IoT-OT and IT Security Convergence

Ruggero Contu

Research Director

Gartner

Strategic Planning Assumption

By 2020, over 25% of identified attacks in enterprises will involve IoT, though IoT will account for less than 10% of IT security budgets

Cyberphysical Security Can Be a Matter of Life or Death

Gartner.

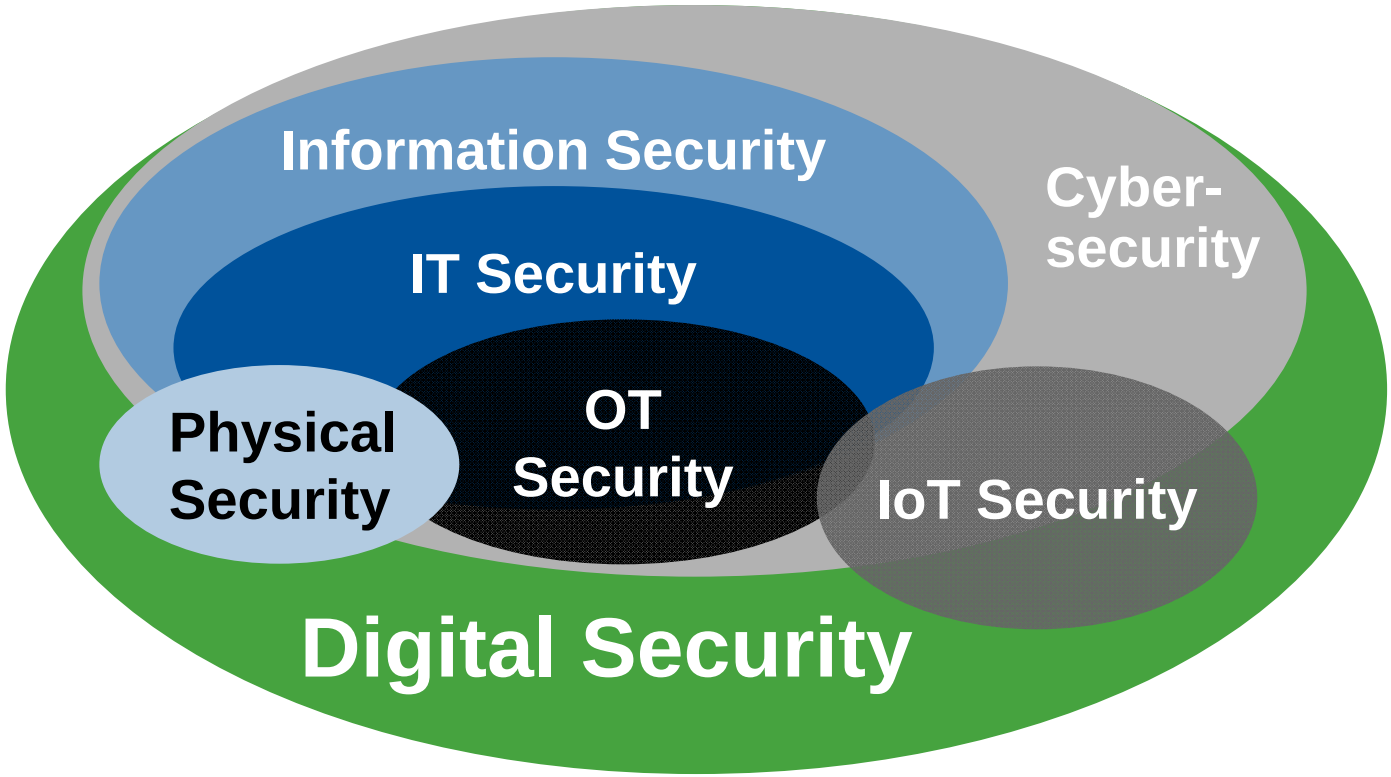
Key Issues

1. What organizational and cultural challenges is the convergence between IoT-OT and IT security bringing?
2. What are the security processes and approaches needed to cater for specific requirements and also for the diversity of ecosystems?
3. What technology should you consider?

