Setting the Standard for Automation™

IEC 62443: INDUSTRIAL NETWORK AND SYSTEM SECURITY

Tom Phinney

Honeywell

Integrated Security Technology Lab

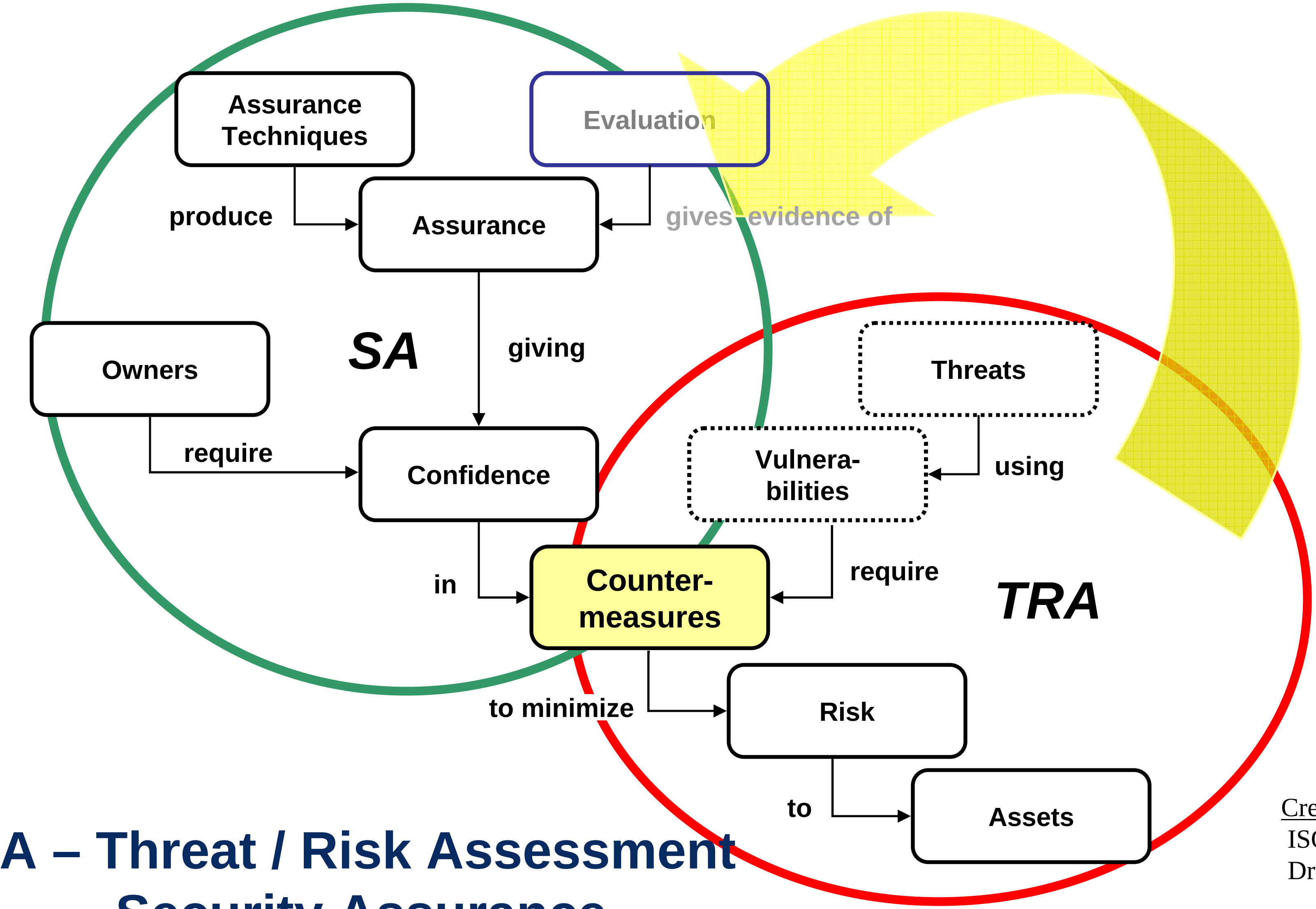
Tom Phinney

- 40+ years experience in software and hardware for real-time systems
- 25+ years as architect and system designer with GE and Honeywell in Phoenix
- Specialized in industrial communications since the late 1970s
- 1980-86: Initial author or early editor of IEEE 802.2, 802.4, 802.5, precursors to 802.11
- 1981-86: Co-founded company making leading-edge POTS and LAN modems
- 1988-1993+: Author/editor of ISA SP50 / IEC SC65C Type 1 fieldbus data-link layer
- 2002: Recipient of ISA's Standards & Practices award for outstanding service
- 2003: Recognized by ISA as one of the 50 most influential people in modern history in advancing automation, instrumentation, and control technologies
- 2005: Recipient of the IEC's 1906 award, which recognizes major contributions to furthering the interests of worldwide electro-technology standardization
- <u>Current:</u>
