Ralph Langner

The Langner Group

Arlington | Hamburg | München

The Kaizen of ICS Security

Old-School (Western) ICS Security Wisdom

Paradigm:
Risk Management

ICS Risk Management

in four easy steps

1. Do nothing for a couple of years

2. Assess risk. No credible threats? GOTO 1.

3. Risk „acceptable“, or mitigation too expensive? GOTO 1.

4. Mitigate the risk you know about (and nothing else) for minimum cost, preferring technical gizmos. GOTO 1.

ICS Risk Fundamentals

1. A threat-driven approach cannot look farther than the predictability window of threats.

2. Lead time in ICS environments is measured in years.

3. New threats and vulnerabilities may pop up at any time.

Risk-based School of Thought

Event-driven: Focus on outside factors that cannot be controlled (→ threats)

Non-empirical: Use of parameters that cannot be measured (example: attack probability)

Biased: Fixation on IT components and technical point solutions that only address part of the problem

New-School (Kaizen) ICS Security Wisdom

Paradigm:
Continuous Improvement

Kaizen: Focus on

- solutions,
- internal factors that we can control,
- systems and processes in context
- long-term improvement

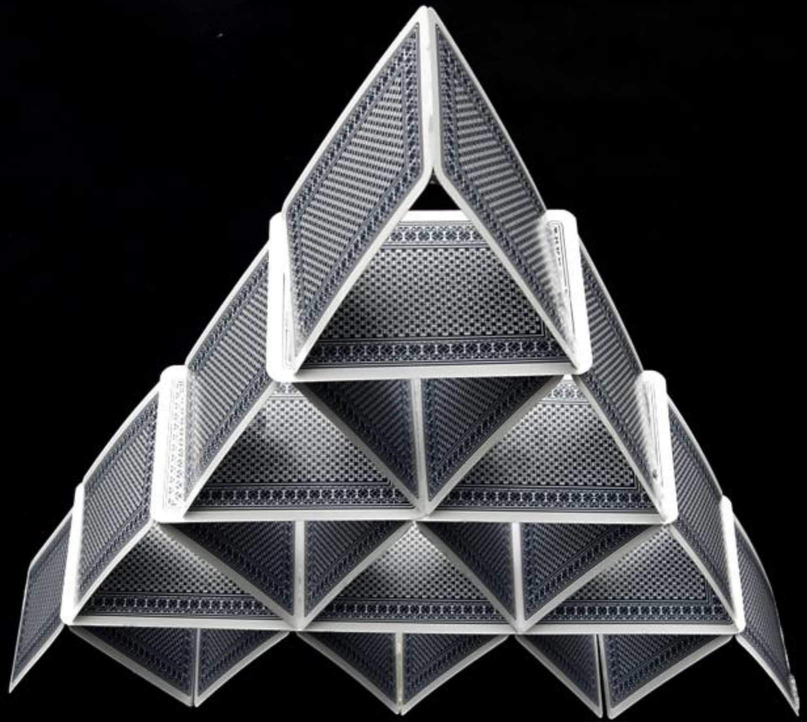
Risk & Threat: Focus on

- the magnitude of the problem,
- external events to which we try to respond,
- components in isolation (single out hot spots)
- short-term trouble control

Security as a property of process control

Process control is insecure (or fragile) to the extent that *more things can happen than planned*

→ Lack of predictability and robustness in systems and procedures



What are relevant threats to this object?

