Closing the IP Protection gap in MBSE collaboration: Granular encryption for secure and controlled model sharing

GLOBAL PRODUCT DATA

INTEROPERABILITY

SUMMIT 2025

BOEING ELYSIUM LOCKHEED MARTIN NORTHROP GRUMMAN Parker PDES, Inc.® Connecting the Digital Enterprise

Sergio Maurencig Barrionuevo, Capgemini Engineering

Juan Carlos Mendo. Boeing Technology Innovation

September 25th 2025, Phoenix AZ

Note 1: Presentation released under **RROI 726320**

Sergio Maurencig Barrionuevo

Position:

Product, Systems & PLM Engineer at **Capgemini Engineering Spain**

Education:

- B.S. in Electronics, Robotics & Mechatronics Engineering – University of Seville
- M.S. in Microelectronics - University of Seville

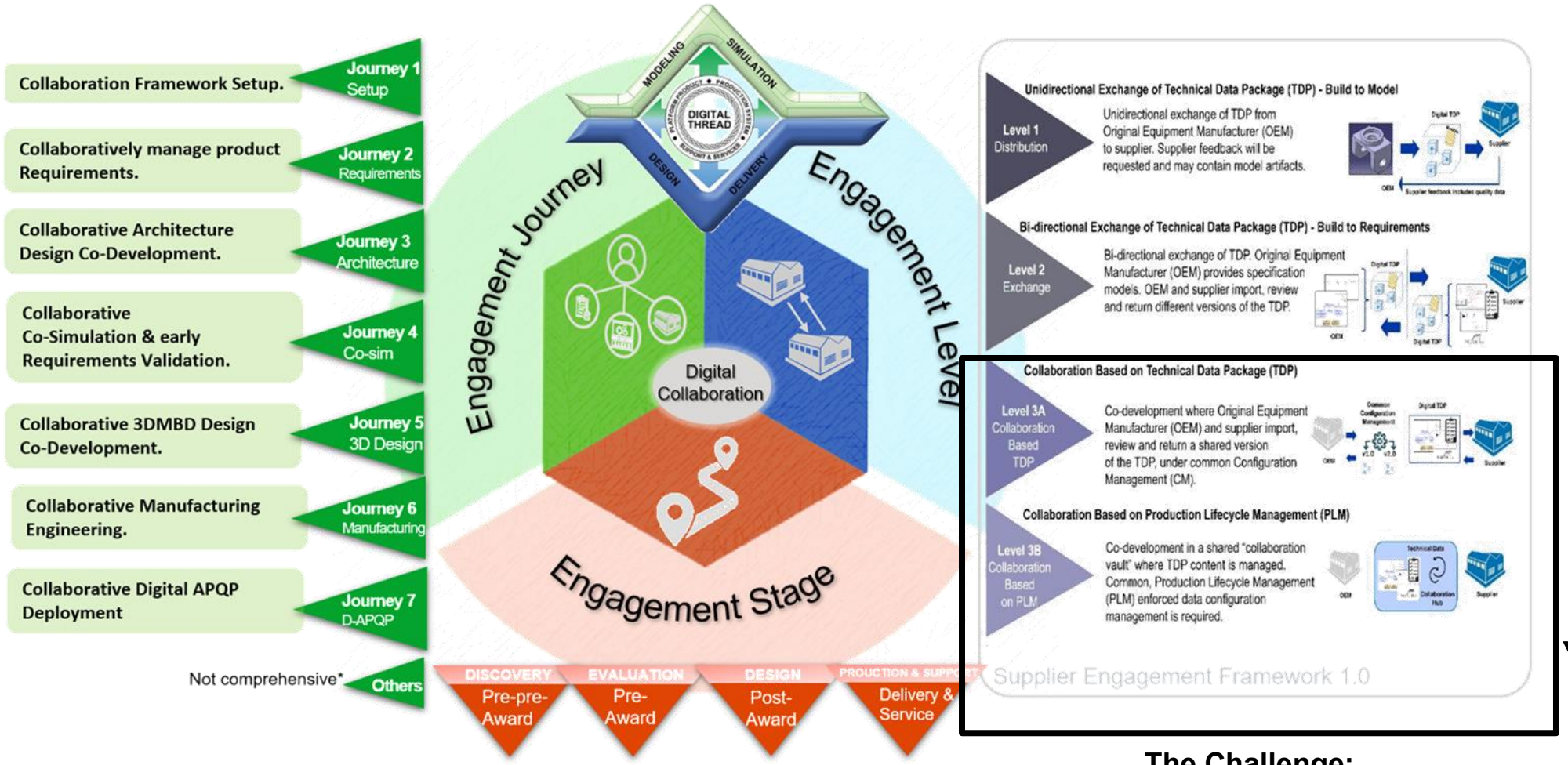
Role:

Expertise in systems engineering, digital engineering and MBSE, R&D and consulting across aerospace, rail and heavy industry. Working with **Boeing Technology Innovation Europe** on model integration, engineering and business process optimization, and MBSE-based supply-chain collaboration to enhance supply-chain resilience and IP protection.

Agenda

1. **The challenge: Enabling the right balance between Collaboration and IP protection**
2. **Encryption solution approach, capabilities & architecture**
3. **User workflow & demo**
4. **Roadmap**
5. **Conclusion & call for action**

Finding the right balance between collaboration and IP protection



The higher the Engagement Mode

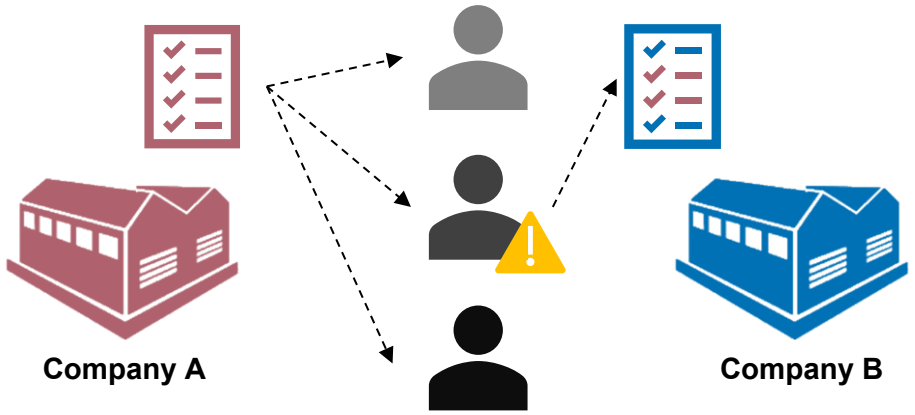
- The more synchronous collaboration between OEM and supplier
- BUT…. Risk of oversharing or overexposing information in the models is present

