Perspectives on Trustworthiness

**Insurer**
- How do I underwrite?

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

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

**Regulator**
- Is it safe?

**Researcher**
- What technology is needed to ensure trust?

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

**Acquirer**
- How do I express requirements?
- Will it work the way it should?

**Commander/Supervisor**
- Can I reliably use in operations?
- What changes operationally?

**Patron**
- Is it safe?
- Should I use it?
- Can I count on it?
Claims, Arguments, and Evidence

Claim = assertion to be proven

Argument = how evidence supports claim

Evidence = required documentation
Safety Case Tooling – Claims-Evidence-Argument in Use for <17 Years

Legend:
- Green = Low Risk
- Yellow = Medium Risk
- Red = High Risk
- ← = “Is solved by”
- ▽ = “In context of”

- Clm1: Top-Level Claim
  - Ctx1: Context
  - Clm2: Sub-Claim
    - Ev1: Evidence
  - Clm3: Sub-Claim
    - Ev1: Evidence
  - Clm4: Sub-Claim
    - Ev3: Evidence
  - Clm5: Sub-Claim
    - Assumption A

© 2017 MITRE. All rights reserved, all other material used with permission.
OMG Structured Assurance Case MetaModel

Exchange and Composition of Assurance Cases between tools and programs

© 2017 MITRE. All rights reserved, all other material used with permission.

Approved for Public Release; Distribution Unlimited. Case Number 17-3226-002
The Key System Characteristics of Trustworthiness as a Quality Measure

- Industrial IoT Quality is a continuum of system characteristics within a context
  - OT Safety (IEC 62443*) meets IT Security (ISO 27000*)
  - Privacy (GDPR*), Resilience (ISO*, IEC*), Reliability (NIS*) are quality features in both OT and IT
  - Determine and ensure quality measures per vertical, e.g. audit, certification

* examples

© 2017 MITRE. All rights reserved, all other material used with permission.
Composition of a Trustworthiness Quality Measure

**Resilience**
- EU: NIS
- UK: … (after Brexit)
- US: …
- CN: ()
- JP: analog NIS

**Reliability**
- Art 1
- Art 2
- Art 3
- Art 4
- Art 5
- Art 6
- Art 7

**Security**
- EU: GDPR
- UK: … (after Brexit)
- US: …
- CN: ()
- JP: analog GDPR

**Privacy**
- EU: GDPR
- UK: … (after Brexit)
- US: …
- CN: ()
- JP: analog GDPR

**Safety**
- EU: IEC 61508/62626
- UK: … (after Brexit)
- US: IEC 61508
- CN: ()
- JP: IEC 61508

* examples

© 2017 MITRE. All rights reserved, all other material used with permission.
Evidence of Trustworthiness as Assurance Cases

- **Resilience**: Evidence-based Assurance Case supporting Resilience claims
- **Reliability**: Evidence-based Assurance Case supporting Reliability claims
- **Security**: Evidence-based Assurance Case supporting Security claims
- **Privacy**: Evidence-based Assurance Case supporting Privacy claims
- **Safety**: Evidence-based Assurance Case supporting Safety claims

Examples:
- EU: NIS
- UK: … (after Brexit)
- US: …
- CN: ()
- JP: analog NIS

- EU: GDPR
- UK: … (after Brexit)
- US: …
- CN: ()
- JP: analog GDPR

- EU: IEC 61508/62626
- UK: … (after Brexit)
- US: IEC 61508
- CN: ()
- JP: IEC 61508
Evidence-based Assurance Case supporting Trustworthiness claims
Industrial Internet Reference Architecture

17 REFERENCES