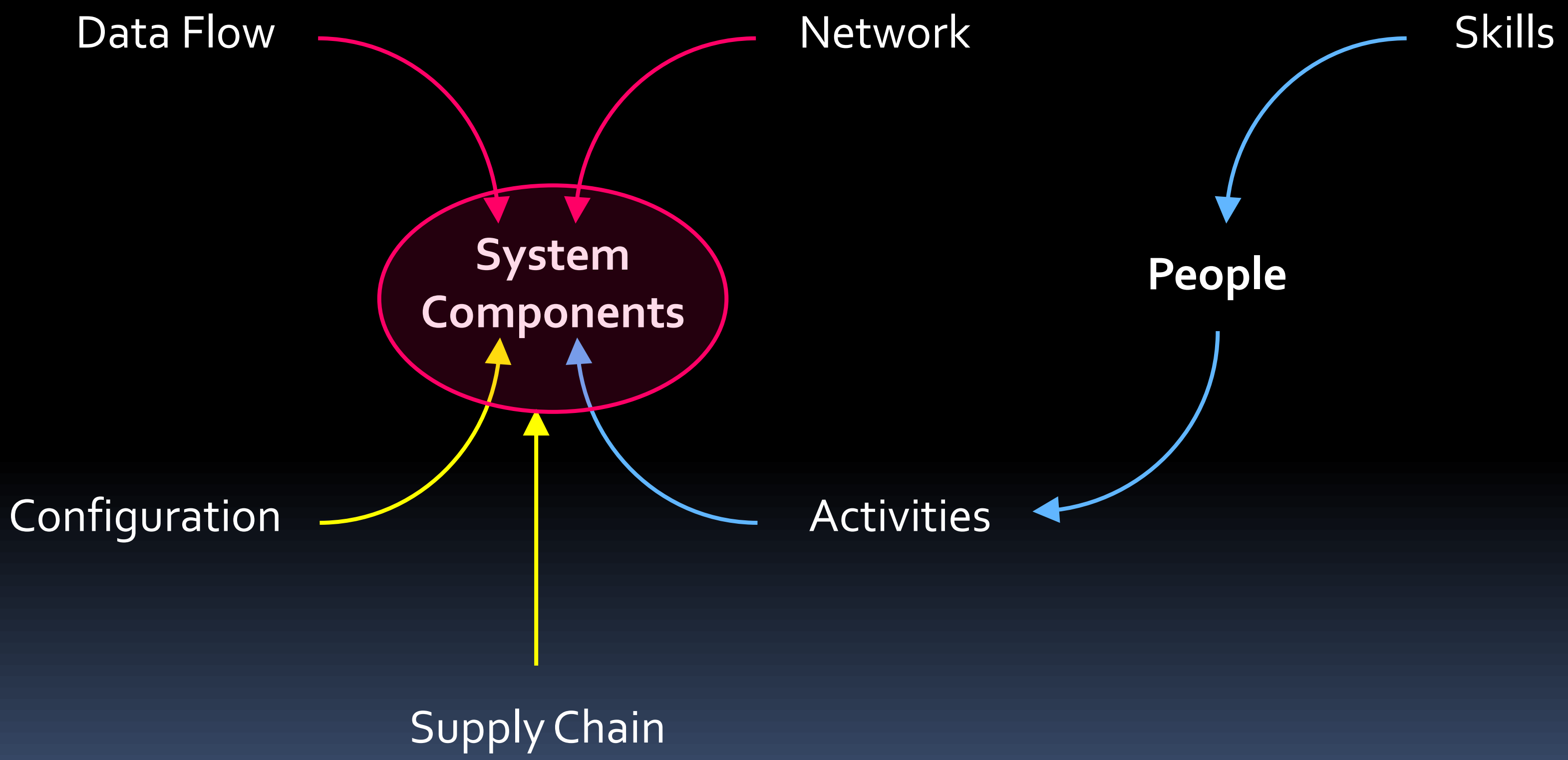
Taguchi on Quality

„Quality is evaluated by quality loss, defined as the amount of functional variation of products plus all possible negative effects, such as environmental damages and operational costs.“

Langner on ICS Security

„ICS Security is evaluated by loss of predictability, defined as the amount of functional variation of process control plus all possible negative effects, such as environmental damages and operational costs.“

