “We can’t do it alone. It’s high time we act – together with strong partners who are leaders in their markets.”

Joe Kaeser
Initiator of the Charter of Trust

Charter of Trust

Charter
of Trust

We sign for cybersecurity! We sign the Charter of Trust.

SIEMENS AES AIRBUS Allianz Atos CISCO DAIMLER DELL Technologies

enel IBM Munich Security Conference MSC Münchner Sicherheitskonferenz NXP SGS T · · TOTAL TÜV SÜD