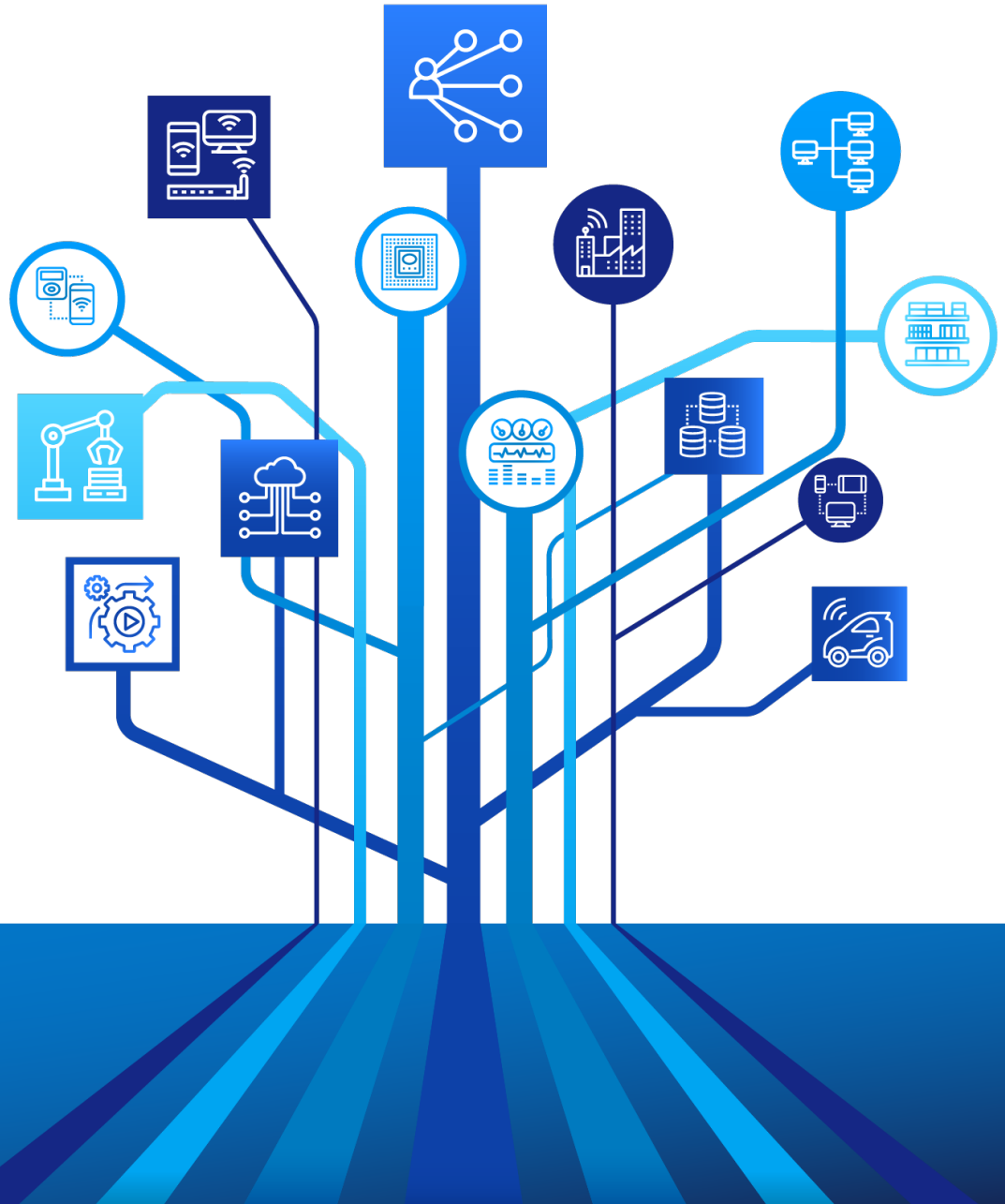
Industry IoT Consortium

Trustworthiness in Industrial IoT Systems:

Trends and issues for the future Collaborative and Computing Enterprise

Stephen J. Mellor, CTO, IIC



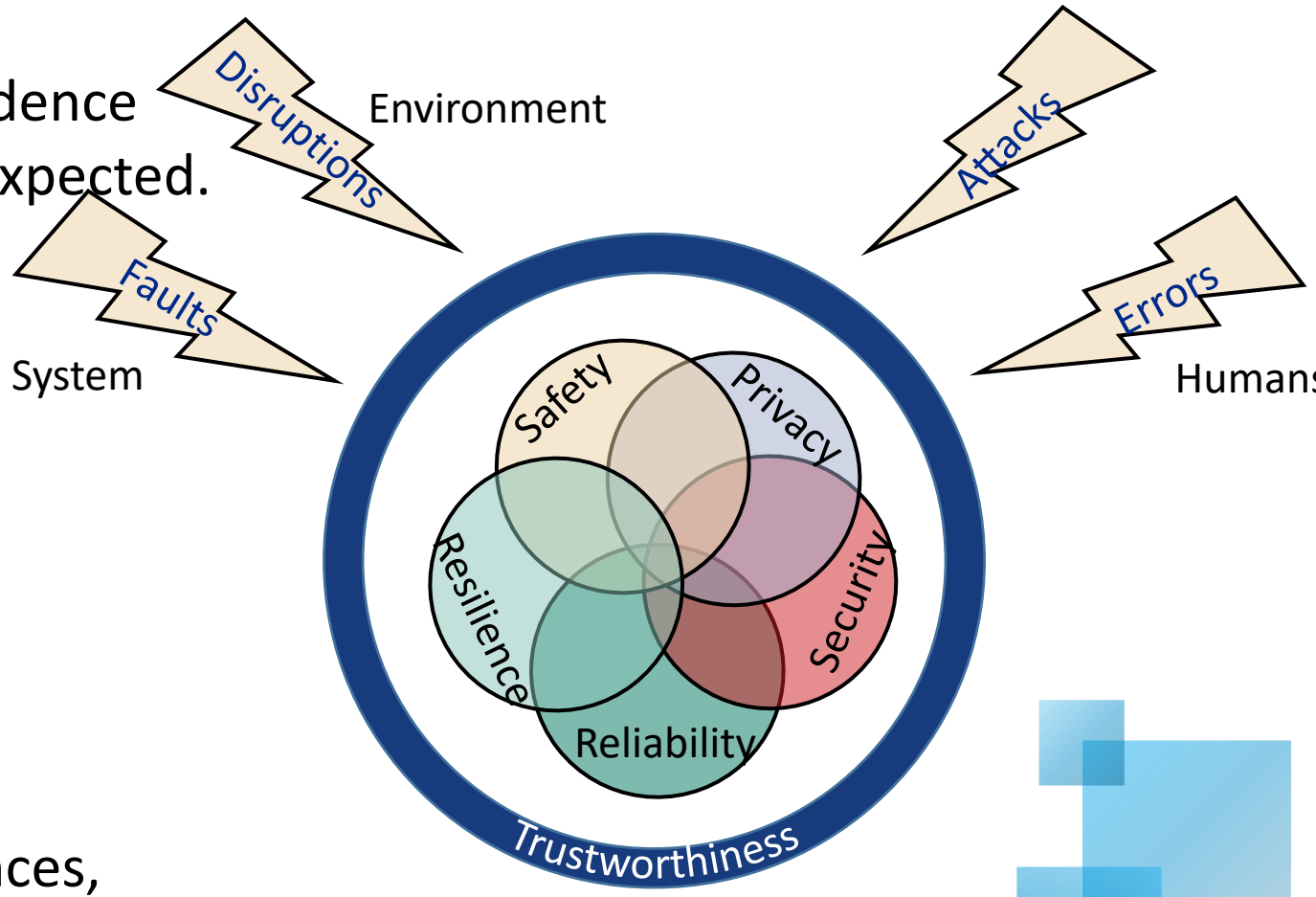
What is Trustworthiness?