Key Issues

1. What organizational and cultural challenges is the convergence between IoT-OT and IT security bringing?

Our View of Security Will Change (Whether We Like It or Not)

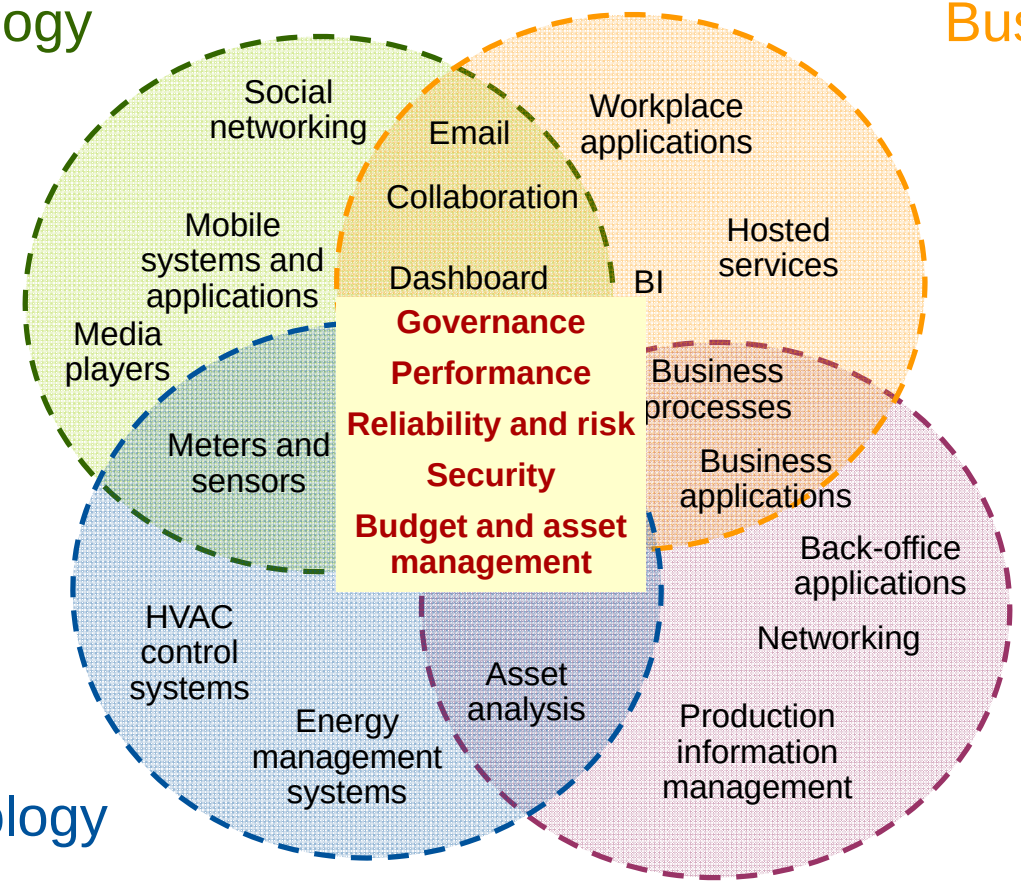


Gartner.

Be Prepared for Blurring of Roles, Decision Rights and Authority

Consumer technology

Business technology



Operational technology

"Traditional" IT

Gartner.

Cultural Differences=Different Priorities

Culture of Engineers: Reliability and safety, fault tolerance, determinism, consistency and longevity.

Solution Approach: Find example, iteratively optimize for performance and use, lockdown.

Culture of IT: Frequent change, shorter lifetimes for products and systems, user or customer convenience and "the user experience".

Solution Approach: Develop standards, assess requirements, build/buy best fit at lowest cost, plan for upgrades and support.

What IT Can Learn From Engineers?

- Physics matter … the physical world always gets in the way.
- Real time, means real time.
- Physical security should always be part of a cybersecurity solution.
- Things wear out, and asset reliability will save you.
- There is no such thing as greenfield, it's brown at best. Learn to live with the old.

Gartner.

What Engineers Can Learn From IT

- Governance and policy for support infrastructure have value
- Continuous asset and threat awareness have value
- Improperly managed IT impacts stability, putting safety and reliability at risk
- IT can prepare OT for pace of technology change
- Use tools and processes to manage constant software change

Gartner.

Move From "Ownership" to Share Responsibility and Accountability

An IT approach that says we need to *control* what gets bought, and how it is deployed, will fail.

An OT (or IoT) approach that says: "We own the technology and make the decisions, but then you guys deal with the implications …" will fail.