  - Chairs three IEC standards working groups in the area of industrial process measurement and control :
    - IEC/TC 65/WG 10: cyber-security
    - IEC/SC 65C/MT 9: fieldbus
    - IEC/SC 65C/WG 13: fieldbus cybersecurity profiles
  - ISA SP99 industrial cyber-security – leadership team
  - ISA SP100 industrial wireless networking – significant technical contributor

Outline

- The threat / risk / response security feedback loop
- Security as a continuing process, not a reachable goal
- The landscape of cybersecurity standards
- IEC 62443: *Network and system security*
  for industrial-process measurement and control

The security feedback loop



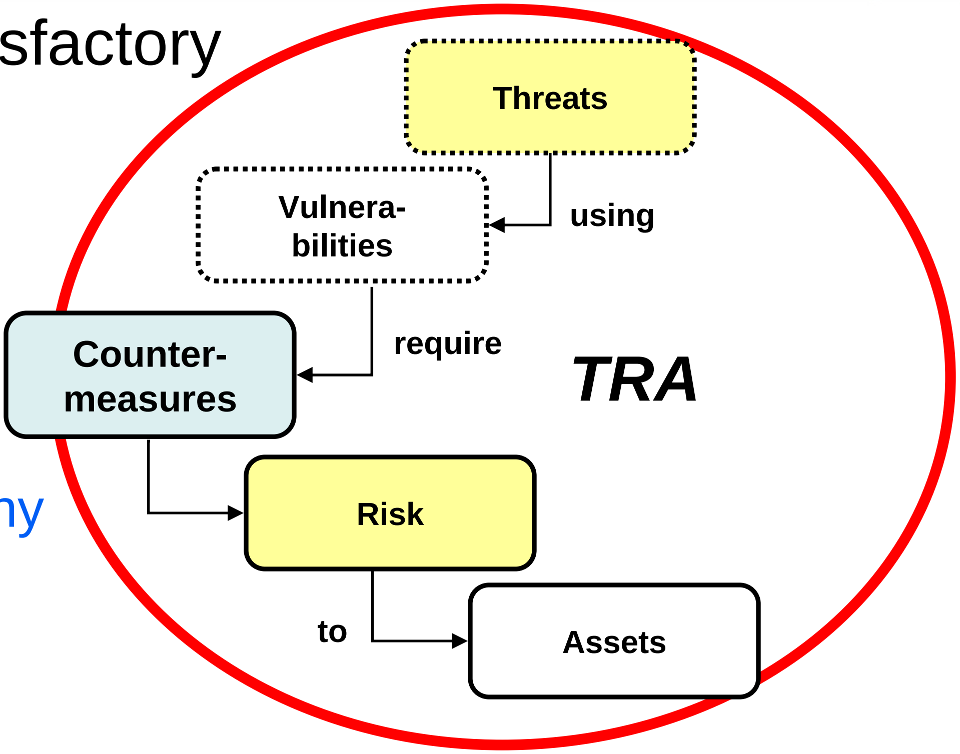
TRA – Threat / Risk Assessment
SA – Security Assurance

Credits:
ISO/IEC 15408-1
Dr. Hans Daniel

Threat / risk assessment

- Existing methods are unsatisfactory
  - Which threats?
  - Which risks?
  - Were any missed?
  - The usual conclusion:

    “The risks are too big and many to protect against them all”



- The real questions are:

  “Which countermeasures are appropriate?”

  “What should I do for the amount I can afford?”