The Challenge:

- Finding right the balance between collaboration and IP protection

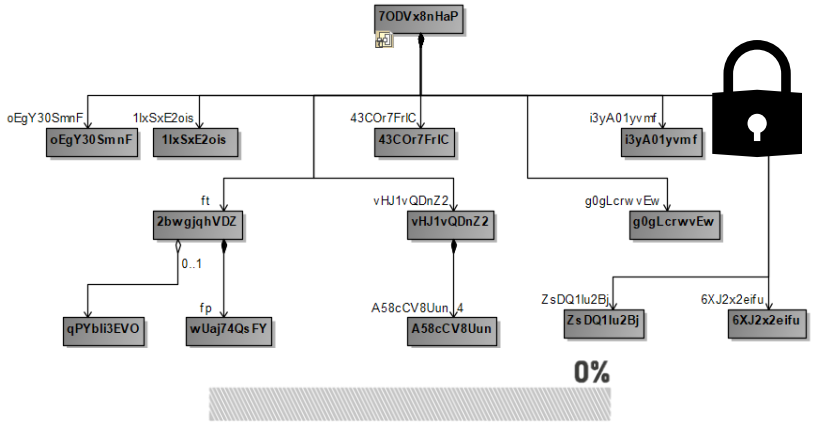
Real-World Cases: The Cost of Overexposure and Overprotection

Case 1: IP Leak



- Supplier contractor accessed requirement sets beyond scope
- Proprietary data surfaced in a competitor's program bid

Case 2: Workflow Lockdown



- Entire model protected for export control compliance
- Development stall, penalty clauses triggered

The IP Exposure Problem: When sharing the model means sharing too much

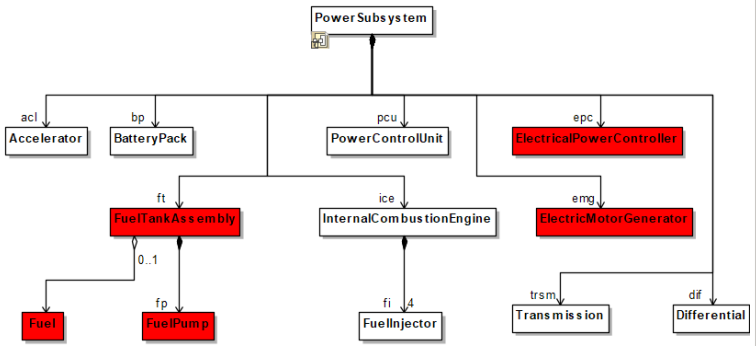
The Reality in Collaborative Engineering

- Full visibility ≠ necessary visibility
- Sensitive elements often exposed to non-essential parties
- Over-protection disrupts workflows and delivery schedules

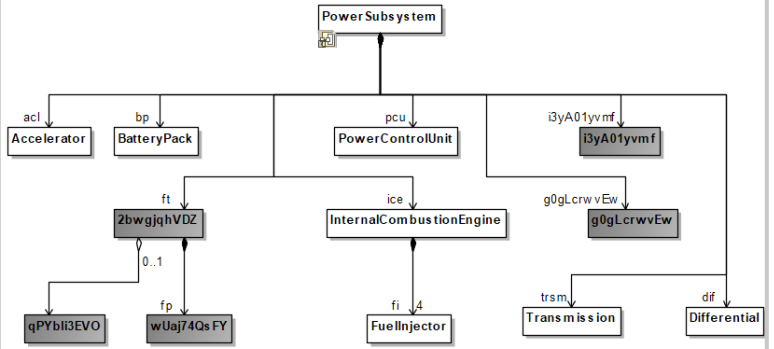
The Challenge:

- Finding right the balance between collaboration and IP protection

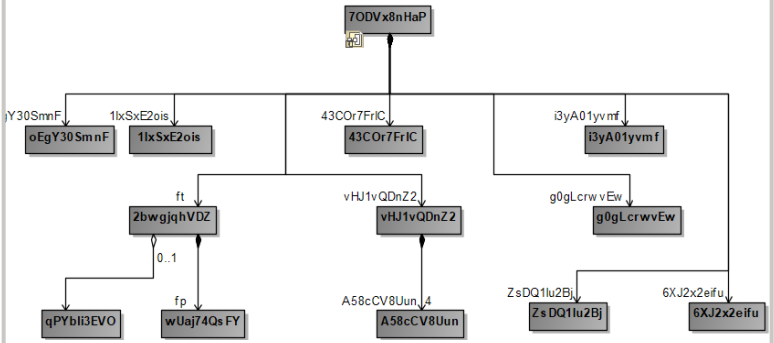
Overexposed



Precisely protected



Overprotected

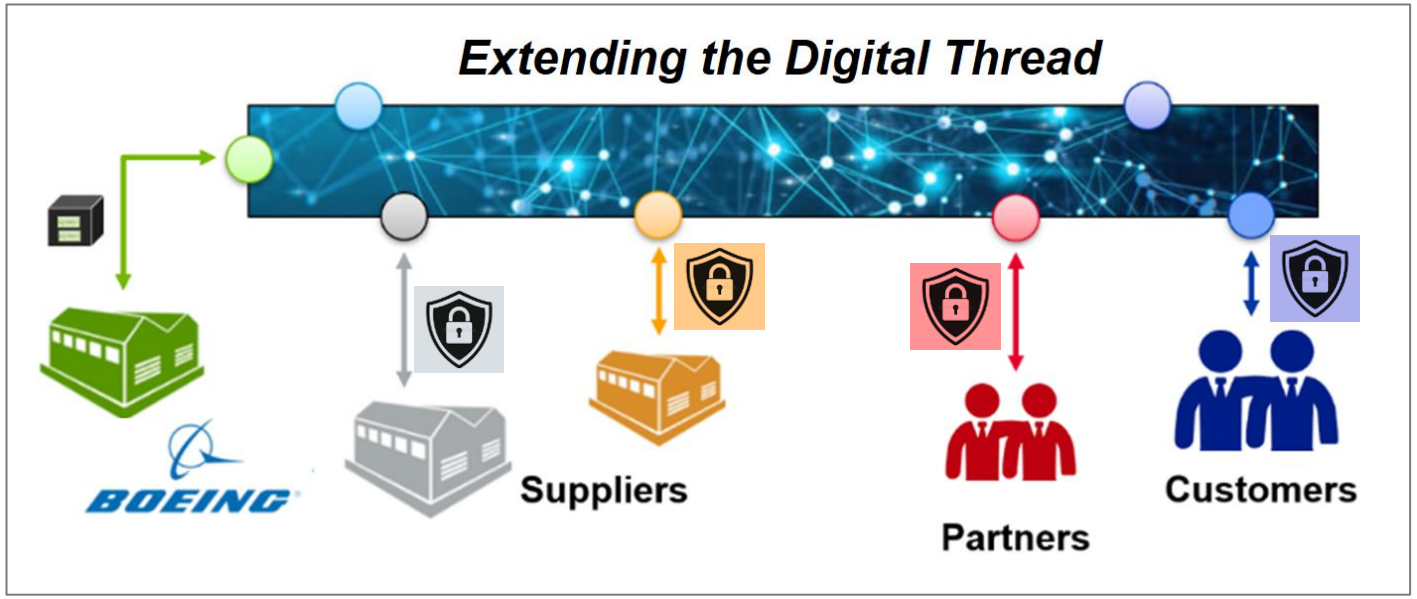


Digital Thread Context: Power and Vulnerability

The Digital Thread integrates requirements, design, manufacturing, operations, and sustainment**.**
Extending the Digital Thread means including external parties in the integrated environment of connected data and processes.

However, without embedded controls:

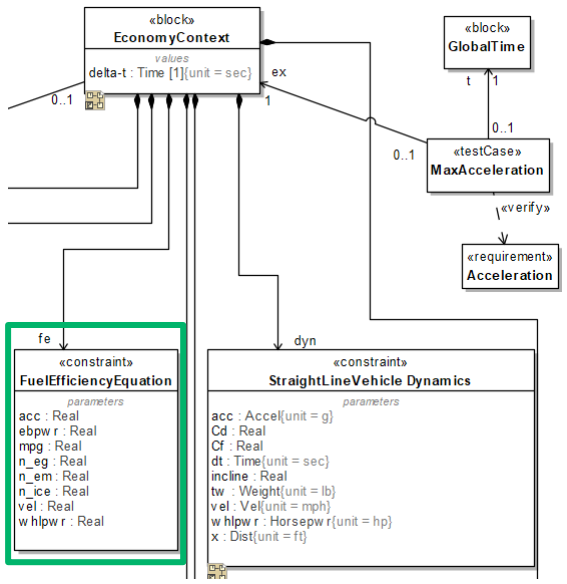
- Every handoff is a potential leak point
- Security becomes perimeter-based and fragile
- IP travels unprotected once outside your walls



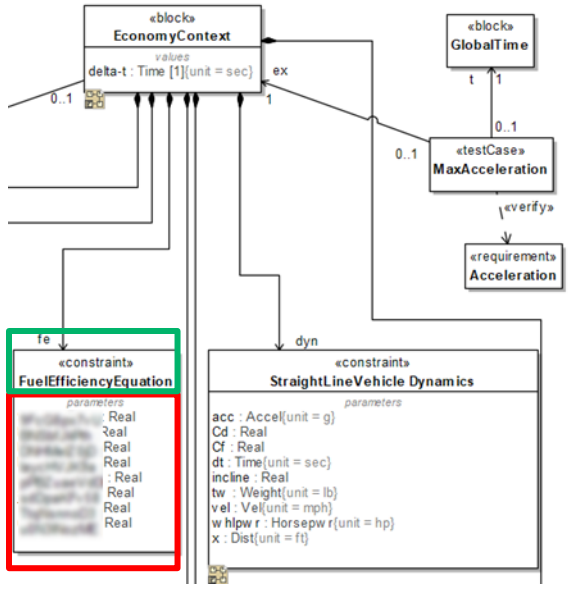
Our Approach: Encryption Where It Matters

- ✓Encrypt only the elements, attributes, or packages that truly require protection
- ✓Maintain full usability for non-protected model content
- ✓Reverse encryption selectively to adapt visibility over time

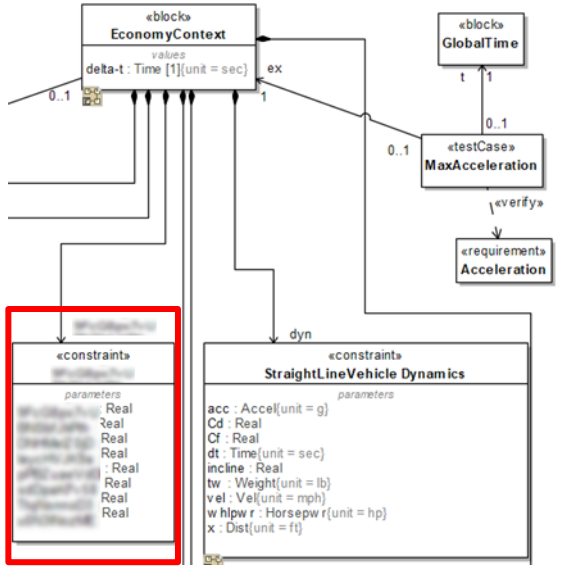
Fully visible



Inner elements protected



Fully encrypted element

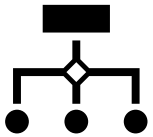


Low protection (Open) **Protection Level** High protection (Closed)

Key Capabilities: What makes this solution different to any other

MULTI-PASSWORD / MULTI-PROTECTED ZONES

Partition the same model into independent encrypted areas, each secured with a unique key for specific use criteria



ROLE, CONTRACT & CONTEXT-BASED ACCESS

Visibility potentially linked to roles, company, contract, security classification, and export

ATTRIBUTE-LEVEL, CONTROL & VISUAL FILTERING

Encrypt elements like names, stereotypes, tags, expressions, requirements, or values, manage encrypted elements with visual filters.

