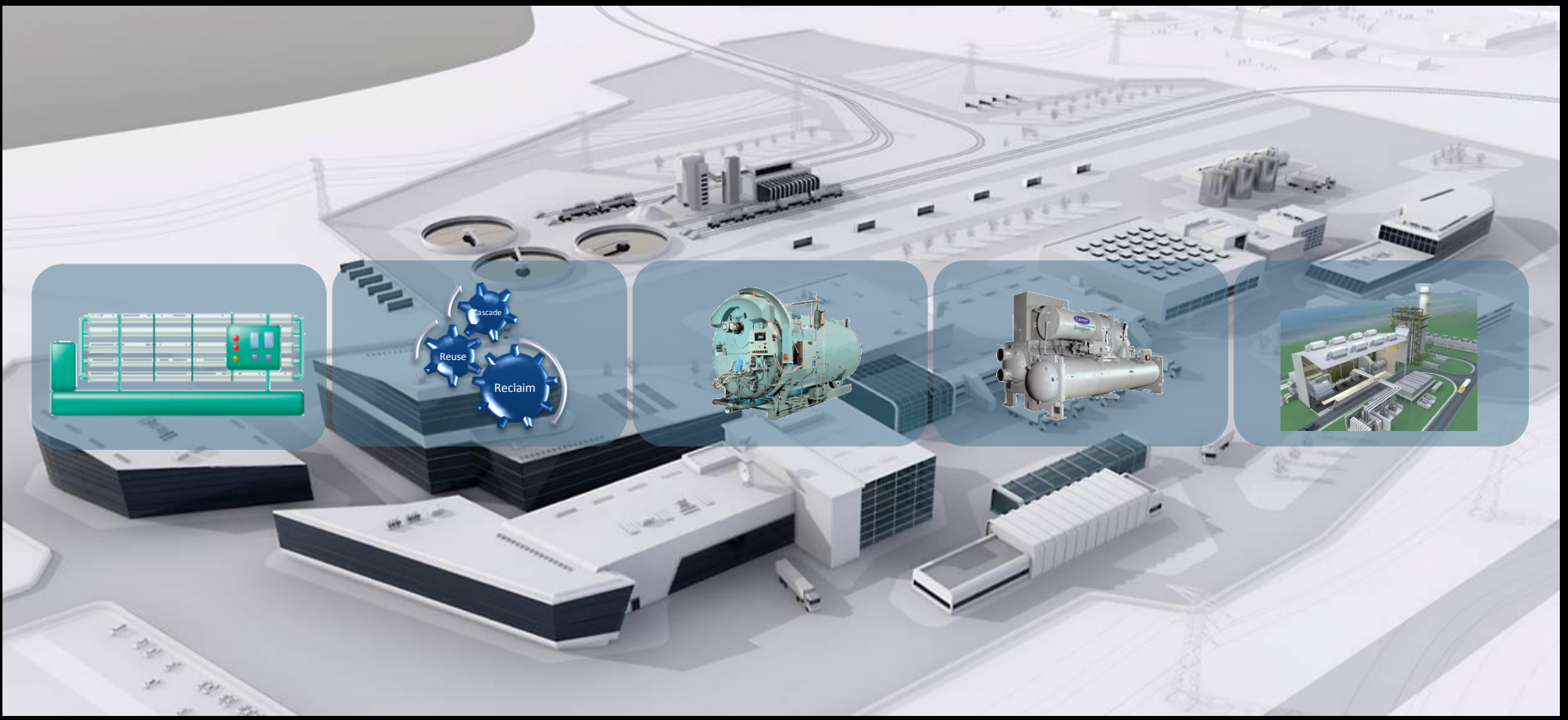
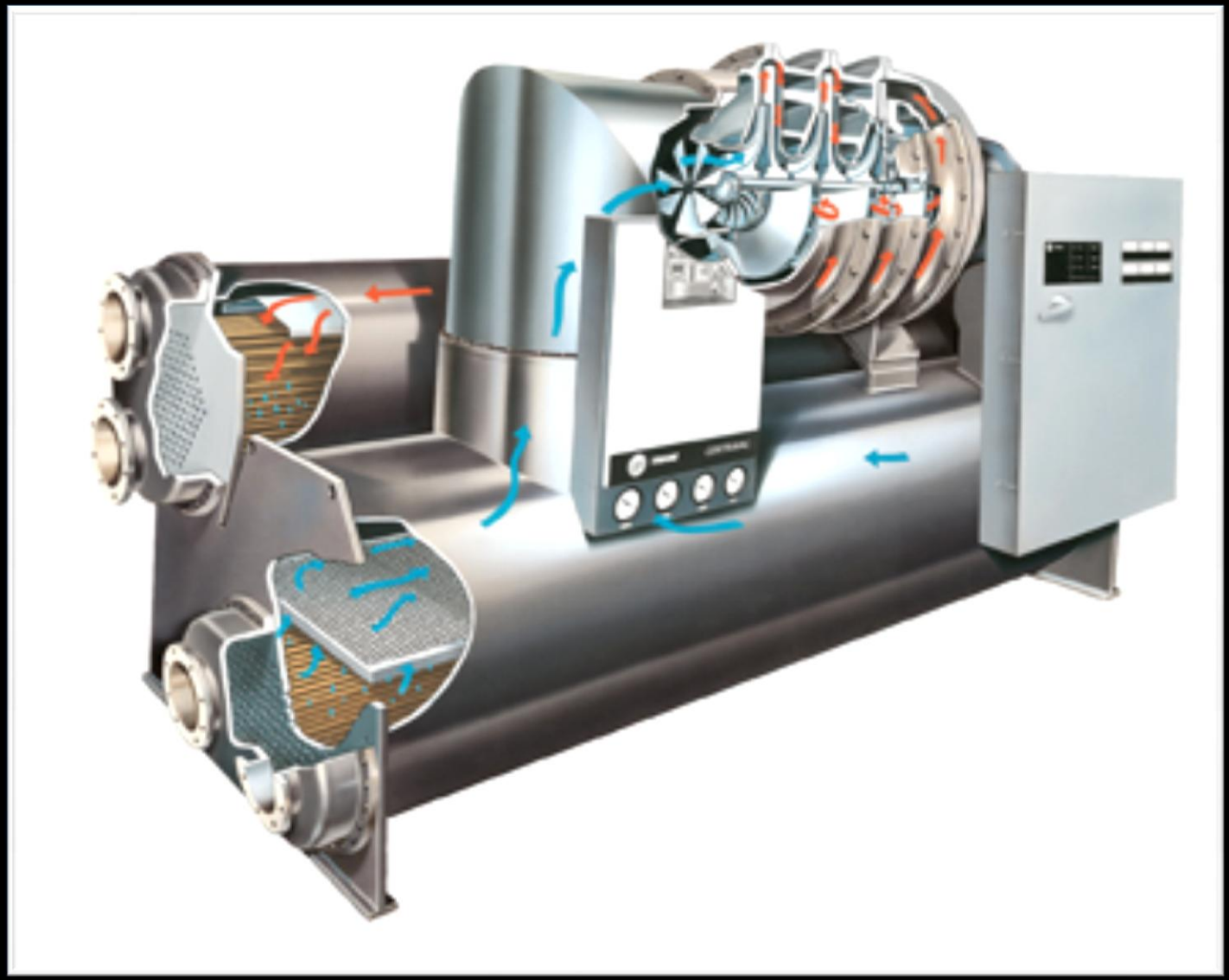