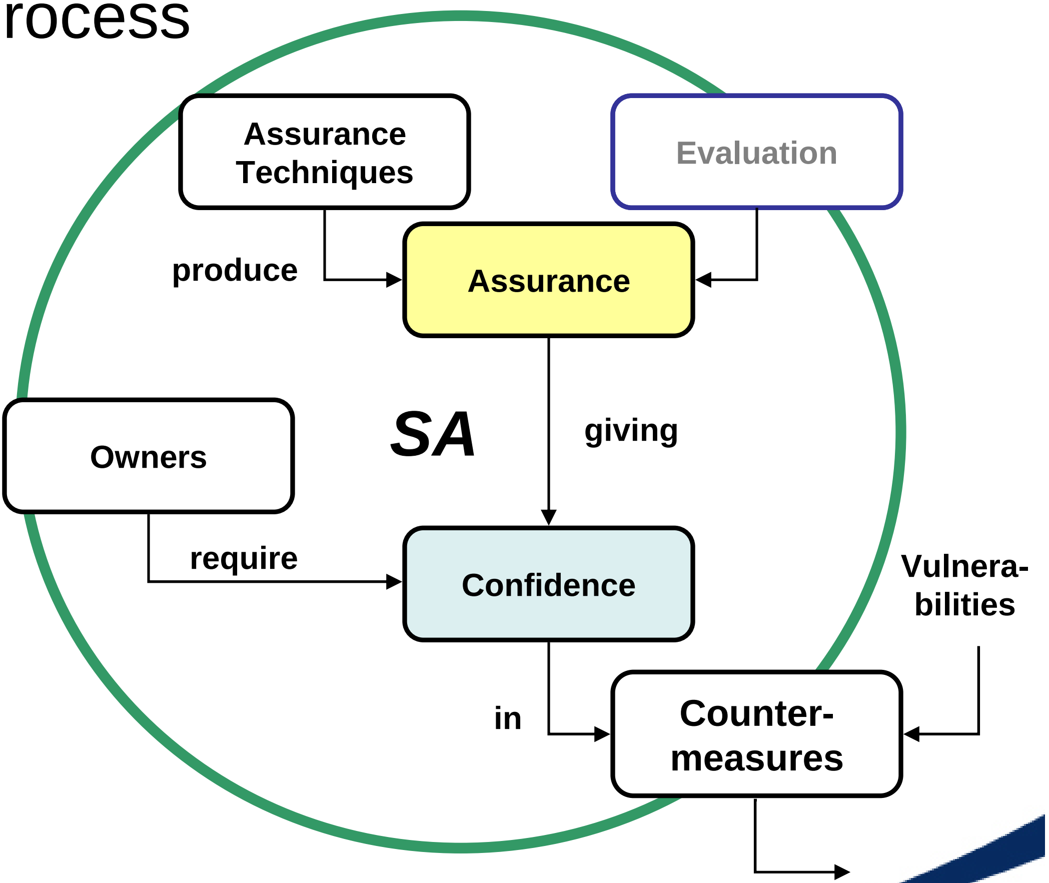
  “What is the marginal benefit per unit cost of doing more, or less?”

Security Assurance

- Assurance (def): The basis for trusting that policies are implemented as intended

- Assurance is an ongoing process and thus a continuing cost
- Confidence is the goal

- How much to spend?
- What to verify, and when?
- What is the marginal cost of doing more? … of doing less?



Security – an ongoing process

- Security is not a goal that can be reached
  - New vulnerabilities are discovered daily
  - Threats continue to evolve
  - Personnel become lax, or find workarounds to security measures
  - ∴ weak points in the system change, becoming new points of attack
- Security is a process and an attitude
  - “All trust is limited”
  - Assume that the attacker is at least as intelligent and motivated as the defenders
  - The weakest points in the system are the most likely targets
  - Security may be achieved, or lost, incrementally through small actions and inactions
  - “Eternal vigilance is the price of security”

The security mindset

"All trust is limited"

- Compartmentalize
  - Minimize what must be defended
  - Minimize increment of potential loss
- Defend in depth
  - One '*Maginot line*' is not sufficient
- Re-verify basis for trust (similar to Reagan's "trust but verify")
  - Verification testing should not be predictable
  - Unverified trust decays with time
- Assume that some personnel & equipment are compromised by the attacker
  - This is one reason why a single 'Maginot line' is not enough

Classes of attackers

- Amateur computer hackers/criminals
- Organized crime groups
- Professional, non-state actors (i.e., terrorists, political activists)
- Traditional adversarial nation-states
- Rival corporations and nation-states seeking competitive advantage
- Angry or unethical employees, contractors and consultants
- Outsourced or subcontracted firms and/or employees
- Software and hardware vendors looking for financial benefits
- Unethical advertisers / commercial entities
  (i.e., spyware and adware providers)