BRUTE-FORCE & UNATHORIZED ACCESS RESISTANCE

Active countermeasures neutralize unauthorized actions before they can succeed

RICH METADATA & VERSION TRACEABILITY

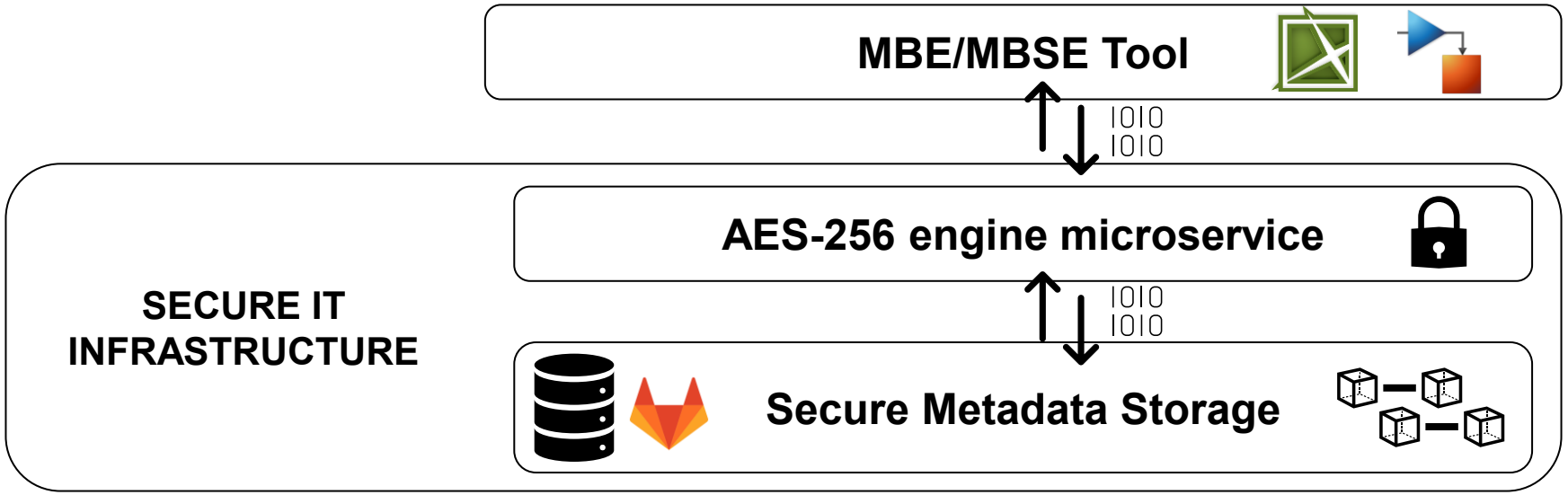
Every action is logged with who, what, when, how – and under what security scope – integrated with version control

REVERSIBLE ENCRYPTION

Full data recovery guaranteed when authorized credentials are provided

Technical Architecture: Designed for Security, built for Integration

- **Core Engine:**
  - AES-256 encryption running inside a secured microservice.
- **Separation of Sensitive Data:**
  - Decryption metadata stored externally – unreachable from the model.
- **Enterprise integration:**
  - Works within secure IT infrastructure
  - Compatible with Teamwork Cloud, Gitlab.
- **Scalability:**
  - Architecture ready for other tools such as Simulink.
  - Ready to scale to different MBSE environments without redesign.



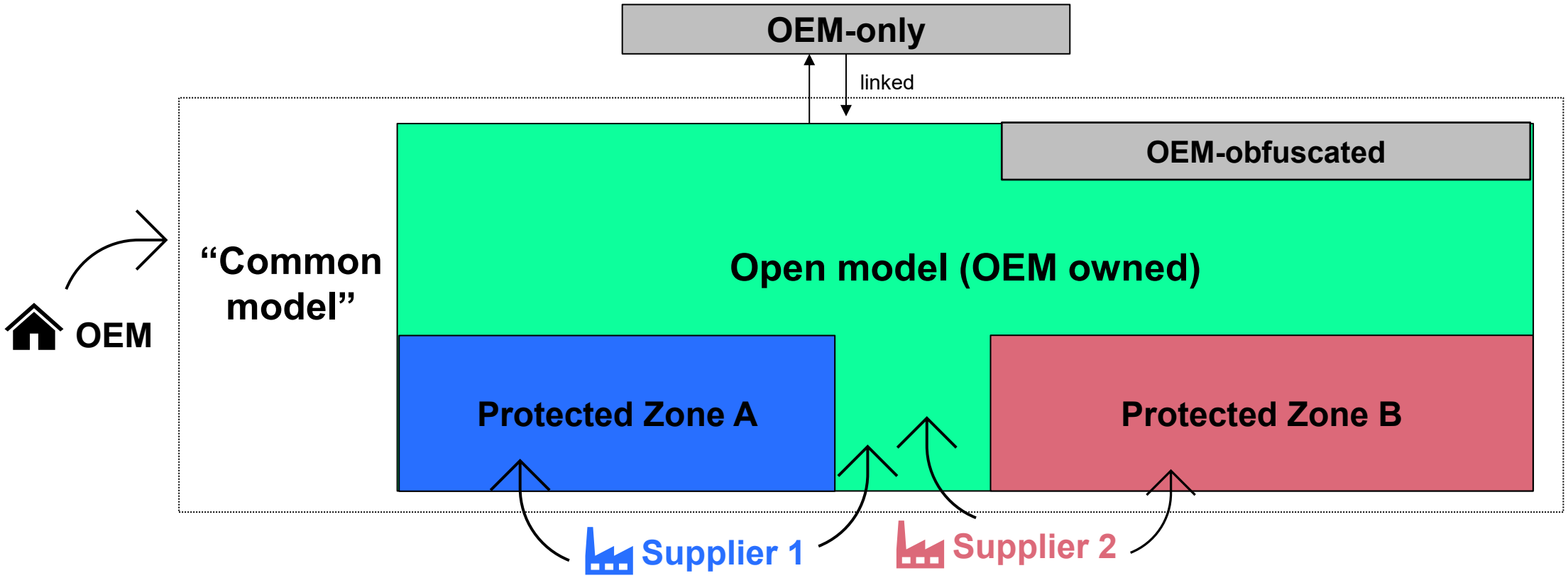
“Common model” model partitioning and obfuscation method for controlled collaboration