Trustworthiness is the degree of confidence one has that the system performs as expected.

Characteristics include:

- safety,
- security,
- privacy,
- reliability and
- resilience

in the face of environmental disturbances, human errors, system faults and attacks.

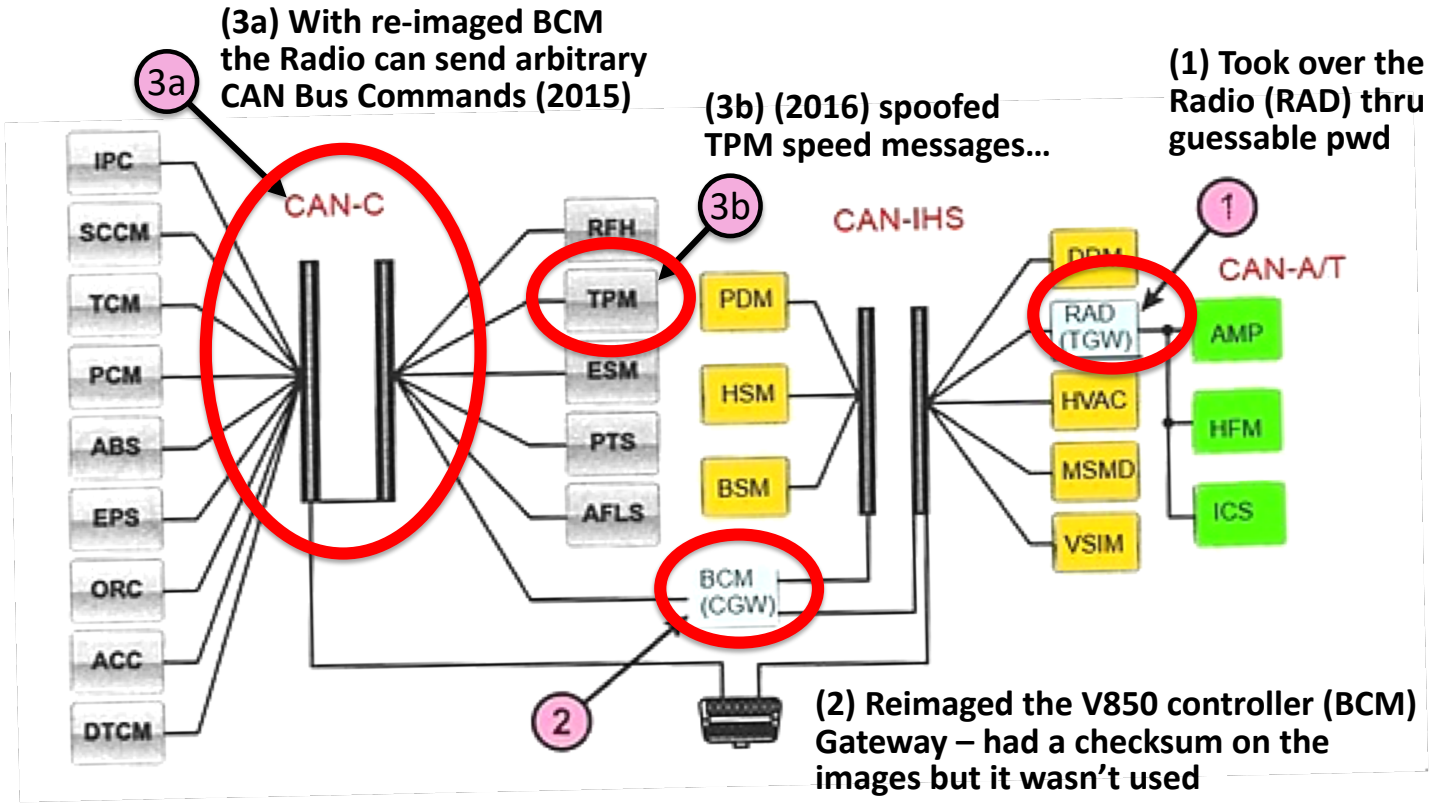


Why do you care?

In a Jeep Cherokee:

1. Easy to guess password
2. Checksum not used
3. Spoofed speed messages

You can take over the vehicle.



Charlie Miller and Chris Valasek in 2015[1] and 2016[2]

Collaborative Computing Enterprises

In industral systems, the major “collaboration” is between IT and OT.

They have different

- languages
- concerns
- time horizons
- emphases

The office floor and the shop floor are entirely different

How can they collaborate effectively?

Languages

What does “security” mean?

- barbed wire? security guards?
- firewalls? worms?

What about “safety”?

- protection from physical harm? culture?
- synonym for “security”? coding practices?

Expect not to have the same understanding.

Concerns

What concerns you daily?

- throughput/productivity?
- safety?
- physical intrusion?

- vulnerability to attack?
- crashes?
- meeting real-time constraints?

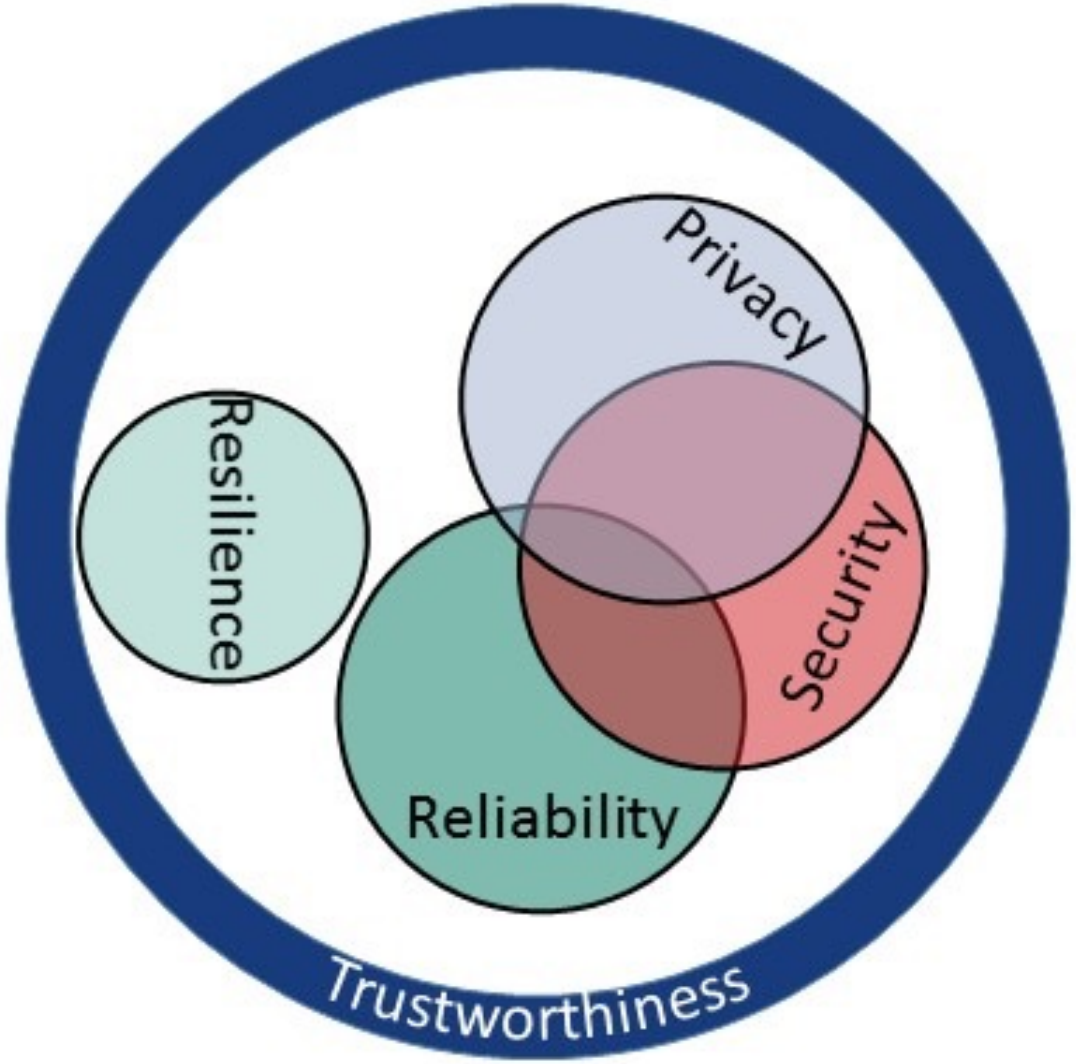
Time Horizons

How much does it cost to update your system?
How frequently? How is it authorized?

