The Need for Security Testing of Devices

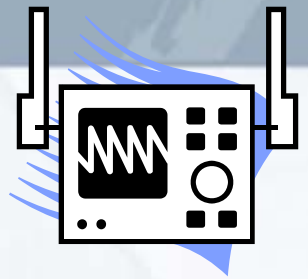
Eric Byres, P.Eng.
Director – Industrial Security
ebyres@wurldtech.com

© 2006 Wurldtech Analytics Inc. – All Rights Reserved

The Need for Security Testing

- Many well established testing methods used to assure the quality and functionality of industrial control products:
  - Electromagnetic Compatibility EN-61000, EN050081…
  - Network Performance IETF RFC 1242, 2544, 2289…
  - Temperature, Humidity, Vibration IEC 68-2-30, 68-2-6…
- Are there any formal testing methods/standards for security of products?

Not All That Stable…



- UDP port scan was performed on hospital equipment that included critical patient monitoring systems.
- The monitors locked up …
- A rare occurrence? Definitely not…
  - ISID has over a dozen incidents where significant control impact was caused by simple network scans or broadcast storms.

Testing, PCSRF and Common Criteria

- Protection Profiles are very useful and specify testing as one of the CC Objectives:

  "O.VULNERABILITY_ANALYSIS_TEST

  The TOE will undergo appropriate independent vulnerability analysis and penetration testing to demonstrate the design and implementation of the TOE does not allow attackers with medium attack potential to violate the TOE's security policies."

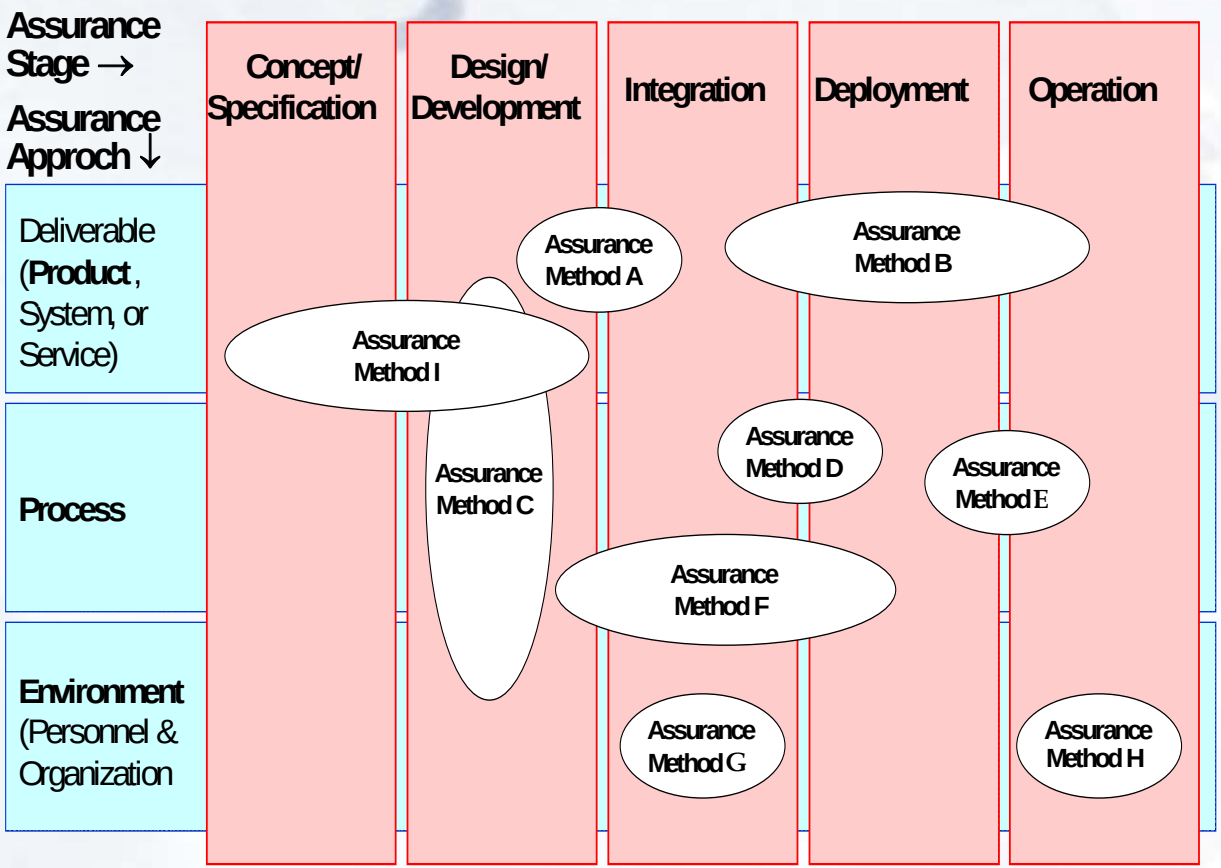
- But what are these "*appropriate*" tests?

Security and the System Life Cycle

- From Dr. Hans Daniel of IEC TC65/WG10:
  - A product or system undergoes a lifecycle.
  - 5 lifecycle stages recognized in ISO/IEC 15288.
  - Methods and standards can be associated with each assurance stage.
  - Security assurance increments are gained at every successful activity.