Credits:
www.sans.org

The management challenge

Security is a never-ending process

- that is every employee’s personal responsibility
- with more uncertainty than other business processes
- with mostly indirect measures of success
- and potentially catastrophic demonstrations of failure

As with all continuing processes,

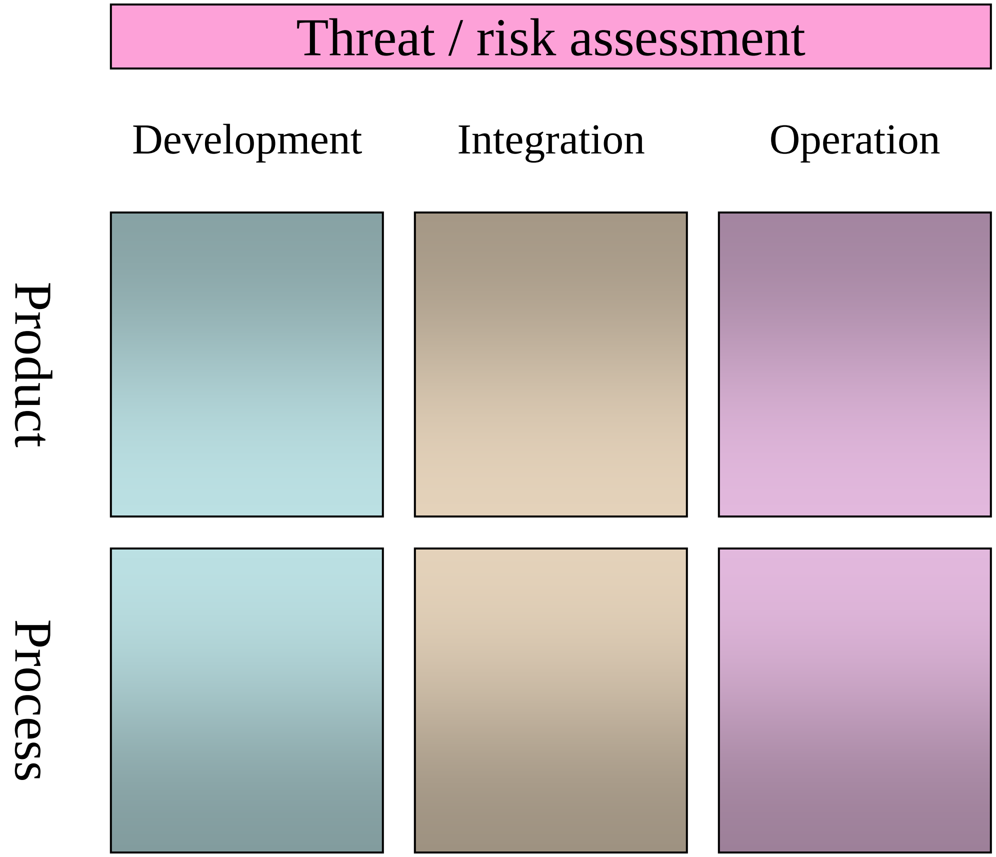
- people become complacent
- or develop workarounds without regard to consequences

Continuing assurance provides the mechanism and driver for maintaining vigilance

Cybersecurity assurance standards

- Product assurance
  - ISO/IEC 15408, Common Criteria
  - ISO/IEC 19790, Security requirements for cryptographic modules (similar to NIST FIPS 140-2)
  - ISO/IEC TR/19791, Security assessment of operational systems
- Process assurance
  - ISO/IEC 21827, SSE capability maturity model (SSE-CMM®)
  - ISO/IEC 17799, Code of practice for information security Mgmt
  - COBIT – Control objectives for information and related technology
  - draft ISA S99 standards: Concepts and process guidance
- Environment assurance
  - ISO 9000, …