Scenario:

- **OEM** – Full access to entire model
- **Supplier 1** – Open model + Protected Zone A (exclusive access)
- **Supplier 2** – Open model + Protected Zone B (exclusive access)

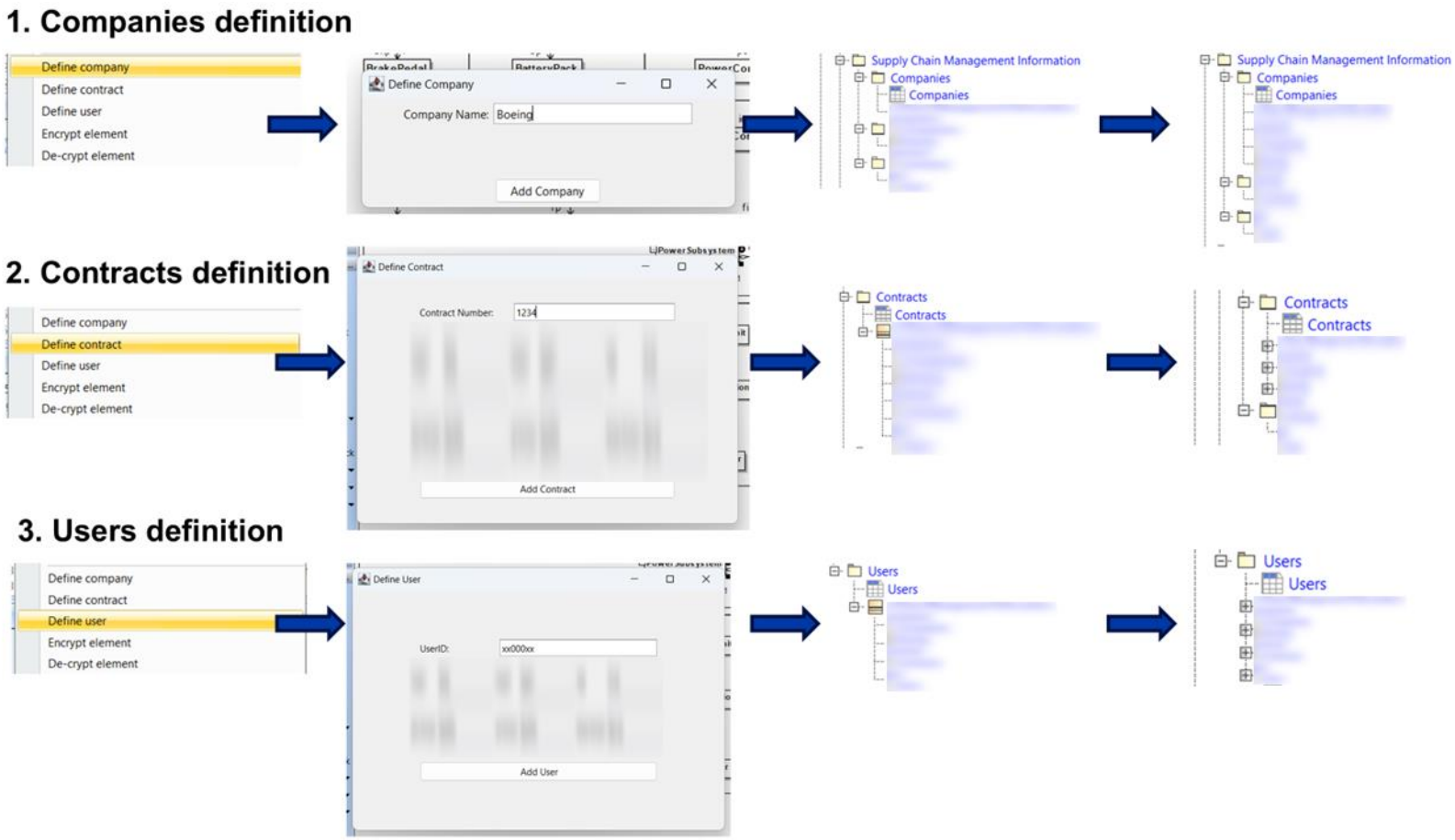
Key Outcomes:

- **Each party sees exactly what they need**—no more, no less
- **Protected zones secured with unique keys**
- **OEM retains ultimate control and full audit trail**



User Workflow / Demo: From Definition to Encryption in Four Steps

A. **Define Context: Companies, contracts, and users—set the operational scope.**
B. Select Elements: Pick the exact model elements or attributes to protect.
C. Configure Scope & Key: Assign password, define visibility, and apply access rules.
D. Apply & Log: Encryption executed; metadata captured for full traceability.



User Workflow / Demo: From Definition to Encryption in Four Steps - cont.