- Lots!
- Annually, unless we can avoid it!
- From the top, during scheduled shutdowns.

- Cost? What do you mean?
- Happened multiple times this month.
- Authorized? It’s automatic

Emphases: Trustworthiness in Information Technology

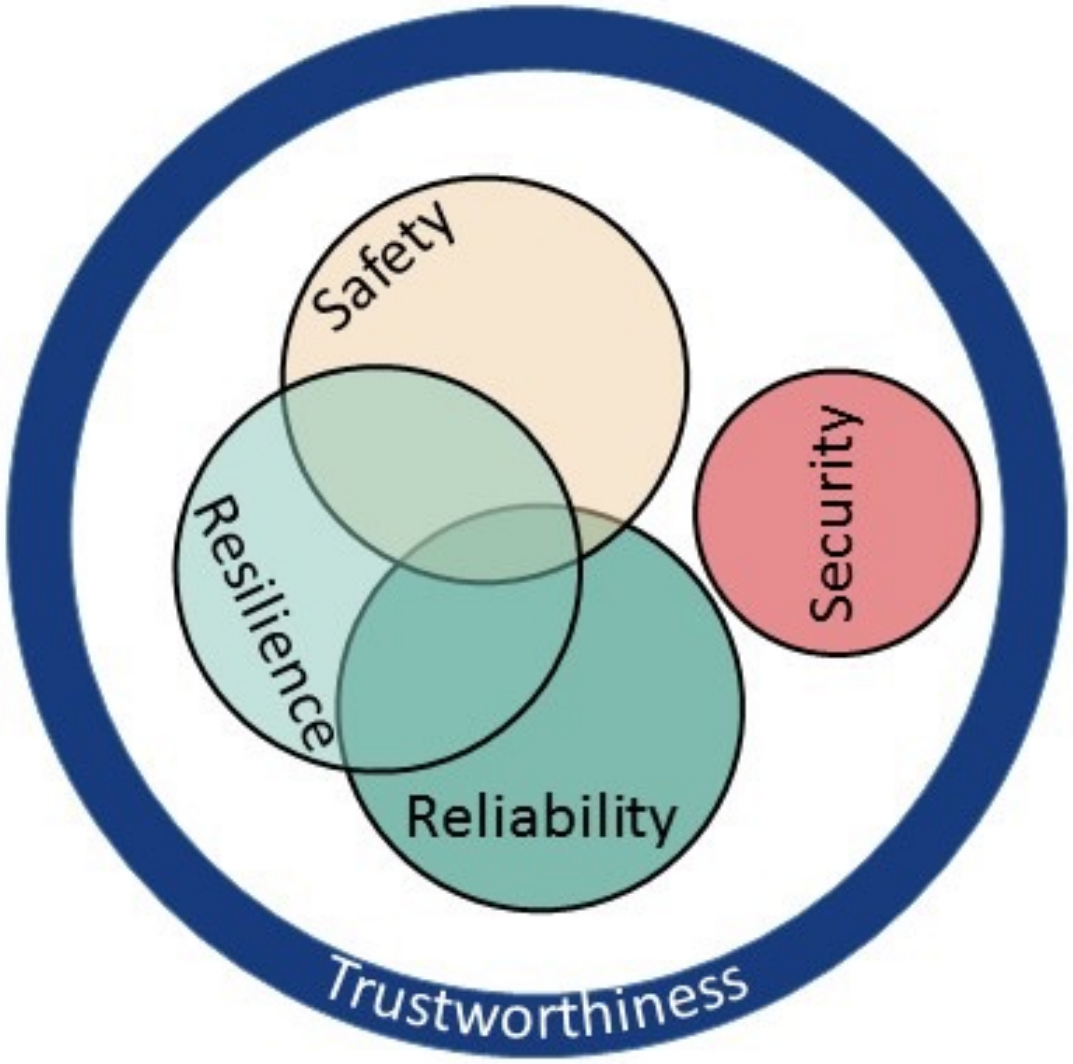


IT Security specialists focus on:

- Security first,
- then Privacy and
- Reliability.

Resilience is “interesting” for financial transactions.