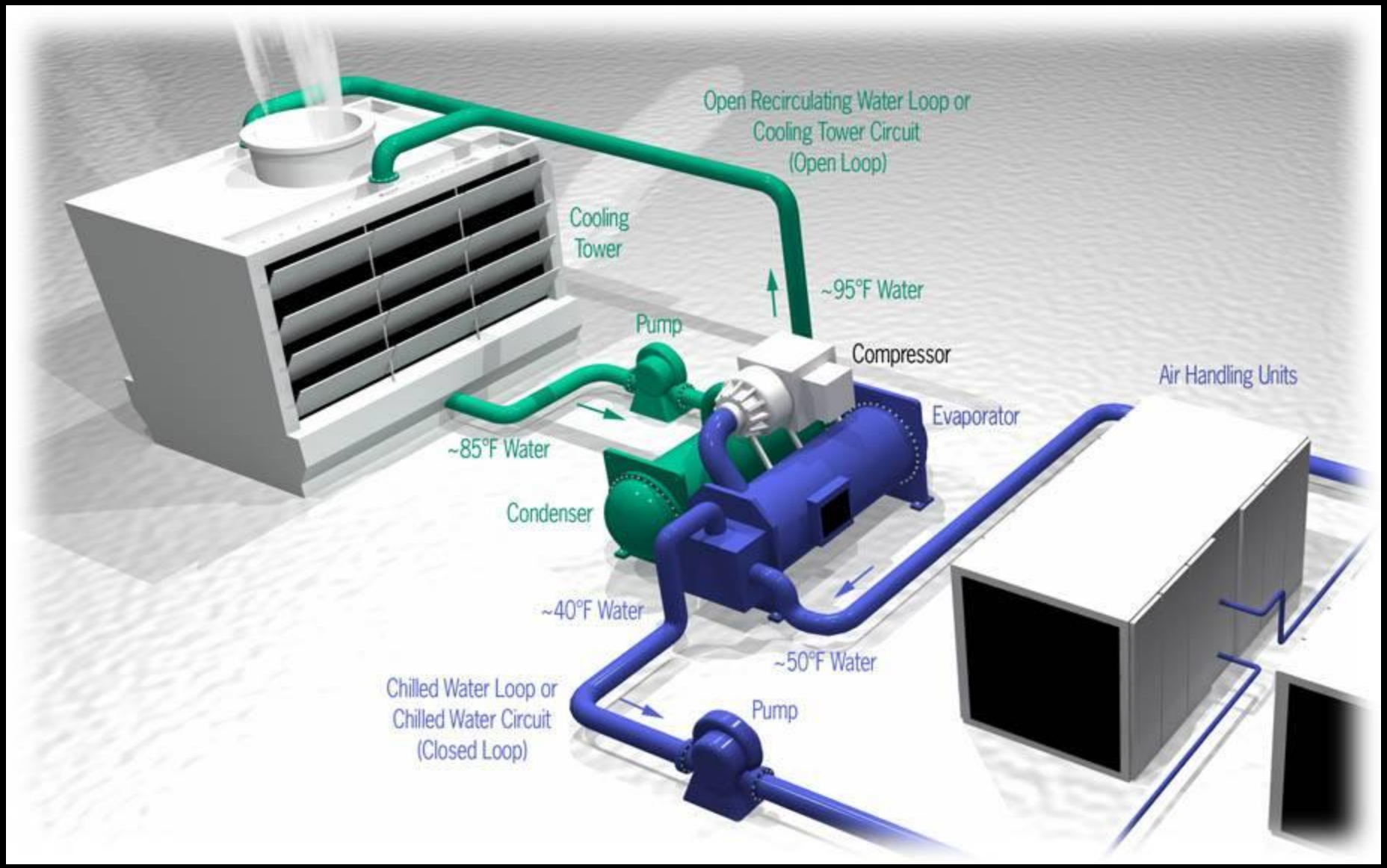
$$E = \cancel{mc}^{H_2O}$$