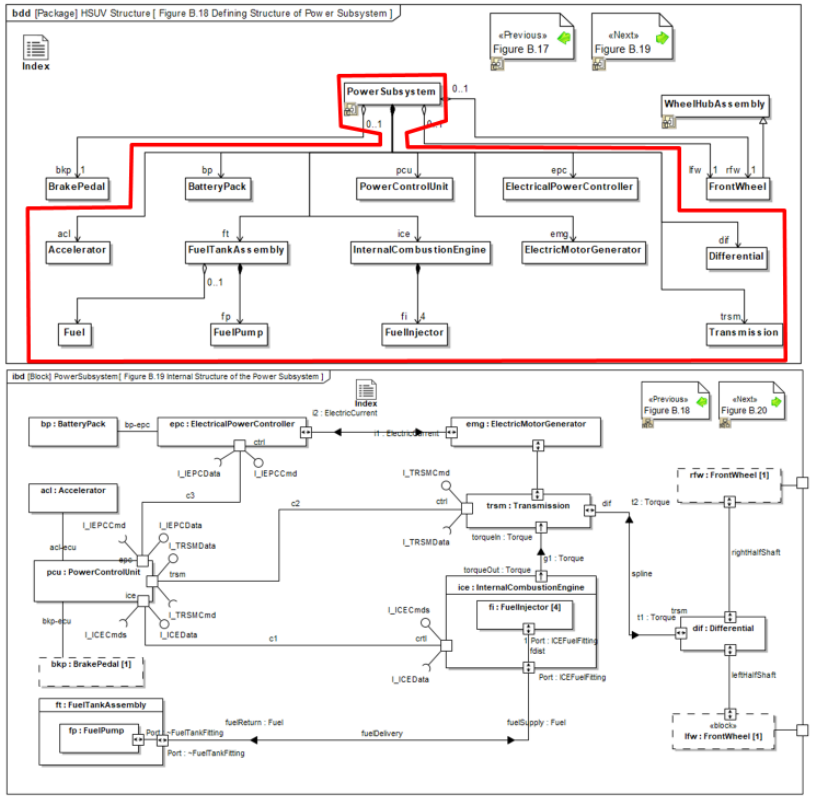
A. Define Context: Companies, contracts, and users—set the operational scope.

B. **Select Elements: Pick the exact model elements or attributes to protect.**

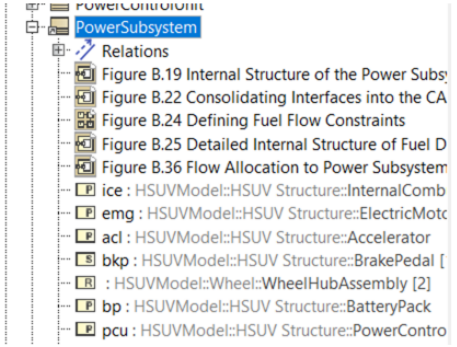
C. Configure Scope & Key: Assign password, define visibility, and apply access rules.

D. Apply & Log: Encryption executed; metadata captured for full traceability.

4. Identify elements to protect



5. Select them in the containment tree

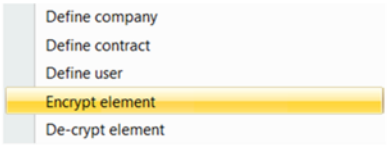


User Workflow / Demo: From Definition to Encryption in Four Steps - cont.

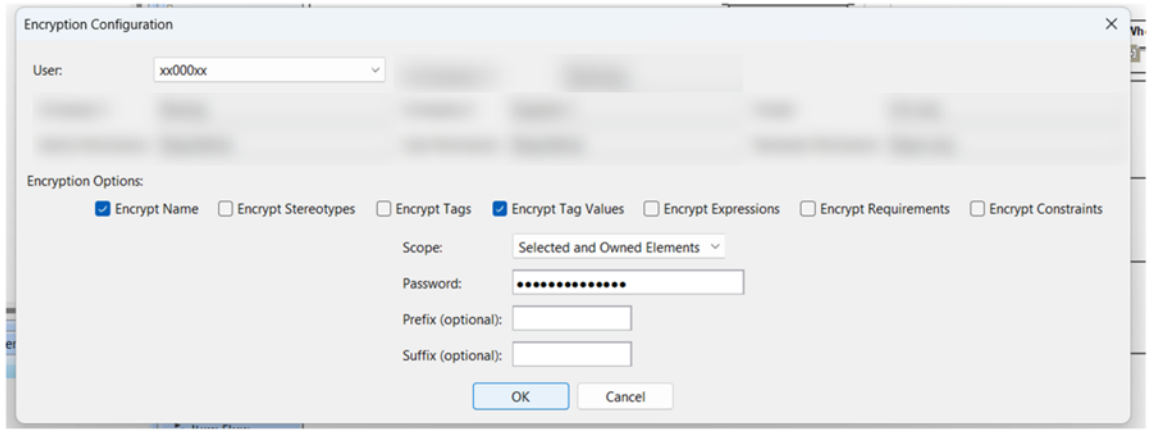
A. Define Context: Companies, contracts, and users—set the operational scope.
B. Select Elements: Pick the exact model elements or attributes to protect.
C. **Configure Scope & Key: Assign password, define visibility, and apply access rules.**
D. Apply & Log: Encryption executed; metadata captured for full traceability.

6. User identification in the model

7. Initiate encryption configuration



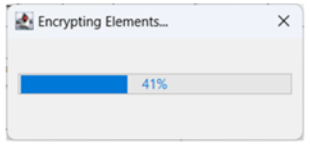
8. Encryption configuration (Select contract, scope and define password)



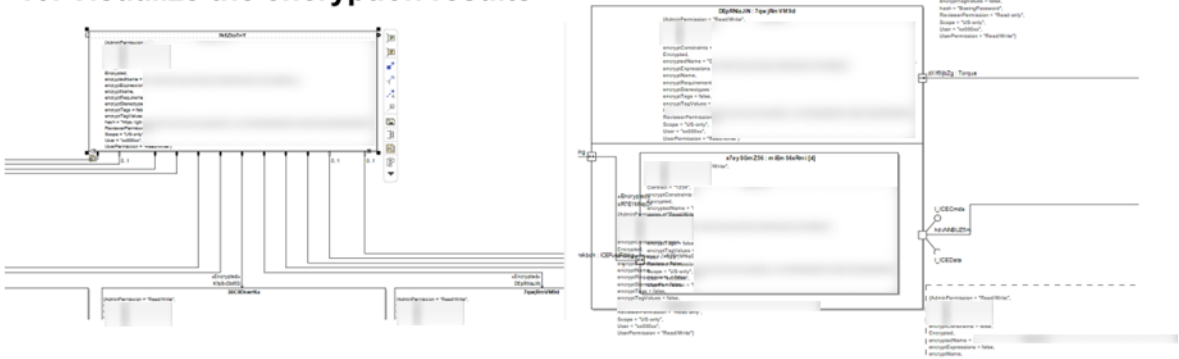
User Workflow / Demo: From Definition to Encryption in Four Steps - cont.