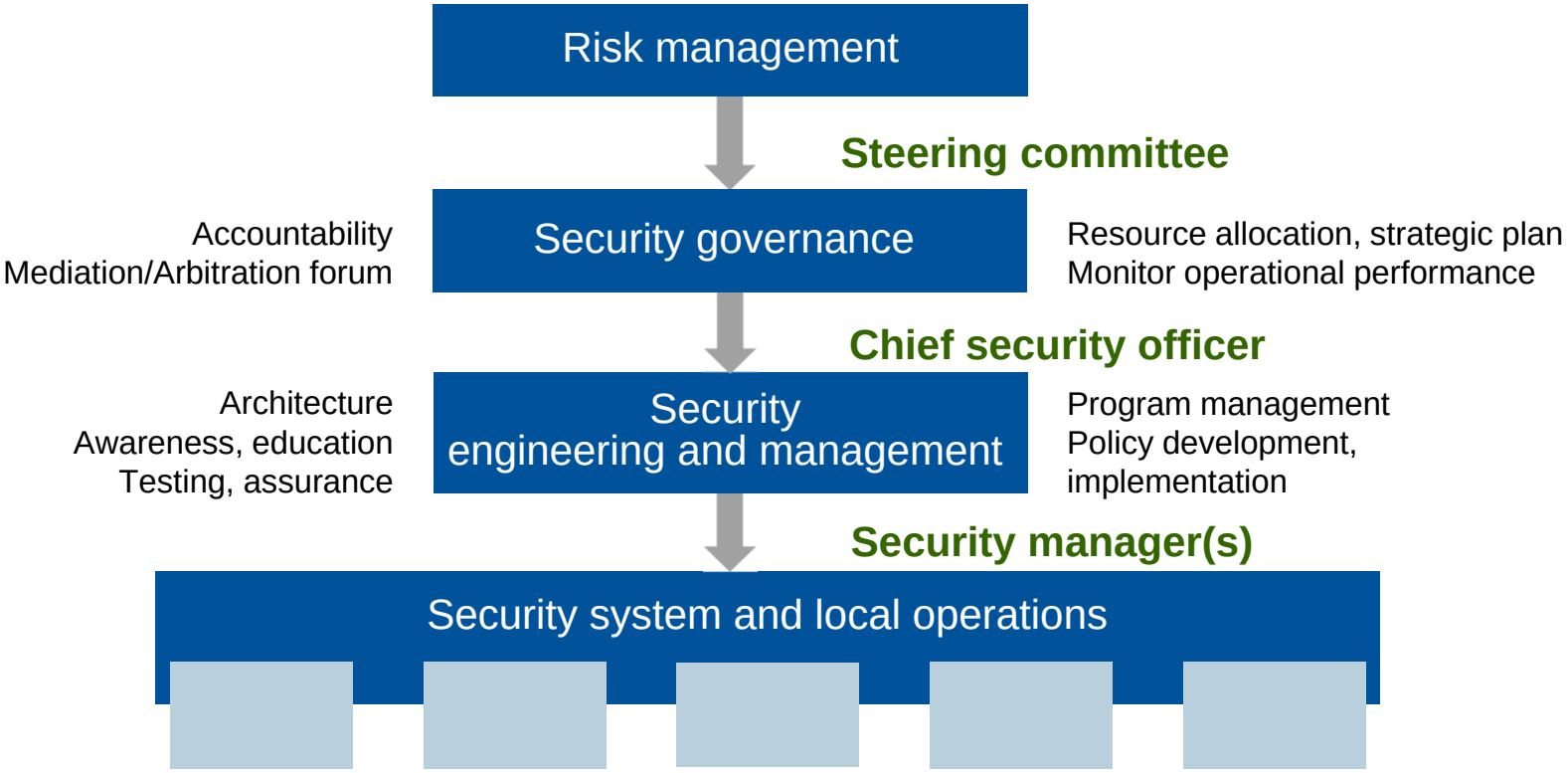
To take on responsibility, and share:

Governance, standards, platforms, security, SLA.

Alignment on these is critical.

Gartner.

Digital Security Requires a Revised View of Organization



Key Issues

1. What are the security processes and approaches needed to cater for specific requirements and also for the diversity of ecosystems?

Gartner.