360˚View: Factors that we can control

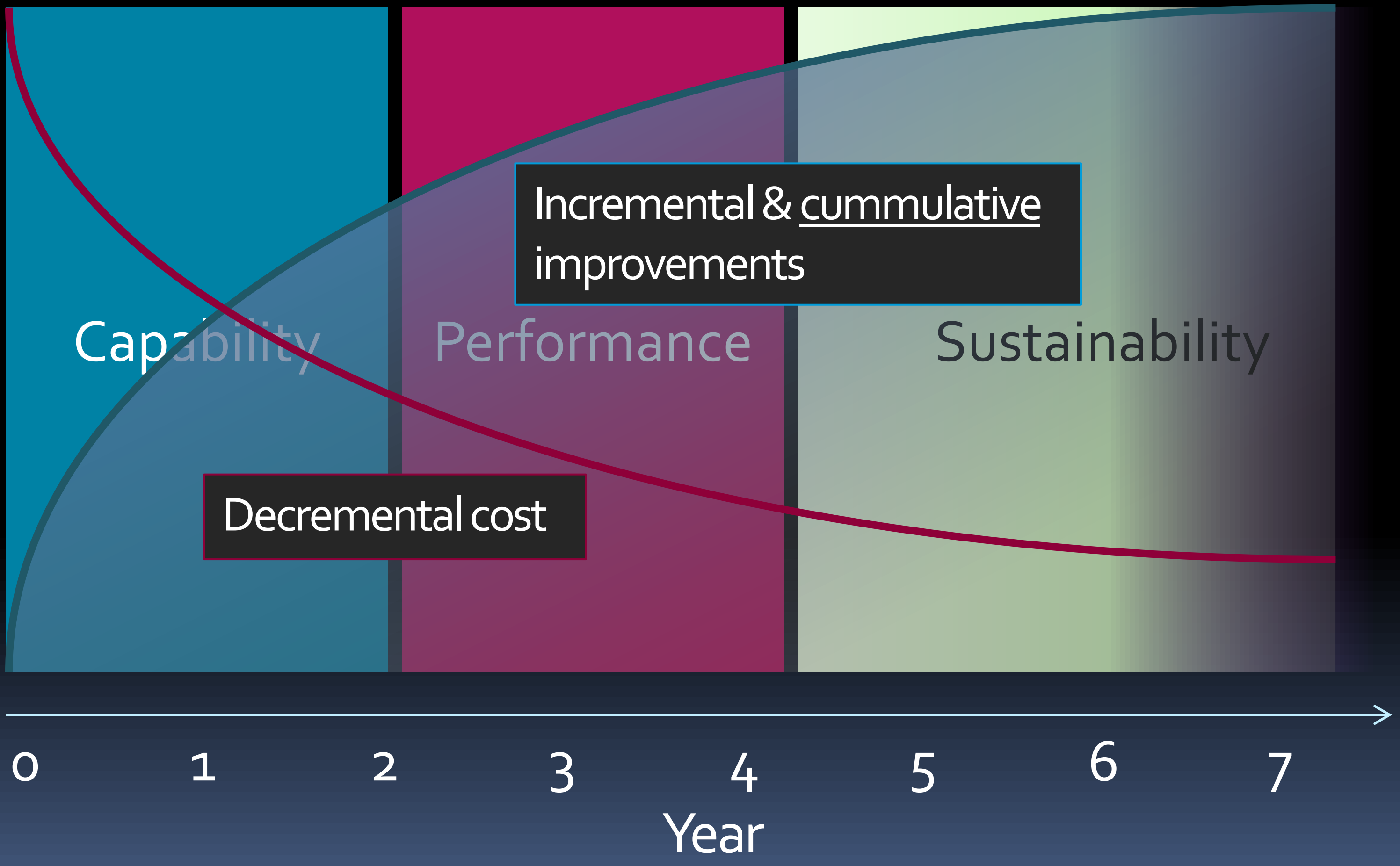


ICS Insecurity Markers

1. You don‘t know exactly which control systems are used in your plant, and their respective versions and configurations
2. You don‘t know the exact data flow and dependencies between components
3. You have inaccurate network diagrams that end at the switch level
4. You don‘t control your supply chain
5. You don‘t know exactly who your contractors are that access your ICS
6. You don‘t enforce security policies
7. You don‘t systematically train your workforce in ICS security
8. You don‘t have clear guidelines for control system design and architecture

