Fraunhofer AISEC

Architecture-Derived CBOMs for Cryptographic Migration: A Security-Aware Architecture Tradeoff Method

Eduard Hirsch and Kristina Raab

Kristina Raab, May 10, 2026

Outline

Motivation and Problem Statement

Cryptographic systems face continuous change:

- Algorithms get deprecated
- Regulatory requirements impose new obligations
- Post-quantum transition approaching
- What will come in future?

To manage this continous change, organizations need to know what cryptography they are running → CBOMs

CBOMs answer...

- ✓ *Which* algorithms are used?
- ✓ *Where* are they found in the system?

CBOMs do not answer:

- × *Why* is this algorithm here?
- × Which *threat* does it mitigate?
- × What *breaks* if I replace it?
- × What *migration risk* is attached?

Research Gap and Paper Objectives

Research Gap

Inventory-based CBOMs lack architectural context, design decisions and security rationale
→ **migration planning disconnected from system-level effects**

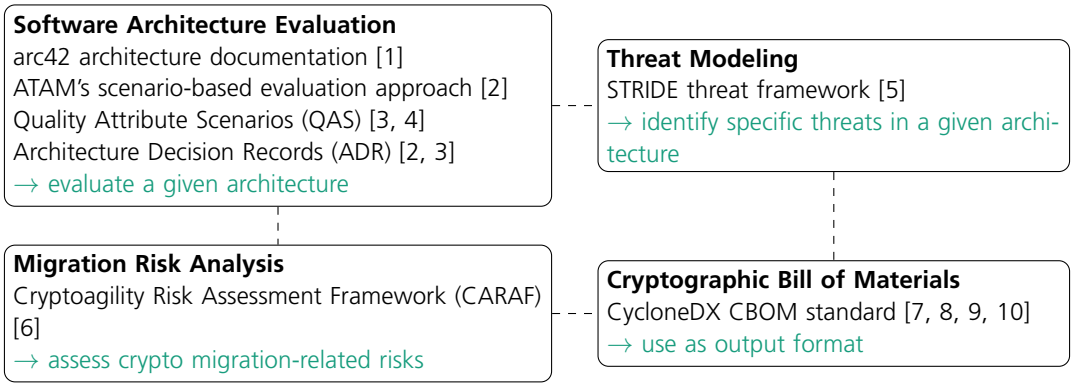
Paper Objectives

Design a Security-Aware Architecture Tradeoff Analysis Method (SATAM)

1. Follow a Design Science Research approach to create a method-level artifact
2. Integrate concepts from architecture evaluation, threat modeling, and migration risk analysis
3. Deliver an CycloneDX-compatible, architecture-driven CBOM as output
4. Evaluate in a proof of concept

Background: SATAM Building Blocks

SATAM does not introduce new techniques from scratch – it integrates four established bodies of work that have, until now, been applied in isolation:



SATAM Phases (adapted from ATAM with security-specific activities and artifacts)

Preparation & Kickoff Phases

- Identify who is accountable for crypto decisions (stakeholders)
- Build security-readable arc42 architecture baseline (trust boundaries and crypto assets explicit)
- Define CBOM ownership
- Establish CBOM as SATAM evaluation output

Evaluation Phase

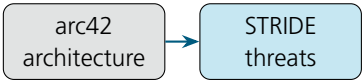
SATAM core: traceability chain

SATAM Traceability Chain

arc42
architecture

I. arc42: contextualizes all **architectural elements** and allows to locate **cryptographic assets** in their architectural context

SATAM Traceability Chain



I. arc42: contextualizes all **architectural elements** and allows to locate **cryptographic assets** in their architectural context

II. STRIDE: applied to specific data flows and trust boundaries to identify **threats**

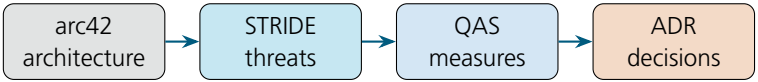
SATAM Traceability Chain

I. arc42: contextualizes all **architectural elements** and allows to locate **cryptographic assets** in their architectural context