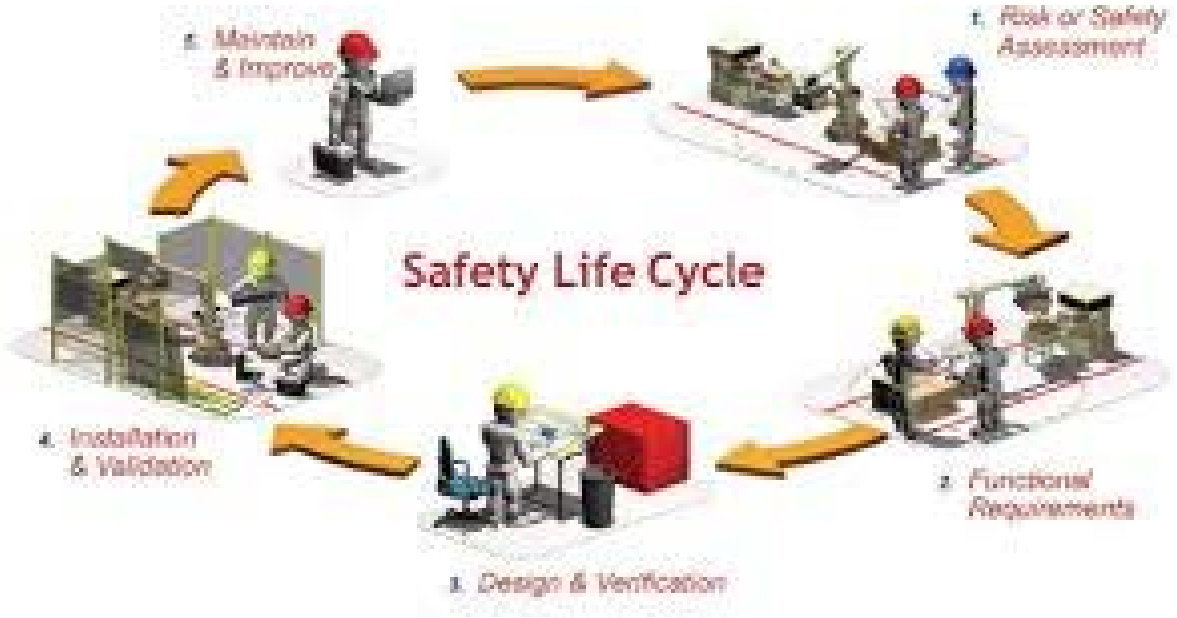
OT Has Its Own Unique Security Needs

- Heterogeneous
- Continuous
- Reliable
- Physical
- Focused

Graphic source: canstockphoto.com

It All Starts (and Ends) With Safety

- Safety is an absolute
- Time is a critical parameter when measuring and controlling mission-critical processes
- Real time is measured in ***milliseconds***
- Resilience: That "fail-safe" is a design practice



Gartner.

Key Approaches

- Show discipline in design
- Adhere to standards
- Identify and address dependencies
- Build independent operations
- Test, test, test — and then test
- Leverage the supply chain

Gartner.

Asset Management Key

- What do we own and where is it?
- What's it worth?
- What condition is it in?
- What do we need to do to it?
- When do we need to do it?
- How much money do we need?
- How do we achieve sustainability?

(aka: What can IT learn from ISO 55000 (physical) asset management and apply to ISO 27036)

Gartner.

Risk-Resilient Balance for the Integrated Organization

RISK

- Governance
- Compliance
- Control
- Protection

RESILIENCE

- Reliability
- Speed
- Assurance
- Transparency

Gartner.

Key Issues

1. What technology should you consider?

What Engineers Know About IoT and OT Vendor Risks

- Many start-ups=risks
- IT vendors increasing partnerships in OT areas.
- OT vendors are exploring IT techniques

Gartner.

Securing Old and Diverse Systems — Back to the Future!

- Learning to live with a hybrid old-new product set
- Prepare for a new breed of vendors — and an old set of vendors
- Beware of vendors limitations
- The supply chain issue

Gartner.

a Very Fragmented Market

Sample List Security Providers

Gartner.

a Very Fragmented Market

Sample List Security Providers

OT Security Controls Approaches

•***Monitoring and response****: A*nomalies detection with provision of functions to permit response to them.

•***Network segmentation****: M*anaging data flow between defined networks, ie firewalls and unidirectional gateways, and products that aid in keeping that data flow secure.

•***Access control****:* Controls to manage access of users to systems or one system to another system. This includes identity and access management, remote access and privileged access management.

•***Endpoint protection****:* Protection of endpoints, including devices besides PCs or mobile devices, ie anti-malware, personal firewall, port and device control, memory protection, and related capabilities

Recommendations

- ✓ Find the OT environments and stakeholders in your organization. What are their roadmaps and plans (hint: this isn't likely your CIO)
- ✓ Assess your current state of OT security using qualified sources.
- ✓ Expand your IT security planning to include OT / IoT security requirements (and vice versa)
- ✓ Identify your IT/OT security supply chain.
- ✓ Leverage OT security principles in IT where applicable.

Recommendations

- ✓ Select OT security products via a formal assessment that addresses reliability and safety concerns of OT production and operations.
- ✓ Establish OT security governance, strategy and management via a combined IT/OT security practice that can evaluate and manage both IT and OT security products.
- ✓ Focus on key areas of OT security, such as network segmentation, access management, and anomaly detection and response.
- ✓ Ensure OT engineers participate in OT security policy development and requirements setting.
- ✓ Include training programs for IT security team members in OT skills.