The assurance matrix



Threat / risk assessment

Development

Integration

Operation

Product

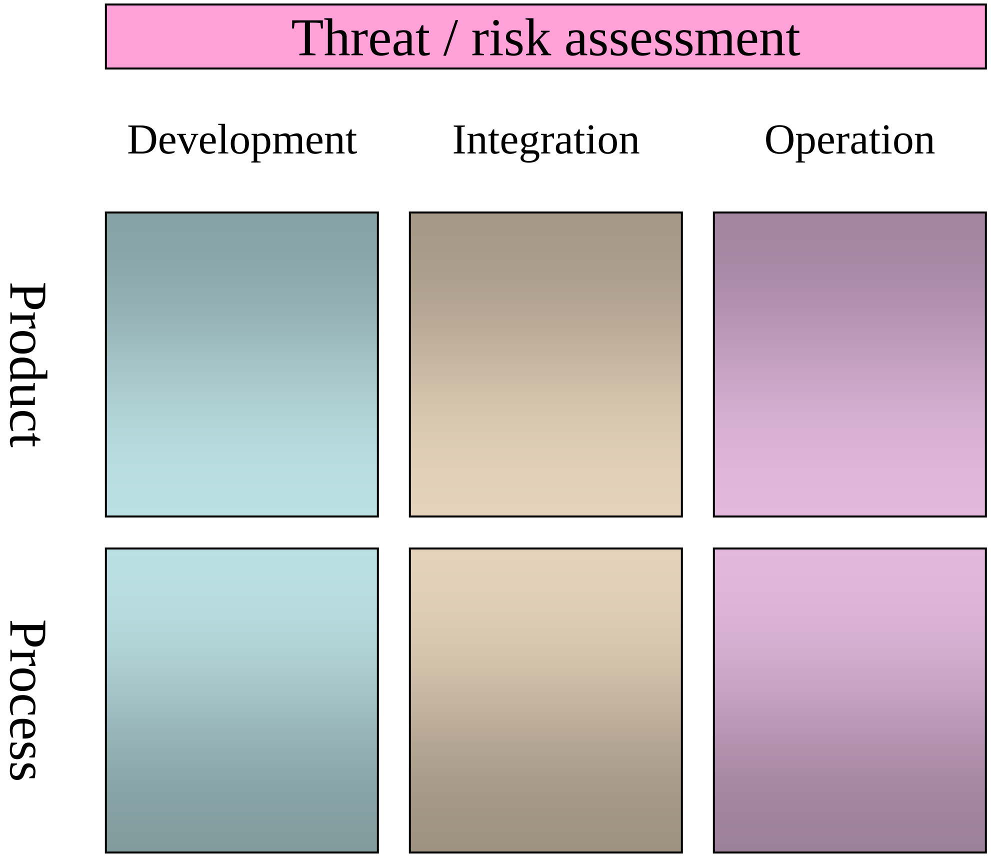
Process

- Existing assurance standards address varying portions of this matrix
- None partition cleanly between development, integration and operation phases
- Some address only process; others address both process and product, but unevenly
- None do a good job with threat / risk assessment, in a form that can provide practical guidance

IEC 62243, Network and system security for industrial-process measurement and control

- Focus to date has been on operational “best practices”
- Undergoing restructuring to a threat/risk assessment plus assurance basis
- Proposed multi-part structure:
  - Concepts and Threat/Risk Assessment
  - Development Assurance
  - Integration Assurance
  - Operational Assurance
  - Sample Security Solutions: Policies and System Configurations (most of the material in the early 62443 drafts will go here)