II. STRIDE: applied to specific data flows and trust boundaries to identify **threats**

III. QAS: threats transformed into concrete **cryptographic response measures** under architectural constraints

SATAM Traceability Chain



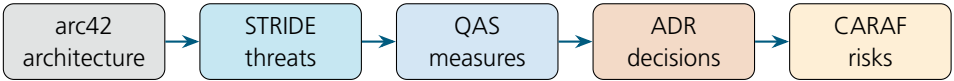
I. arc42: contextualizes all **architectural elements** and allows to locate **cryptographic assets** in their architectural context

II. STRIDE: applied to specific data flows and trust boundaries to identify **threats**

III. QAS: threats transformed into concrete **cryptographic response measures** under architectural constraints

IV. ADR: measures translate into **architectural requirements**; capture **decision**, **rationale** and **consequences**

SATAM Traceability Chain



I. arc42: contextualizes all **architectural elements** and allows to locate **cryptographic assets** in their architectural context

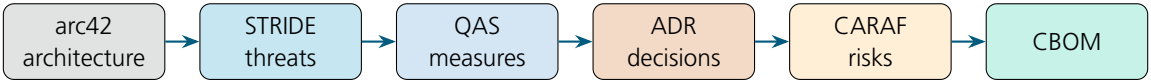
II. STRIDE: applied to specific data flows and trust boundaries to identify **threats**

III. QAS: threats transformed into concrete **cryptographic response measures** under architectural constraints

IV. ADR: measures translate into **architectural requirements**; capture **decision**, **rationale** and **consequences**

V. CARAF: ADR fed into CARAF to assess **migration risk** using **Mosca's Theorem**

SATAM Traceability Chain



I. arc42: contextualizes all **architectural elements** and allows to locate **cryptographic assets** in their architectural context

II. STRIDE: applied to specific data flows and trust boundaries to identify **threats**

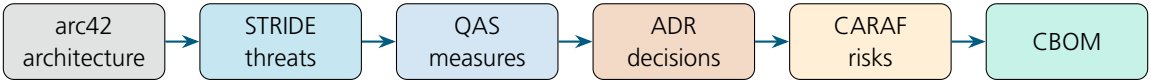
III. QAS: threats transformed into concrete **cryptographic response measures** under architectural constraints

IV. ADR: measures translate into **architectural requirements**; capture **decision**, **rationale** and **consequences**

V. CARAF: ADR fed into CARAF to assess **migration risk** using **Mosca's Theorem**

VI. CBOM: all steps consolidated into **machine-readable CBOM** with full architectural context per entry

SATAM Traceability Chain



I. arc42: contextualizes all **architectural elements** and allows to locate **cryptographic assets** in their architectural context

II. STRIDE: applied to specific data flows and trust boundaries to identify **threats**

III. QAS: threats transformed into concrete **cryptographic response measures** under architectural constraints

IV. ADR: measures translate into **architectural requirements**; capture **decision**, **rationale** and **consequences**

V. CARAF: ADR fed into CARAF to assess **migration risk** using **Mosca's Theorem**

VI. CBOM: all steps consolidated into **machine-readable CBOM** with full architectural context per entry

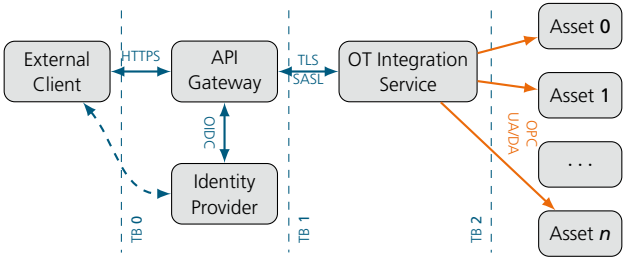
SATAM is a continuous process:

changes in architectural elements propagate along the traceability chain

Proof of Concept – Step I: arc42 Architecture

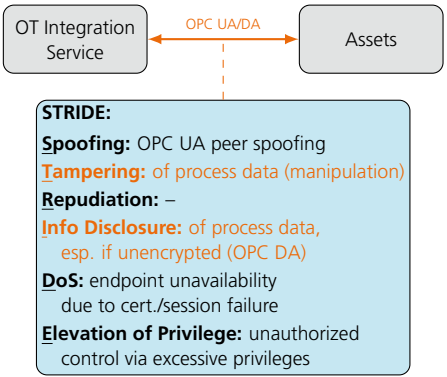
Examplary industrial OT architecture as arc42 baseline:

- Three explicit trust boundaries (TB)
- External client communicates with OT network via API gateway and OT integration service
- OT integration service communicates with industrial assets via protocols OPC UA (modern, security-capable) and legacy OPC DA (no cryptographic protection, deliberate weak point)



Proof of Concept – Step II: STRIDE Threats & Step III: QAS Measures

STRIDE threat framework applied to data flow:



Proof of Concept – Step II: STRIDE Threats & Step III: QAS Measures

STRIDE threat framework applied to data flow:

STRIDE:

Spoofing: OPC UA peer spoofing

Tampering: of process data (manipulation)

Repudiation: –

Info Disclosure: of process data, esp. if unencrypted (OPC DA)

DoS: endpoint unavailability due to cert./session failure

Elevation of Privilege: unauthorized control via excessive privileges

QAS cryptographic response measures under architectural constraints:

QAS-OT-OPC-1:

Source: attacker in IT/OT network

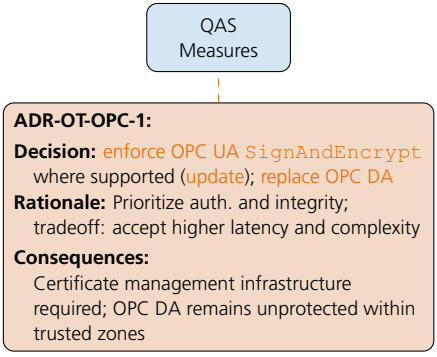
Stimulus: info. disclosure (I) and/or tampering (T) of process data

Response: auth. and integrity enforced for OPC UA (`SignAndEncrypt`); OPC DA legacy risks controlled

Measures: auth. failures rejected at handshake; integrity violations detected within one cycle; latency below given threshold; availability above 99.9 % during cert. rotation; OPC DA confined to high-risk trusted zones

Proof of Concept – Step IV: ADR Decisions & Step V: CARAF Risks

ADR architectural decision based on QAS:



Proof of Concept – Step IV: ADR Decisions & Step V: CARAF Risks

ADR architectural decision based on QAS:

QAS Measures

ADR-OT-OPC-1:

Decision: enforce OPC UA `SignAndEncrypt` where supported (update); replace OPC DA

Rationale: Prioritize auth. and integrity; tradeoff: accept higher latency and complexity

Consequences: Certificate management infrastructure required; OPC DA remains unprotected within trusted zones

CARAF migration risk assessment based on Mosca's Theorem:

CARAF-OT-OPC-1:

X: required process data lifetime

Y: migration time to enforce `SignAndEncrypt` (phased rollout), replace OPC DA (legacy client/hardware interface replacement)

Z: quantum horizon

X + Y > Z → action required now

Crypto asset	Migration risk
OPC UA *SignAndEncrypt*	150 000 € (update)
OPC DA	500 000 € (replace)