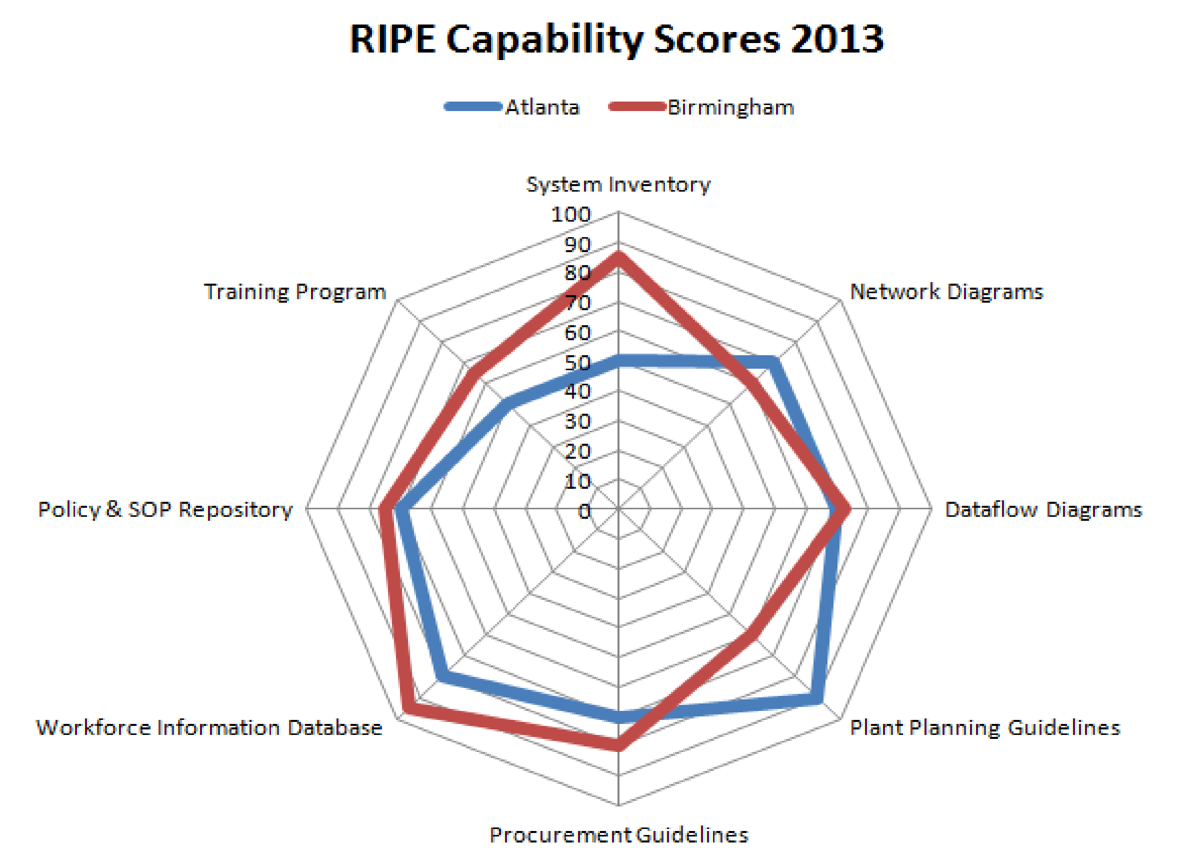
Langner

Continuous Improvement



Langner

Capability metrics & benchmarks



Recommended Reading

Langner, R.: *Robust control system networks. How to achieve reliable control after Stuxnet.* New York, Momentum Press 2012

Langner, R.: *The RIPE Framework. A process-driven approach towards effective and sustainable industrial control system security.* http://www.langner.com/en/wp-content/uploads/2013/09/The-RIPE-Framework.pdf

Langner, R.: *To kill a centrifuge. A technical analysis of what Stuxnet's creators tried to achieve.* http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

Langner, R. & Pederson, P.: *Bound to fail. Why cyber risk cannot simply be „managed" away.* http://www.brookings.edu/~/media/research/files/papers/2013/02/cyber%20security%20langner%20pederson/cybersecurity_langner_pederson_0225.pdf

Q & A

Ralph Langner

The Langner Group

Arlington | Hamburg | München

www.langner.com