Emphases: Trustworthiness in Operational Technology

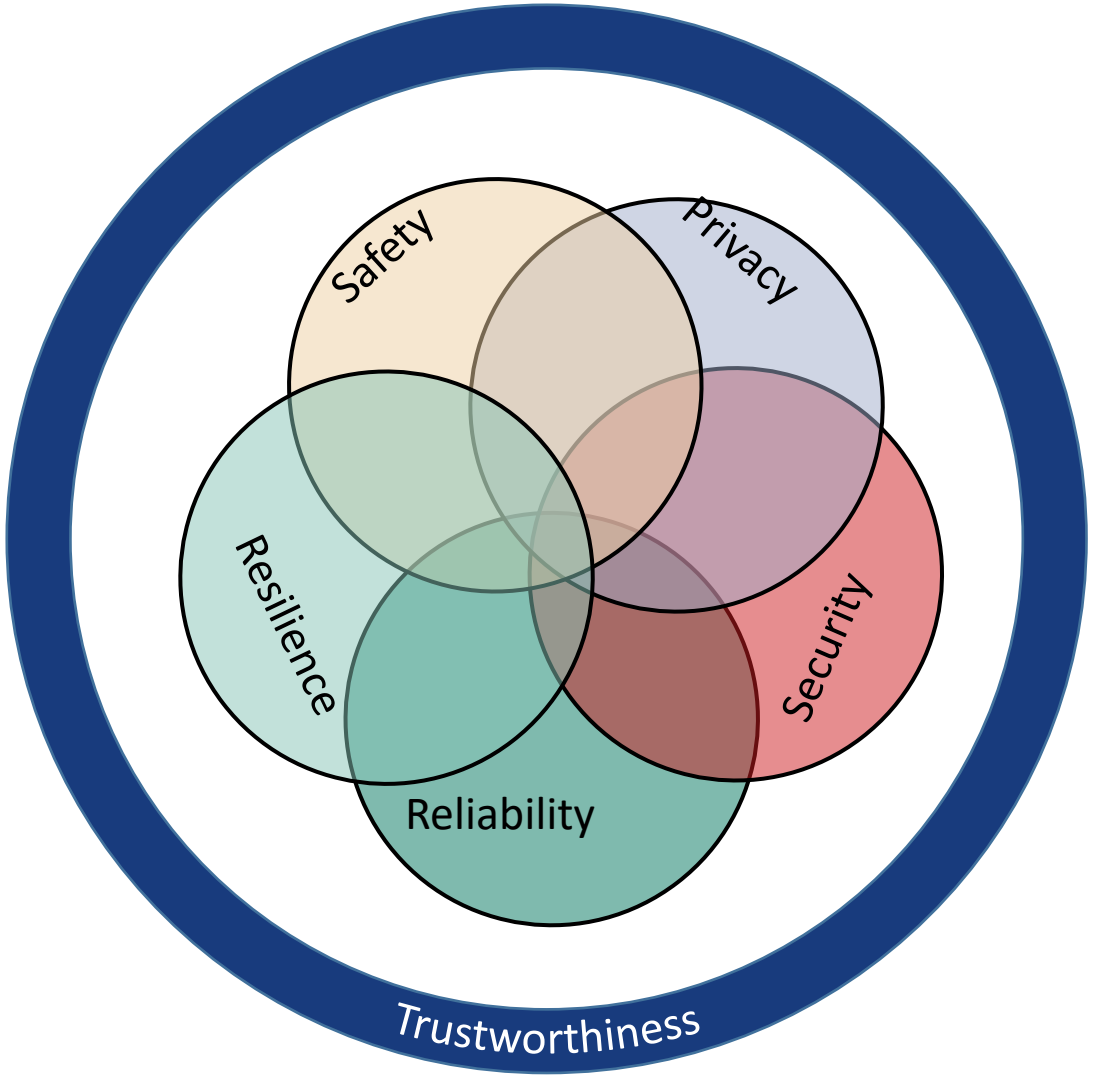


Operational Technology experts focus on:

- Safety,
- Resilience and
- Reliability

Security is “interesting” now that control sytems are connected to the Wide Wide World.

IT/OT Convergence



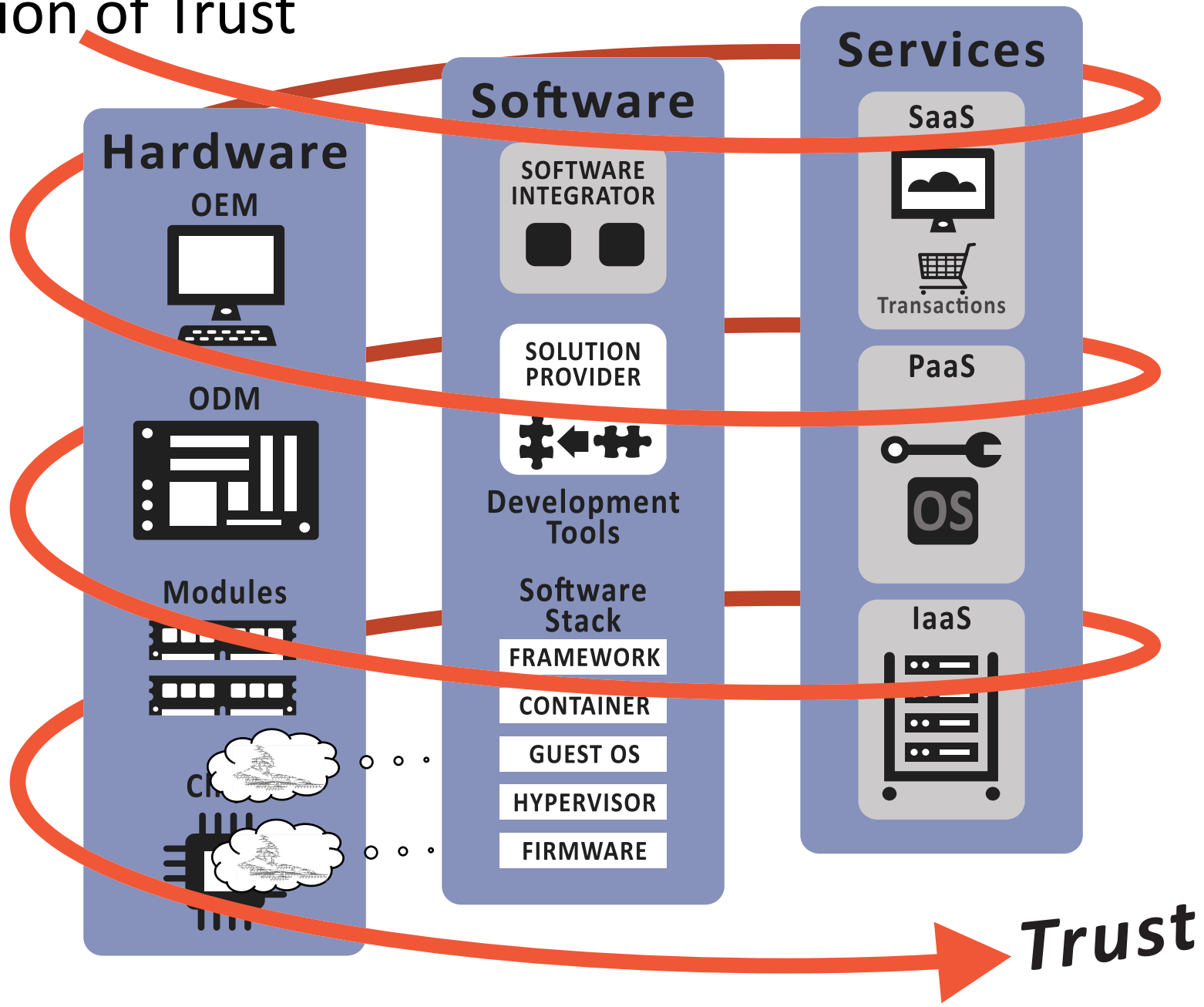
Trustworthiness is a combination of these five elements:

- Safety
- Security
- Resilience
- Reliability
- Privacy

(not only security and privacy).

These must be reconciled.

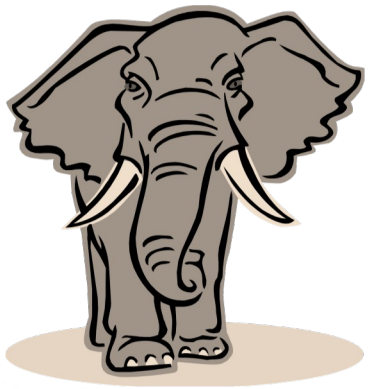
Permeation of Trust



Trust and Assurance

For trust, we need *assurance*.

Perspectives on Assurance



Insurer

- How do I underwrite?

Researcher

- What technology is needed to ensure trust?

Creator

- How should I design and build?
- Will I be liable for problems?

Community

- Do I want this in my backyard?
- Can I count on it?

Operator

- How do I use this?
- Can I trust it?
- Am I responsible if it makes a mistake?

Commander/ Supervisor

- Can I reliably use in operations?
- What changes operationally?

Regulator

- Is it safe?