Proof of Concept – Step VI: CBOM Output

SATAM output: CycloneDX-compatible CBOM with architectural context

```
{
  "bom-ref":  "CBOM-OPCUA-1",
  "type":  "cryptographic-asset",
  "name":  "OPC UA Security",
  "version":  "SignAndEncrypt",
  "properties":  [
    { "name":  "satam.context.flow",
      "value":  "svc-assets" },
    { "name":  "satam.stride",
      "value":  "S,T,I,D,E" },
    { "name":  "satam.securityQasRefs",
      "value":  "QAS-OT-OPC-1" },
    { "name":  "satam.adrRefs",
      "value":  "ADR-OT-OPC-1" },
    { "name":  "satam.caraf.risk",
      "value":  "150000 Euro" }
  ]
}
```

```
{
  "bom-ref":  "CBOM-OT-OPCDA-1",
  "type":  "cryptographic-asset",
  "name":  "OPC DA",
  "version":  "legacy",
  "properties":  [
    { "name":  "satam.context.flow",
      "value":  "svc-assets" },
    { "name":  "satam.stride",
      "value":  "S,T,I,E" },
    { "name":  "satam.securityQasRefs",
      "value":  "QAS-OT-OPC-1" },
    { "name":  "satam.adrRefs",
      "value":  "ADR-OT-OPC-1" },
    { "name":  "satam.caraf.risk",
      "value":  "500000 Euro"
  ]
}
```

Limitations and Future Work

Current Limitations:

- Proof-of-concept experimental – no industrial case study yet
- Scalability for large, evolving systems not empirically assessed
- CARAF cost parameters are illustrative – real numbers require calibration to specific organizational context

Next Steps:

- Empirical validation in industrial settings
- Tool support for automated traceability linking, consistency checks, and CBOM generation (using existing tools such as [11])
- SATAM integration into secure development pipelines for continuous architecture evaluation

Conclusion

SATAM produces a CBOM that explains:

- ✓ *why* cryptography is used
- ✓ which threats it addresses
- ✓ what architectural decisions constrain changes (tradeoffs)
- ✓ what the quantified migration risk is

Organizations already have architecture documentation – SATAM builds on it:

- ✓ No greenfield effort: architecture documentations serve directly as SATAM baseline
- ✓ SATAM continuously updates architecture descriptions as a side effect
- ✓ Broader value: architecture review surfaces architectural risks and optimization potential together with crypto issues

→ Crypto migration planning integrated into architectural governance at low additional cost

→ Big picture perspective

Fraunhofer AISEC

Contact

Kristina Raab
Department
Secure Infrastructure
kristina.raab@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security AISEC
Lichtenbergstr. 11
85748 Garching (near Munich)
Germany

Contact me on LinkedIn

Bibliography I

[1] Starke et al.: *arc42 by Example*. Leanpub, 3rd edn. (2023).

[2] Kazman, Klein, Clements: *ATAM: Method for Architecture Evaluation*. Tech. Rep. CMU/SEI-2000-TR-004 (2000).

[3] Bass, Clements, Kazman: *Software Architecture in Practice*. Addison-Wesley, 4th edn. (2021).

[4] Hassouna, A.B.: *ATRAF-driven IMRAD Methodology*. arXiv:2505.03624 (2025).

[5] Ibnugraha et al.: *Evaluation of Security in Software Architecture Using Combination of ATAM and STRIDE*. JATIT (2015).

[6] Ma, Colon, Dera, Rashidi, Garg: *CARAF: Crypto Agility Risk Assessment Framework*. Journal of Cybersecurity **7**(1), tyab013 (2021).

[7] Arora, Wright, Garman: *Strengthening the Security of OT: Understanding Contemporary Bill of Materials*. J. Critical Infrastructure Policy **3** (2022).

Bibliography II

[8] Hess, Körtge: *Standardization of CBOM in OWASP CycloneDX*. Poster, ETSI/IQC QSC 2024.

[9] OWASP CycloneDX Project: *Authoritative Guide to CBOM*. Tech. rep., OWASP Foundation (2024).

[10] OWASP CycloneDX Project: *Cryptography Bill of Materials (CBOM)*. Web page (2024). `cyclonedx.org/capabilities/cbom/`

[11] Sparx Systems: *Enterprise Architect*. Web page (2025). `sparxsystems.de/enterprise-architect/`