A. Define Context: Companies, contracts, and users—set the operational scope.
B. Select Elements: Pick the exact model elements or attributes to protect.
C. Configure Scope & Key: Assign password, define visibility, and apply access rules.
D. **Apply & Log: Encryption executed; metadata captured for full traceability.**

9. Launch encryption

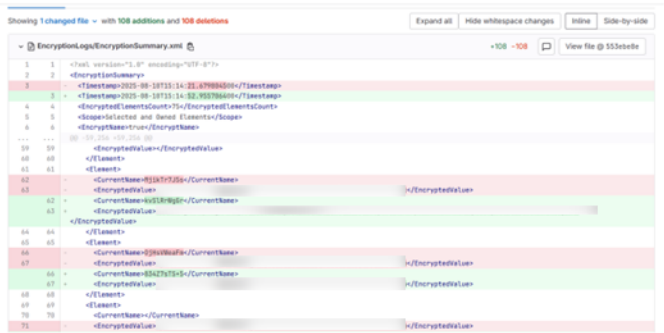


10. Visualize the encryption results



11. Check encryption summary

12. Check the information in the repository



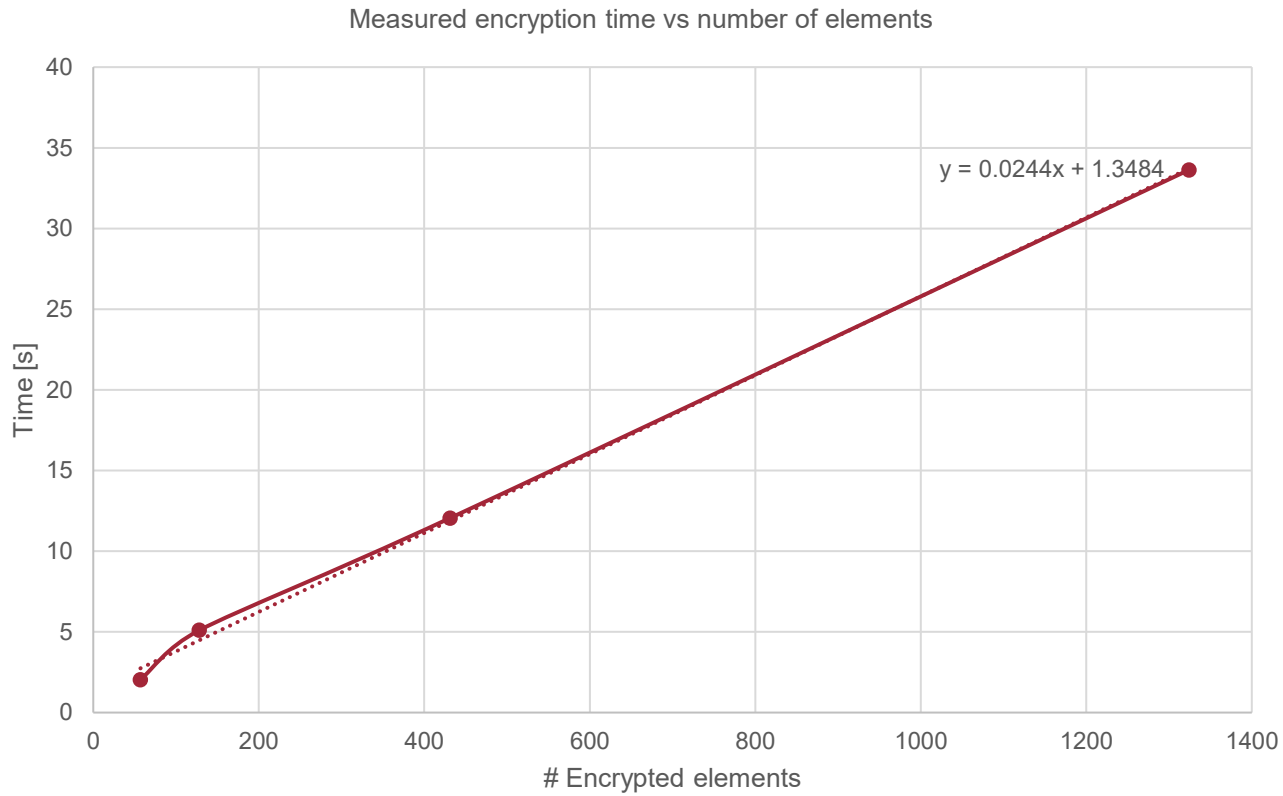
Performance & Validation

Measured Results

- Predictable scaling: encryption time grows linearly with number of elements
- Validated in MSoSA models under operational conditions
- PoC in MATLAB/Simulink demonstrating cross-platform potential