Acquirer

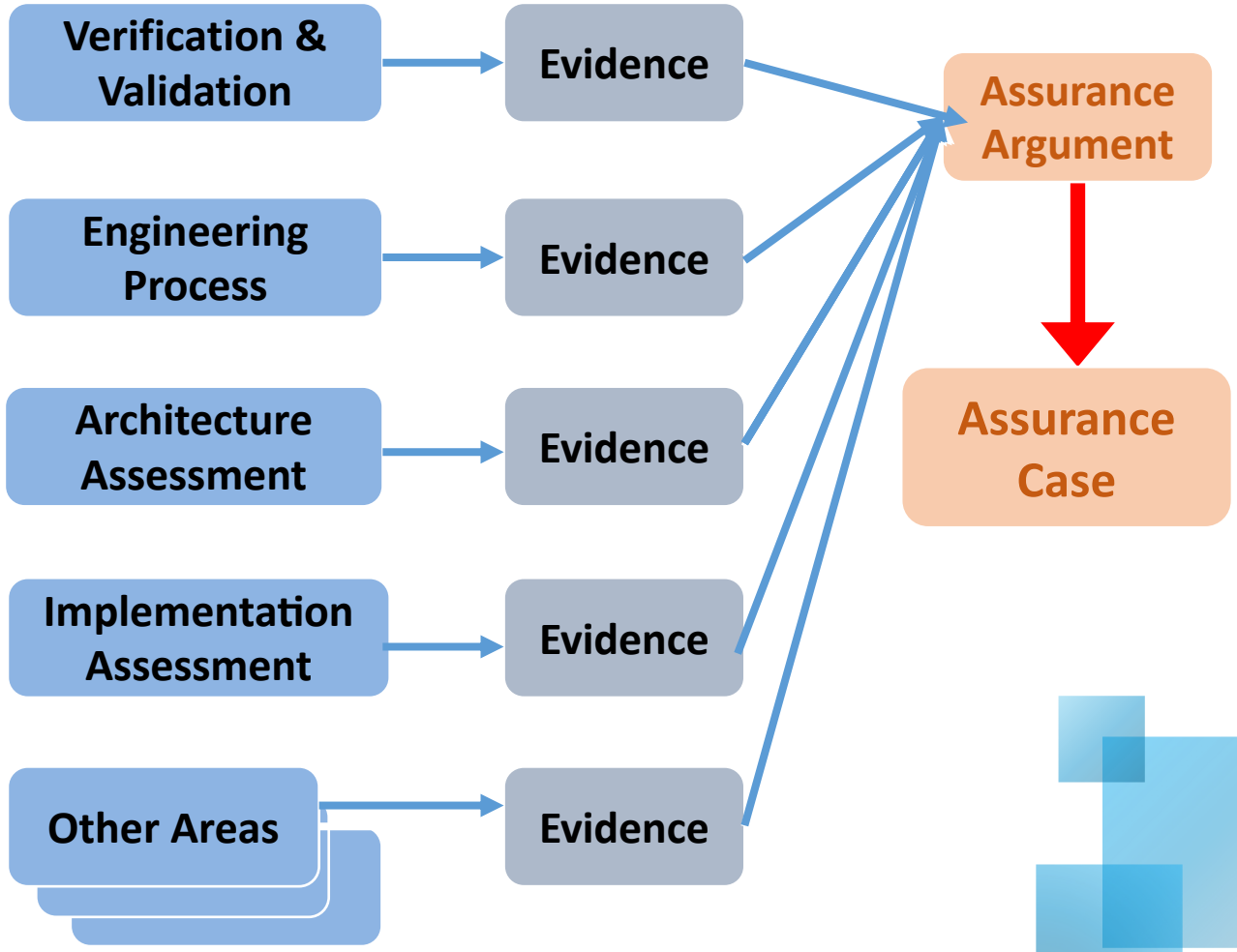
- How do I express requirements?
- Will it work they way it should?

Patron

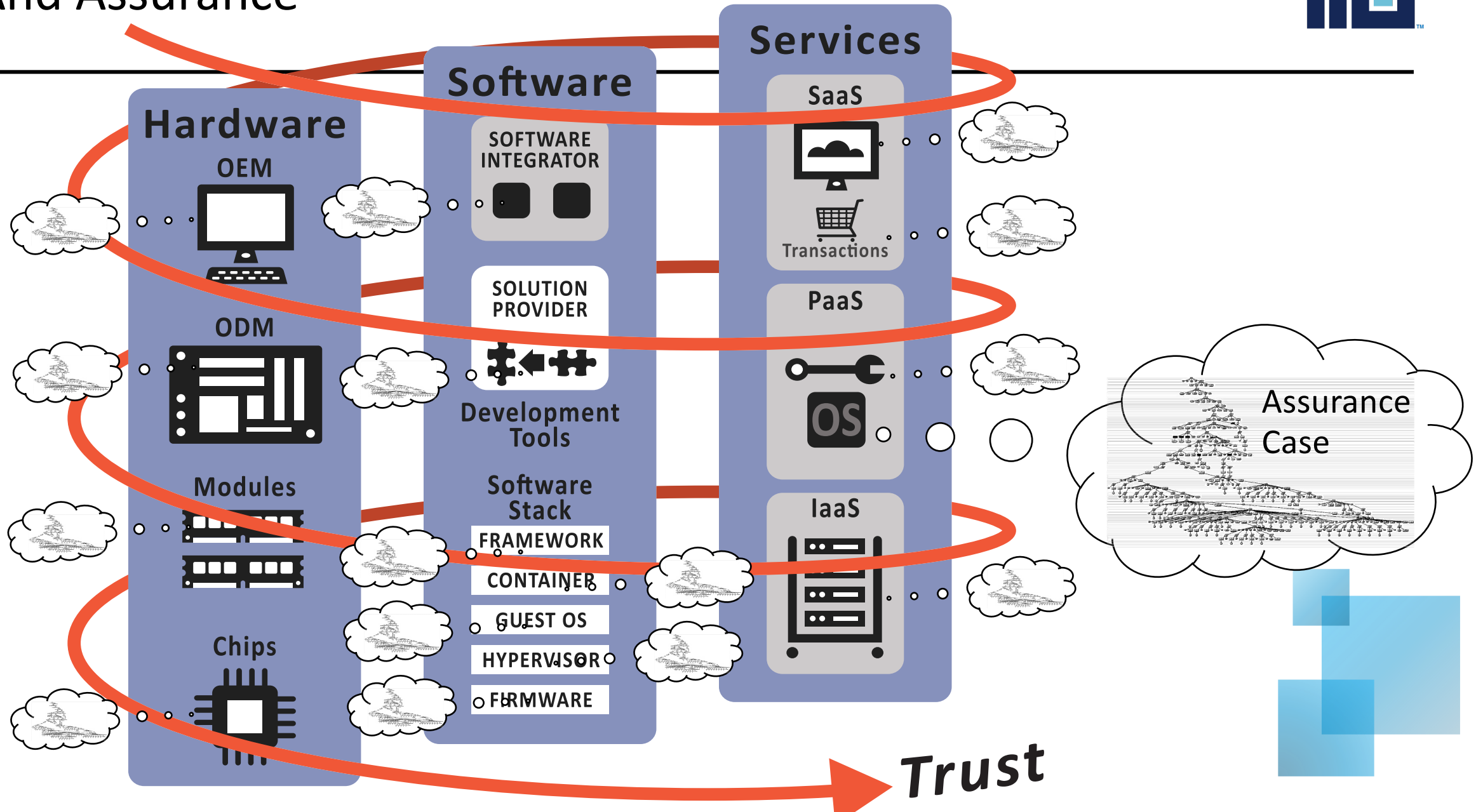
- Is it safe?
- Should I use it?
- Can I count on it?

Definition of Assurance Case

A documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding a system's properties are adequately justified for a given application in a given environment.