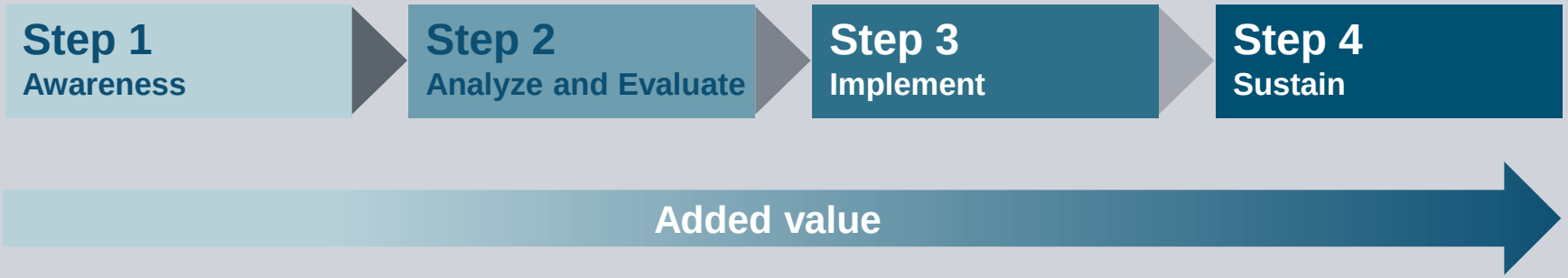

Cascade
Reuse
Reclaim




Open Recirculating Water Loop or
Cooling Tower Circuit
(Open Loop)
Cooling
Tower
~95°F Water
Pump
Compressor
Air Handling Units
Evaporator
~85°F Water
Condenser
~40°F Water
~50°F Water
Chilled Water Loop or
Chilled Water Circuit
(Closed Loop)
Pump