The assurance matrix



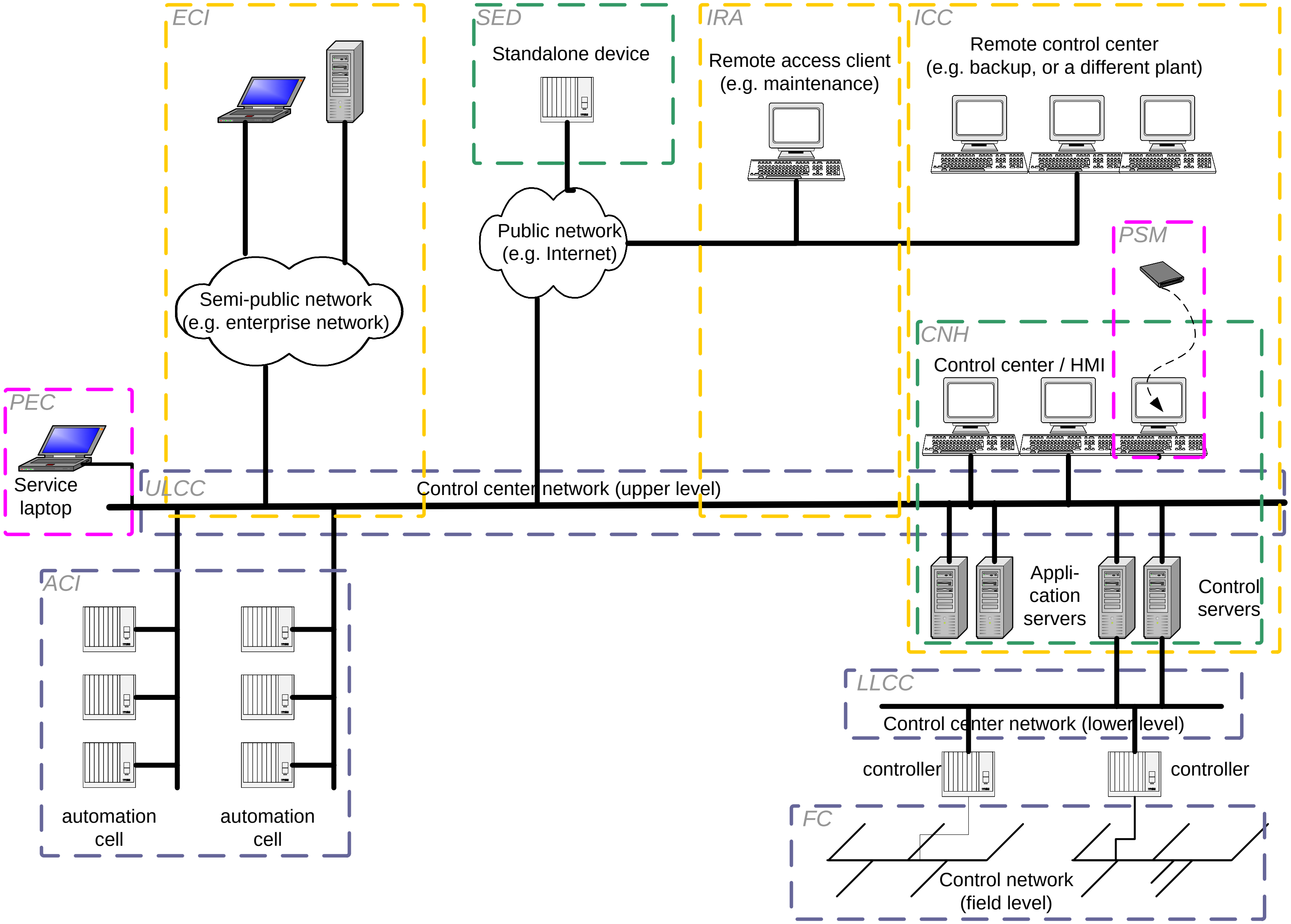
Probable structure of
IEC 62443–***n***

1. Threat / risk assessment
2. Development assurance
3. Integration assurance
4. Operation assurance
5. Sample security solutions (also known as
 “Good practices 2006”)

Anticipate heavy reference to other assurance standards

Part 5 likely will be the first part issued, as a TS

IEC 62443 working reference model



Acronyms of working reference model

- Securing external network communications paths into automation networks:

– ECI:	External network – Control network Interconnection
– IRA:	Interactive Remote Access to a control network
– ICC:	Inter-Control Center access to a shared control net
– SED:	Standalone Embedded Device
– PEC:	Portable Engineering Computer
– PSM:	Portable Storage Medium

- Securing internal network communication paths within automation networks:

– ACI:	Inter-Area Communication within a hierarchical multi-area control network
– CCN:	Control Center Networks within a single control area
– FCN:	Field Control Networks within a single control area

- Securing devices within automation networks:

– CNH:	Control Network Host
– AFD:	Automation Field Device

Example profile outline from 62443

- n.2 ECI: External network – control network interconnection
- n.2.1 Introduction
- n.2.1.1 Use cases
- n.2.1.2 Threats addressed by this profile
- n.2.1.3 Terminology and definitions
- n.2.1.4 Applicable network topology
- n.2.2 Assumptions
- n.2.3 Network topology requirements
- n.2.4 Data flow requirements
- n.2.5 Required security functionality
- n.2.6 Operations requirements
- n.2.7 Policy requirements
- n.2.8 Responsibilities by vendor, integrator, owner/operator

Thank you