And Assurance



Key Messages

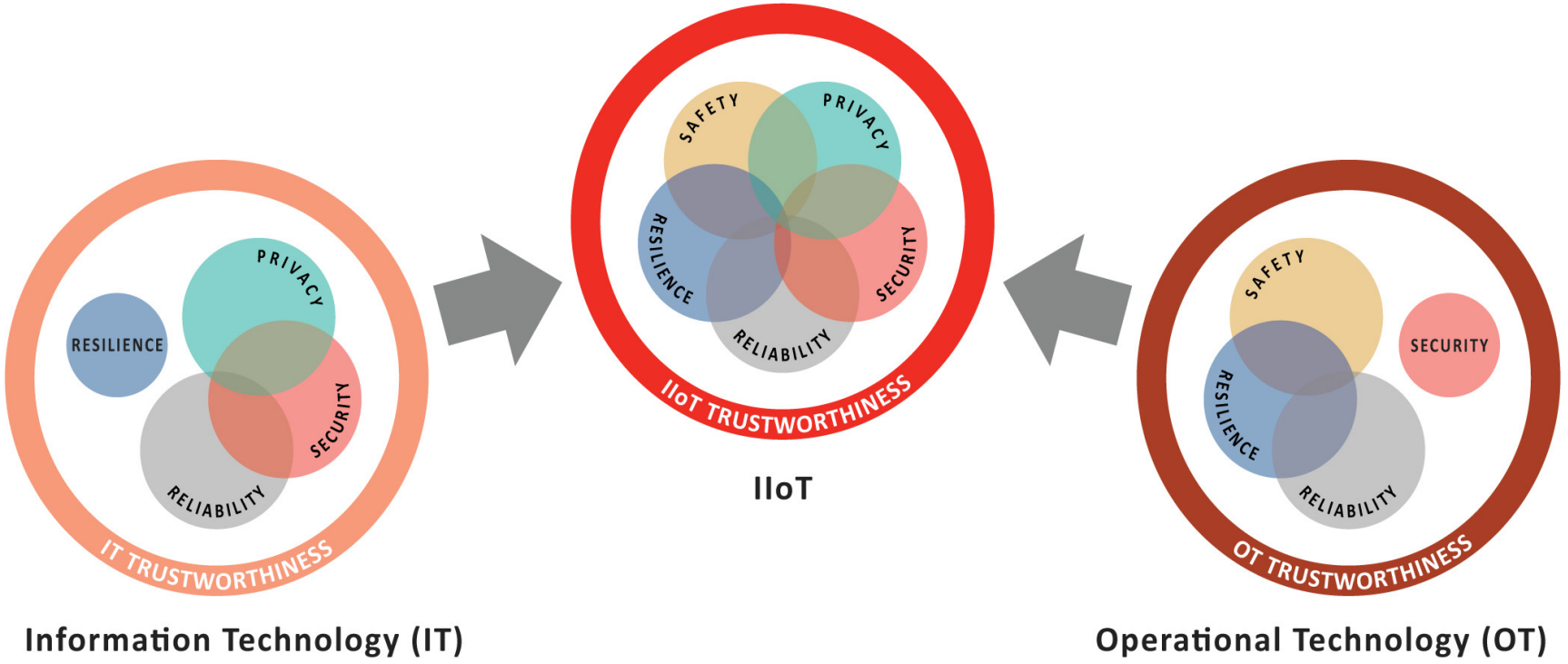
1. Trust does not happen on its own. It must be requested
2. Owners need to drive trust requirements top down
3. Trust is only achieved when capabilities that meet trust requirement are delivered and assured by the recipient
4. All players in the supply chain have a role and responsibility in delivering trust
5. Trust must exist in the components of the system, their integration and their use
6. Trust that must exist among all the vendors and suppliers that contribute to the delivery of the system and its operational use
7. Trust requires assurance

But how?

Principle 1: Trustworthiness characteristics must be considered holistically.
Principle 2: Understanding context is necessary for making Trustworthiness tradeoffs.
Principle 3: Organizational consistency over time enables reputation and trust.
Principle 4: Accountability is an essential underlying foundation of trustworthiness.
Principle 5: A culture of trustworthiness is essential to achieving trustworthiness.
Principle 6: Assurance based on evidence is essential to establish trustworthiness.
Principle 7: Software trustworthiness must be managed throughout the entire software lifecycle.
Principle 8: Implementing trustworthiness means implementing trustworthiness methods
Principle 9: Maintaining change and audit records is necessary for trustworthiness.
Principle 10: A trustworthiness framework must enable timely business decisions.
Principle 11: Assurance requires a systems viewpoint with evidence of multiple factors.

Principle 1

Trustworthiness characteristics must be considered holistically.



Varying weights are given to each characteristic by each community.

Principle 2

Understanding context is necessary for making trustworthiness tradeoffs.

There are multiple differences in context:

- Company differences
- Local environment
- Balancing aspects of trustworthiness in different industries
- Affected parties

Principles 3 & 4

Organizational consistency over time enables reputation and trust.

Accountability is an essential underlying foundation of trustworthiness.

Principle 5

A culture of trustworthiness is essential to achieving trustworthiness.

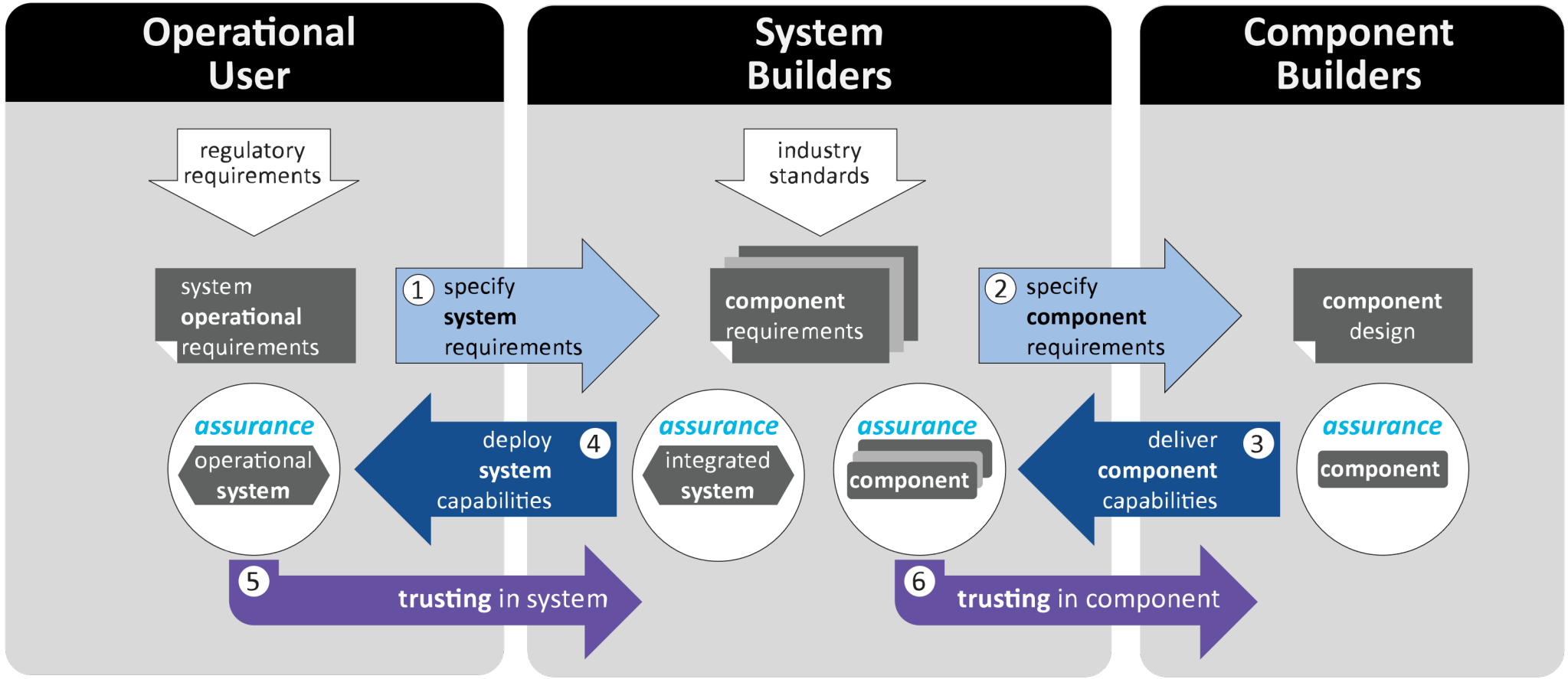
If the organization does not support trustworthiness, it won't happen:

- separate teams for development and monitoring
- free from undue influence from budget or management

This is especially true in software.