Slides courtesy of Dr. Hans Daniel

Security and the System Life Cycle



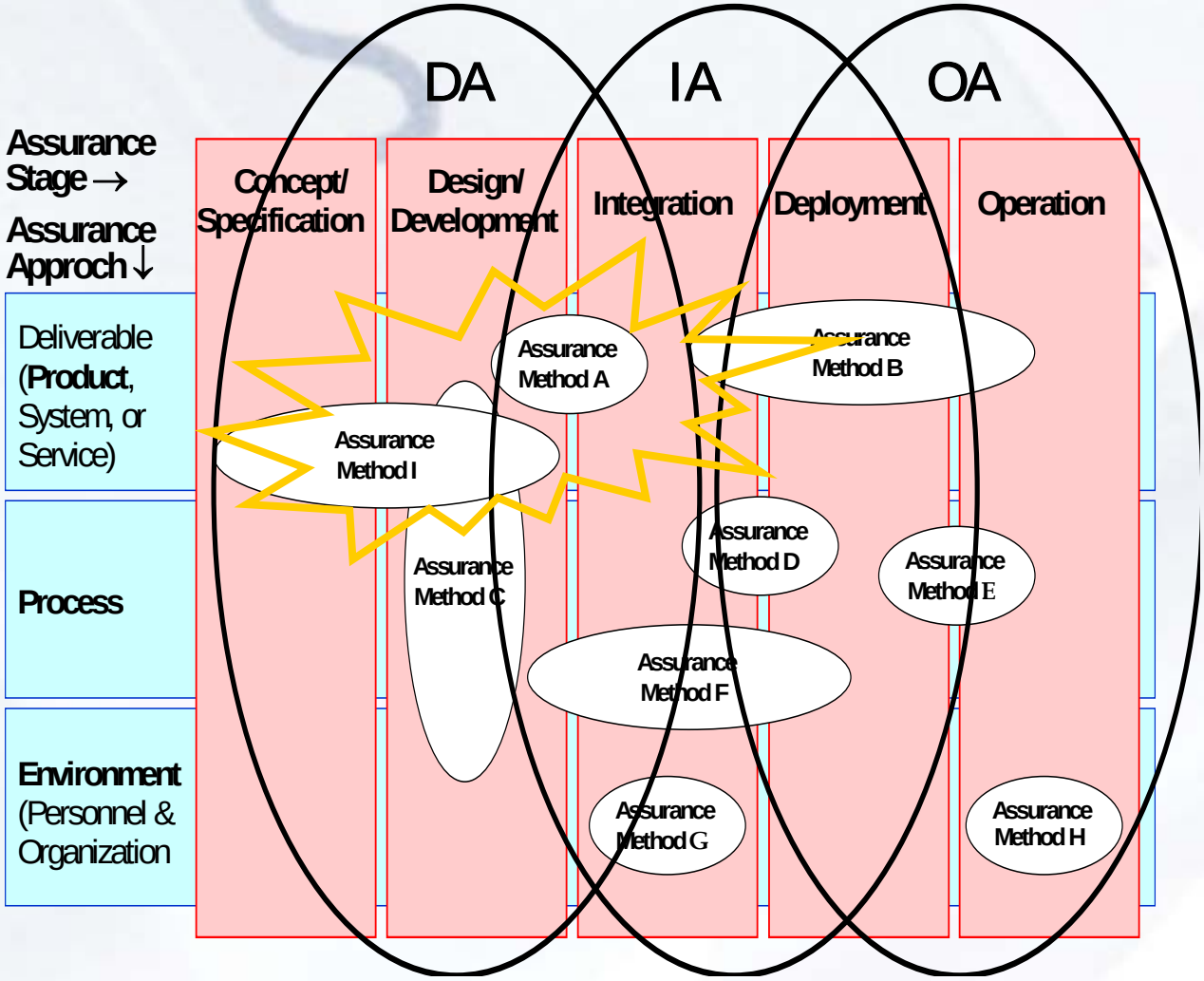
Slides courtesy of Dr. Hans Daniel

Security and the System Life Cycle

- 3 major user/provider concerns.
- Addressed by Standards and methods:
  - Development of products and systems;
  - Integration of products into operational systems;
  - Operating a specific system, in a facility and personnel context;

Slides courtesy of Dr. Hans Daniel

Security and the System Life Cycle



Slides courtesy of Dr. Hans Daniel

System vs. Component Testing

- Tendency to make the ToE the whole control system (e.g. penetration tests).
- Initial ToE should be the basic building blocks.
- Engineering 101 for building a wall:
  - Start by accurately understanding the materials (e.g. direct testing, industrial standards, etc.).
  - Next design wall as a system based on step #1.
  - Inspect/test final installation.
- Don’t design by guessing the bricks are strong!

Example – MS-SQL & Slammer

- Slammer is still the most active worm in ISID industrial security events.
- Yet the patch is over 4 years old!
- Why – People don’t realize that Microsoft SQL Server is a component of their system.
- They don’t understand the “bricks” holding up their wall.

What Device Test Standards Can Do

- Provide a Level of Confidence
  - Example: Users know that they can safely scan their system.
- Provide a common measure for comparing control products.
  - Example: All “certified” devices can withstand scan.
- Allow focusing of system design and mitigation on the untested vulnerabilities.
- Create level playing field for vendors.

What Device Test Standards Can’t Do

- Can't Guarantee Security – we are simply setting a bar for minimum device robustness.
- Can't uncover device interactions that cause system vulnerabilities.
- Can't address issues in other stages of the life cycle. Example:
  - Inappropriate configuration in the field.

Next Steps - KISS

- Focus on individual components and not systems (for now).
- Clearly decide where in the life cycle the tests are targeted.
- Create simple taxonomy for organizing tests.
- Define basic tests that can be conducted reliably & inexpensively by vendors and users.
- Create tests for all components, not just controllers.

Questions?

© 2006 Wurldtech Analytics Inc. – All Rights Reserved