A holistic approach identifies, evaluates and realizes improvements

SIEMENS



What others have achieved

- Improve productivity by up to 7%
- Decrease energy consumption by as much as 30%*
- Reduce water consumption by up to 50%*
- Lower waste water production by as much as 75%*
- “Maintain the gains” through continued long-term improvements

* Per unit produced

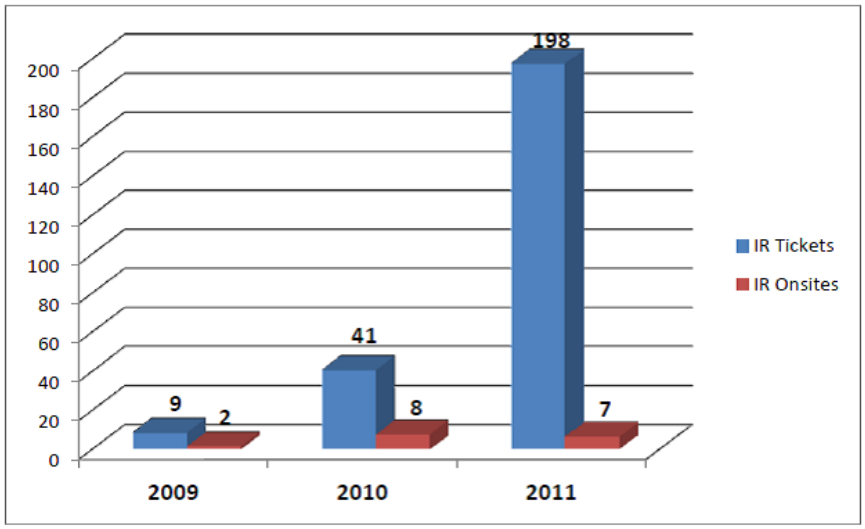
Industrial Control System – Cyber Security

Cyber threat is a serious challenge facing US industry & infrastructure today

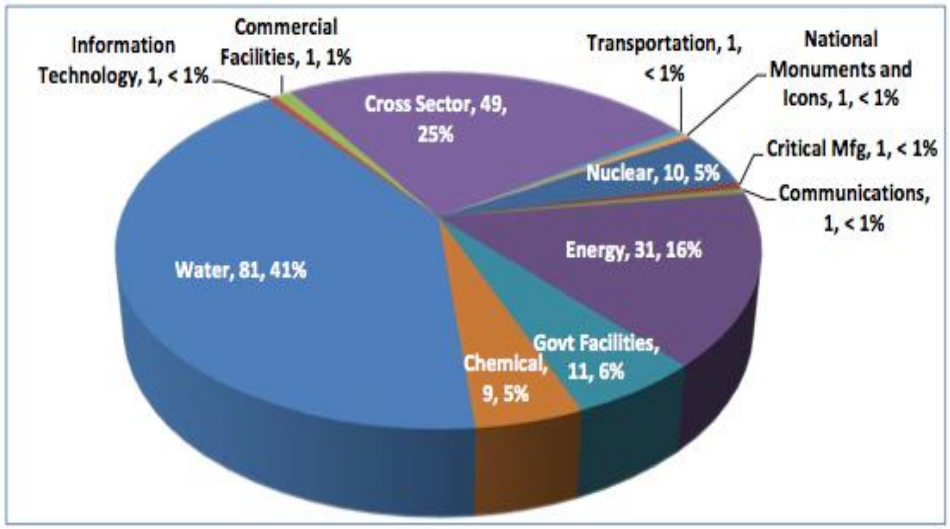
SIEMENS

The ICS-CERT Incident Summary Annual Report tells the story

- Cyber threats to Industrial Control Systems (ICS) are on the rise
- There is a critical need to protect our critical infrastructure from cyber attacks



ICS-CERT incident response trends data



Incident reports by sector (2011)