Principle 6

Assurance based on evidence is essential to establish trustworthiness.



Principle 7

Software trustworthiness must be managed through the lifecycle.

Techniques include:

- Software composition must be managed:
  - software bill of materials,
  - and how it was built.
- Software protection: software executables must be resistant to modification and hinder discovery of the intellectual property.

throughout the lifecycle: including creation, operation, updating and decommissioning.

Principle 8

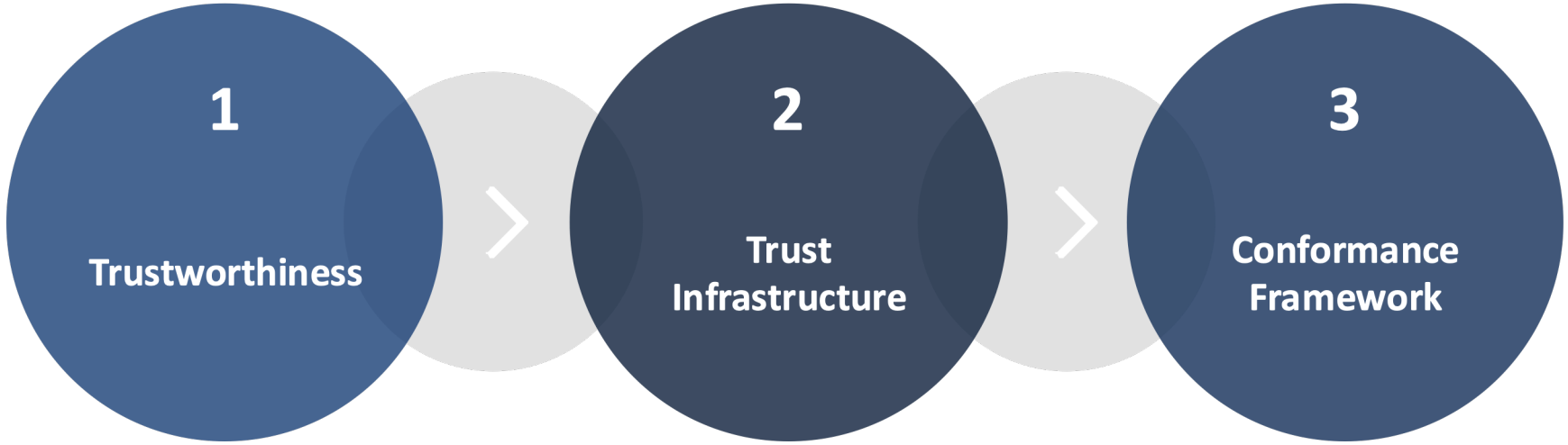
Implementing trustworthiness means implementing *trustworthiness methods*.

Examples:

- *Fire extinguisher*: a tool and a safety method
- CO2 fire suppression system*:* a tool and a resilience method.
- *Network firewall*: a tool and a security method.
- *Melt-resistant steel*: technology and a resilience method.
- *Windmill restart:* operational procedure for airplanes during an engine flameout and a resilience method.
- *Encryption of all social security numbers on servers*: management directive and a privacy method.

Principle 9

Maintaining change and audit records is necessary for trustworthiness.



measurement of security, safety, reliability, resilience and privacy as well as other optional trustworthiness characteristics

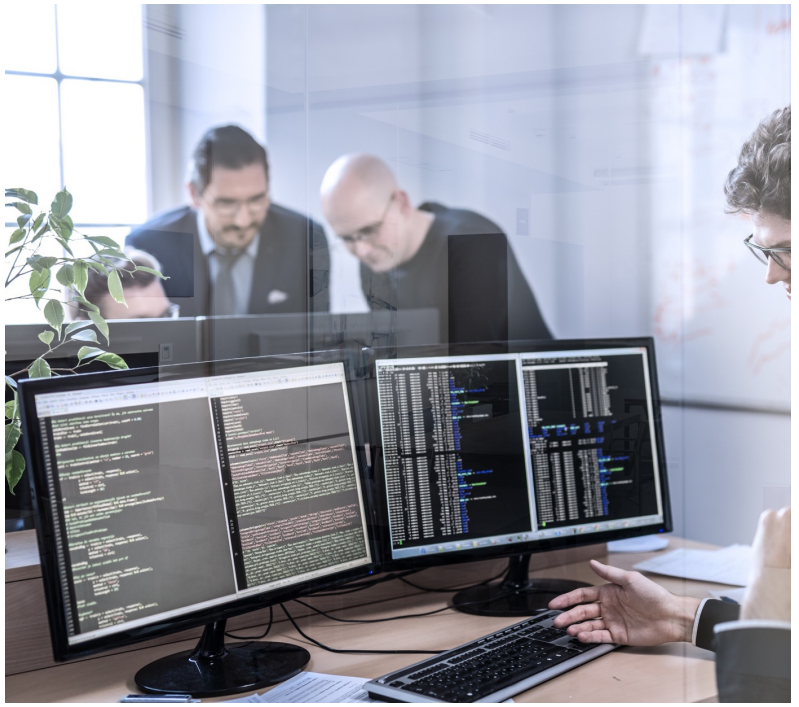
transparency
traceability
trust rating

compliance
sustainability

Principle 10

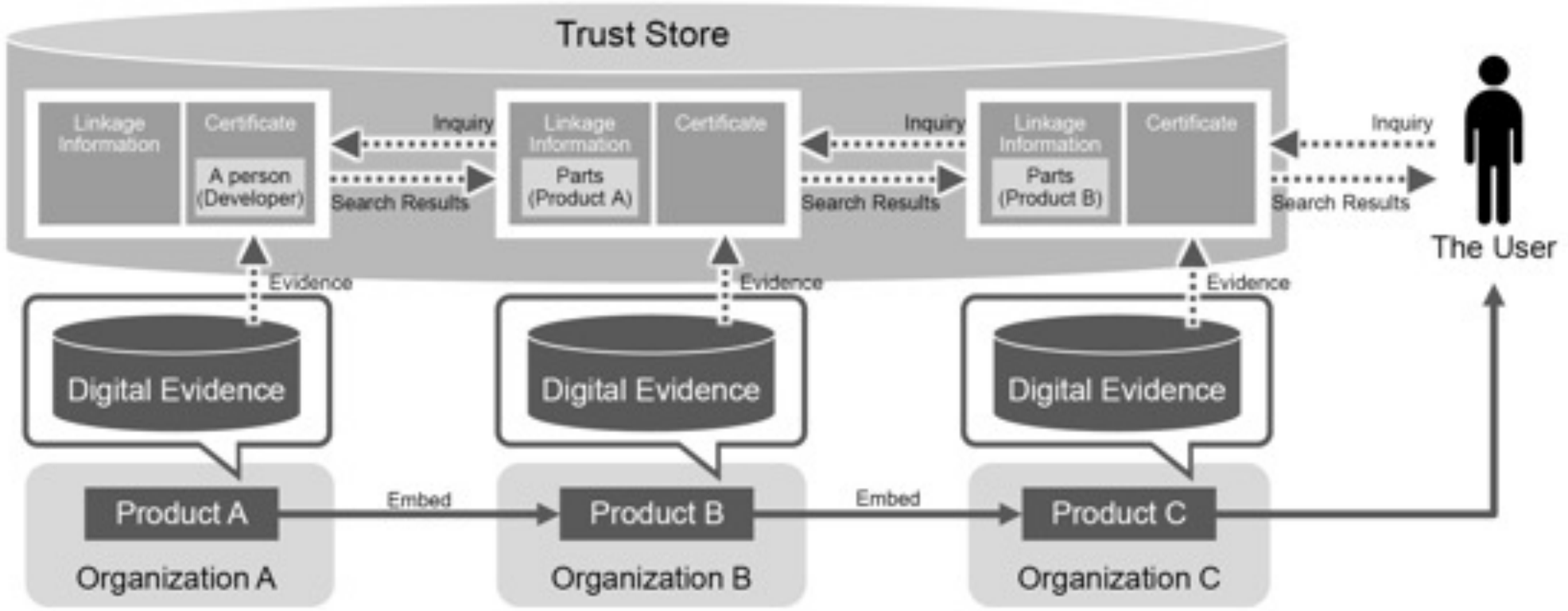
A trustworthiness framework must enable timely business decisions to gain confidence that the system performs as expected.