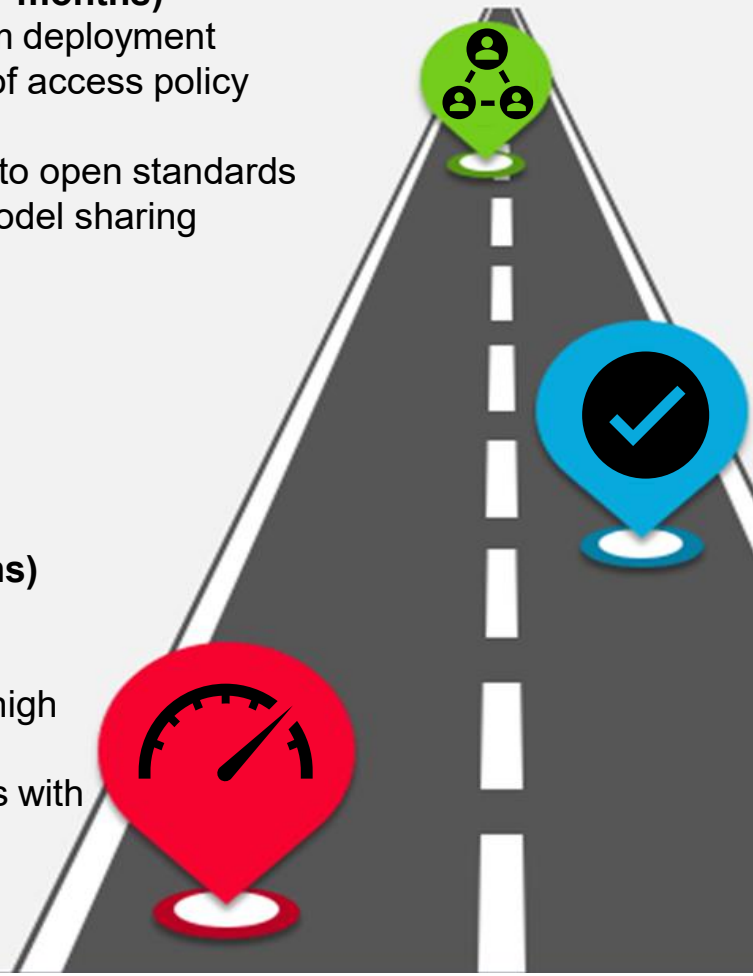
Operational Impact

- Minimal disruption to engineering workflows
- Encryption and decryption times suitable for daily use (~0.02 s/element)



Next steps: IP protection in MBSE Collaboration

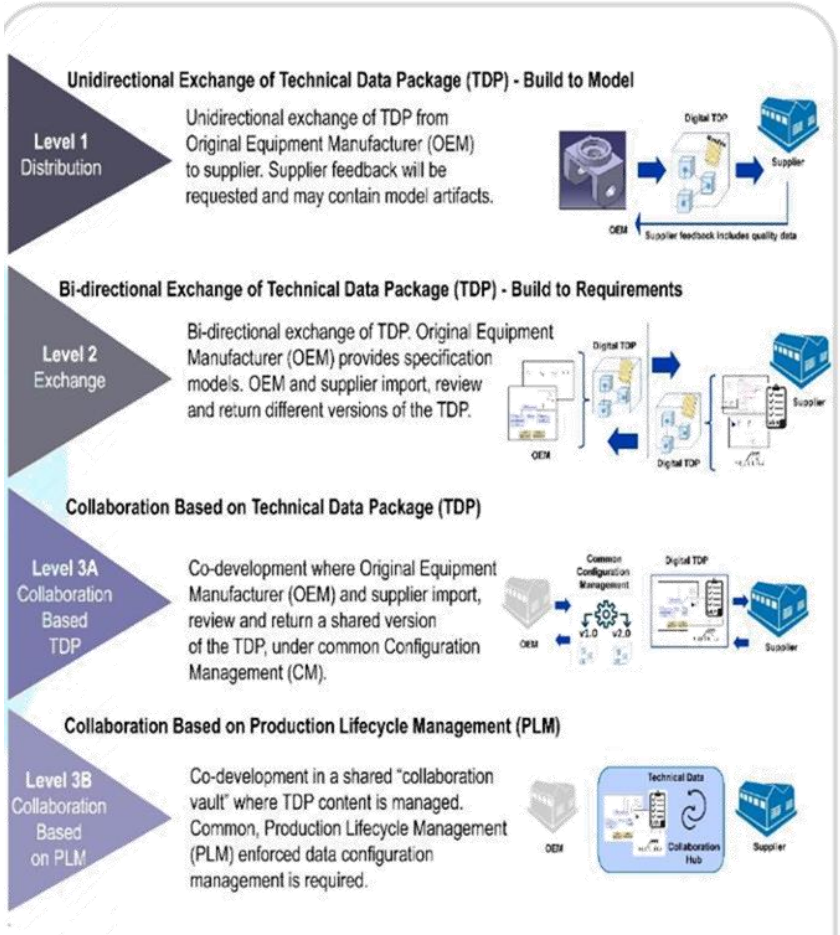
Long Term (9+ months)
- Multi-platform deployment
- Automation of access policy enforcement
- Contribution to open standards for secure model sharing



Mid Term (3–9 months)
- Additional integration with PLM and MBSE platforms, including integration with Configuration Management capabilities
- Alignment with NIST, ITAR, ISO 27001
- Enhanced key management & access revocation

Short Term (0–3 months)
- Large-scale model performance tests
- Optimization for very high element counts
- Expand pilot programs with industry partners

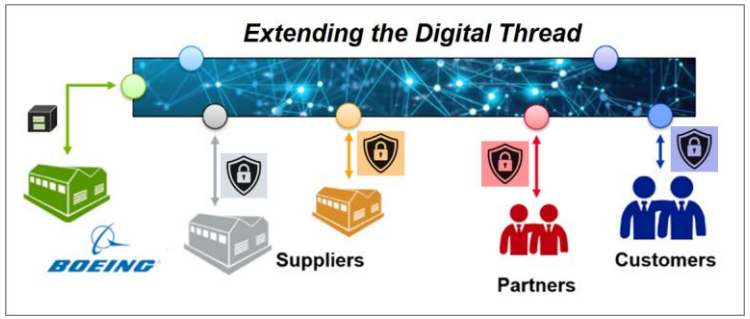
Closing & Call to Action: IP protection in MBSE Collaborations



More synchronous, but IP needs protection

Achievements:

- Enabling higher Engagement Modes, 2, 3A and 3B Collaboration without losing IP control
- Precision encryption: role based, attribute level and reversible.
- Proven concept, ready for pilots and scale



Call for Action:

- Seeking industry partners for pilot programs, scalability testing,
- Input to standards: SysML V2
- Share your alternative approaches

Thank you!

Sergio Maurencig Barrionuevo
sergio.maurencig-barrionuevo@capgemini.com

GLOBAL PRODUCT DATA

INTEROPERABILITY

SUMMIT 2025

BOEING ELYSIUM LOCKHEED MARTIN NORTHROP GRUMMAN Parker PDES, Inc.® Connecting the Digital Enterprise