Cyber Security incidents can have devastating consequences and lasting impact

SIEMENS

2000 – Maroochy Water Shire Attack

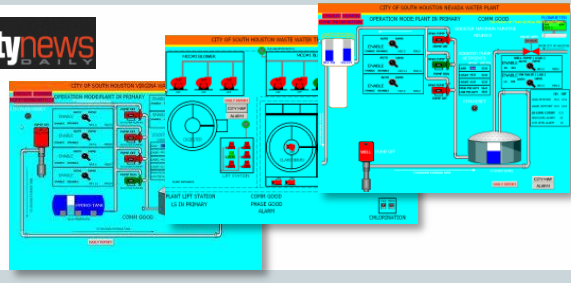
Vitek Boden used radio equipment to hack into a water treatment system. Caused over 211,000 gal. of raw sewage to spill into local parks, rivers and the grounds of a Hyatt Regency.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

2011 – Texas Water Treatment Plant

Hacktivist “pr0f” claims to hack Texas water treatment plant in South Houston. Published screen shots from SCADA on the Internet to raise awareness.

securitynews DAILY

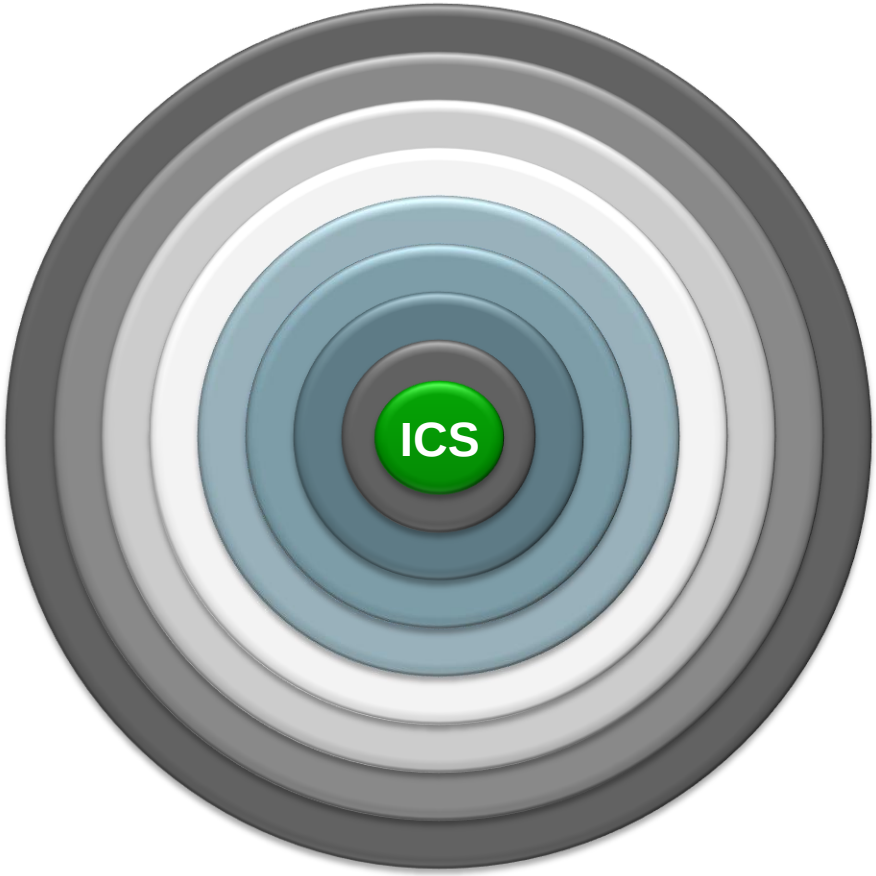


March 2013 – TREND Micro SCADA Honeypot

In the course of 28 days, 39 attacks from 14 countries.
12 classified as targeted. 13 repeated by same attacker.
35% of attacks from China

TREND MICRO™

The Defense in Depth Concept



Industrial Security levels according to current standards and regulations

Plant security
- Access blocked for unauthorized persons
- Physical prevention of access to critical components

Network security
- Controlled interfaces between office and plant network e.g. via firewalls
- Further segmentation of plant network

System integrity
- Antivirus and whitelisting software
- Maintenance and update processes User authentication for plant or machine operators
- Integrated access protection mechanisms in automation components

Security solutions in an industrial context must take account of all protection levels

SIEMENS