- transparent and traceable
- measuring trustworthiness must be rigorous, pragmatic, and address operating concerns
- make decisions in a timely manner
- intuitive and actionable so that organizations



Principle 11

Assurance requires a systems viewpoint with evidence of multiple factors.



You can’t live without trustworthiness!

Principle 1: Trustworthiness characteristics must be considered holistically.
Principle 2: Understanding context is necessary for making Trustworthiness tradeoffs.
Principle 3: Organizational consistency over time enables reputation and trust.
Principle 4: Accountability is an essential underlying foundation of trustworthiness.
Principle 5: A culture of trustworthiness is essential to achieving trustworthiness.
Principle 6: Assurance based on evidence is essential to establish trustworthiness.
Principle 7: Software trustworthiness must be managed throughout the entire software lifecycle.
Principle 8: Implementing trustworthiness means implementing trustworthiness methods
Principle 9: Maintaining change and audit records is necessary for trustworthiness.
Principle 10: A trustworthiness framework must enable timely business decisions.
Principle 11: Assurance requires a systems viewpoint with evidence of multiple factors.

Questions?

mellor@omg.org

hub.iiconsortium.org
www.iiconsortium.org

info@iiconsortium.org

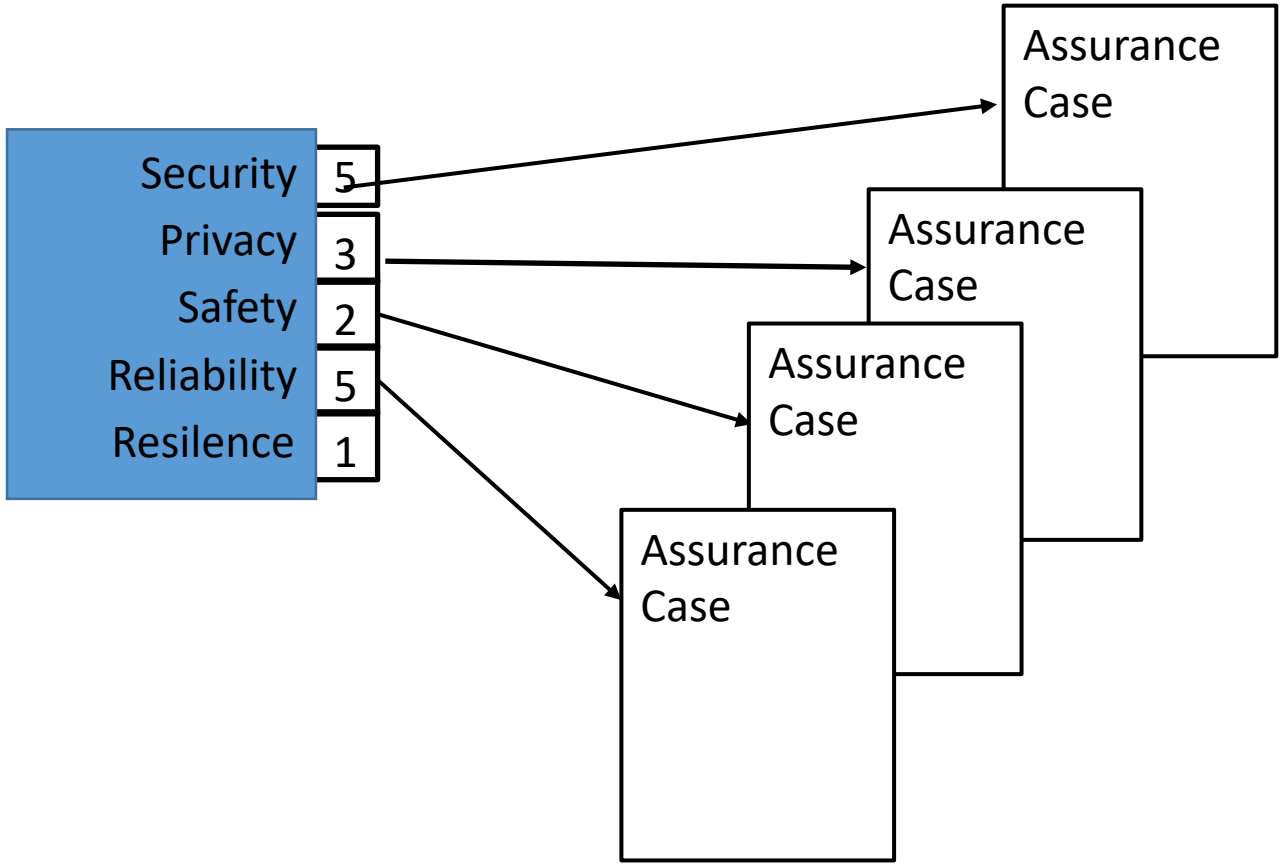
Trusted Enterprise

Trustworthiness is difficult enough to establish for a single system.

What about collaborating systems?

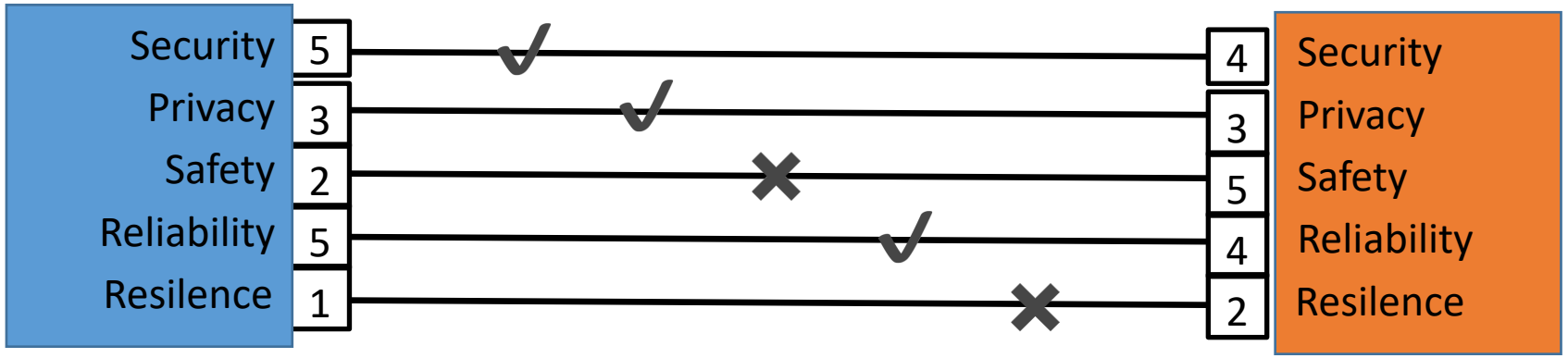
Trust Vectors (Supplied)

What is the trustworthiness level of another system component?



Trust Vectors (Required)

What level of trustworthiness do I need?



Questions?

mellor@omg.org

hub.iiconsortium.org
www.iiconsortium.org

info@iiconsortium.org