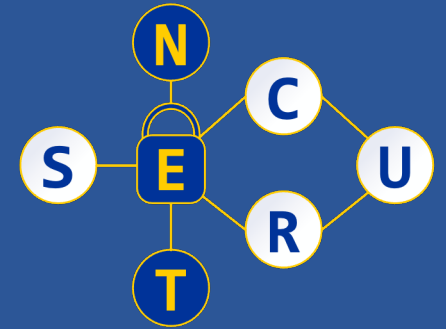




Cyber-security Excellence Hub in
Estonia and South Moravia

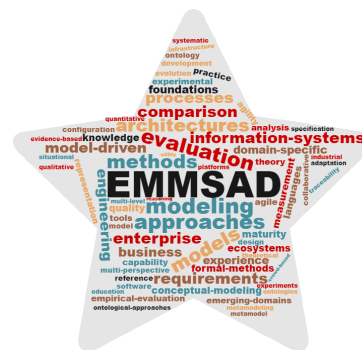


Enhancing Cross-Sectoral Collaboration
in Cybersecurity in Estonia, Czechia,
Lithuania, Ukraine, and the Netherlands

Agentic Architecture for Formalising Security Risk Elicitation

Vjatšeslav Antipenko,
Raimundas Matulevičius

*Institute of Computer Science
University of Tartu*



Business scenario

“Well, usually our suppliers just send the invoices as PDFs to our general office email. Once I see them, I download the file and put it into a folder on our shared office drive so the accountant can look at it later.”

Security flags

Input validation

Secure communication

“Well, usually our suppliers just send the invoices as PDFs to our general office email. Once I see them, I download the file and put it into a folder on our shared office drive so the accountant can look at it later.”

Secure storing

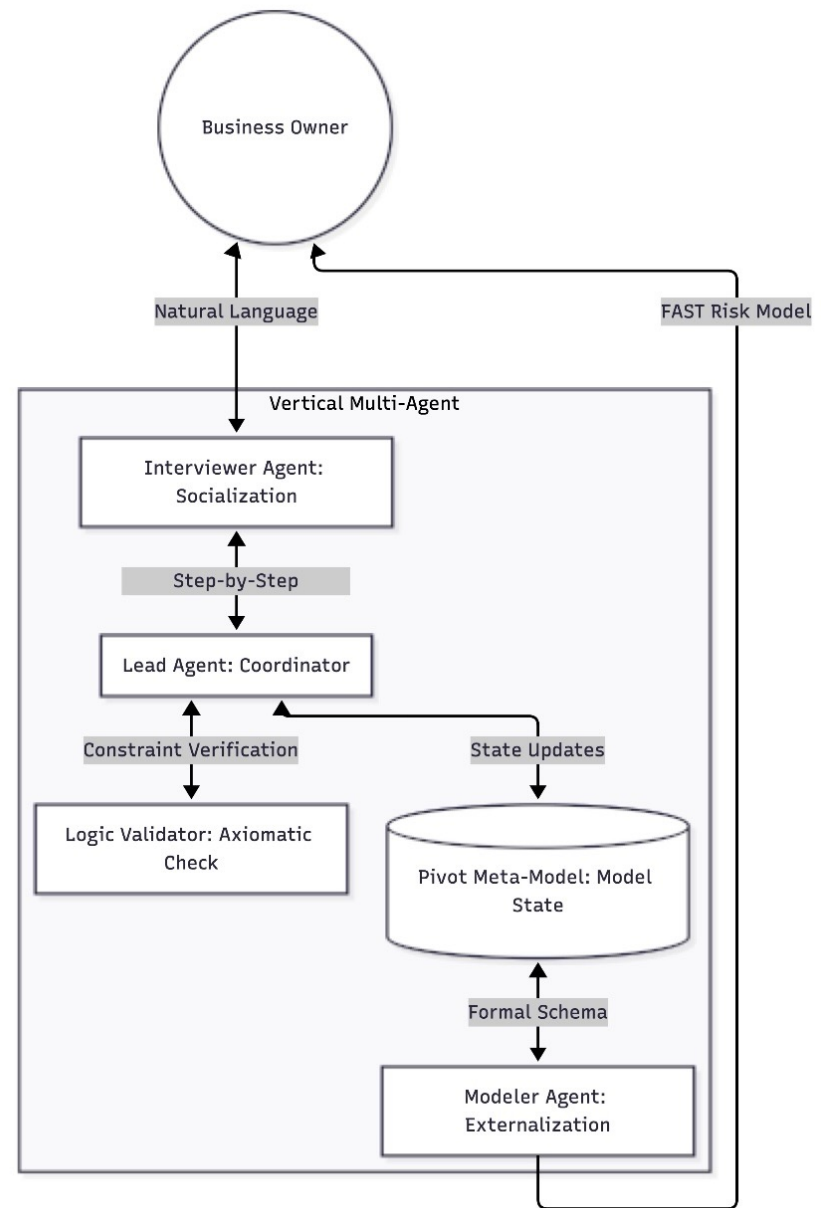
Information Manipulation

Access control

Research question

How can an agentic AI architecture formalise the elicitation of security risks from non-technical stakeholders?

Agentic FAST Assessor



Socio-technical system theory as a foundation for reasoning

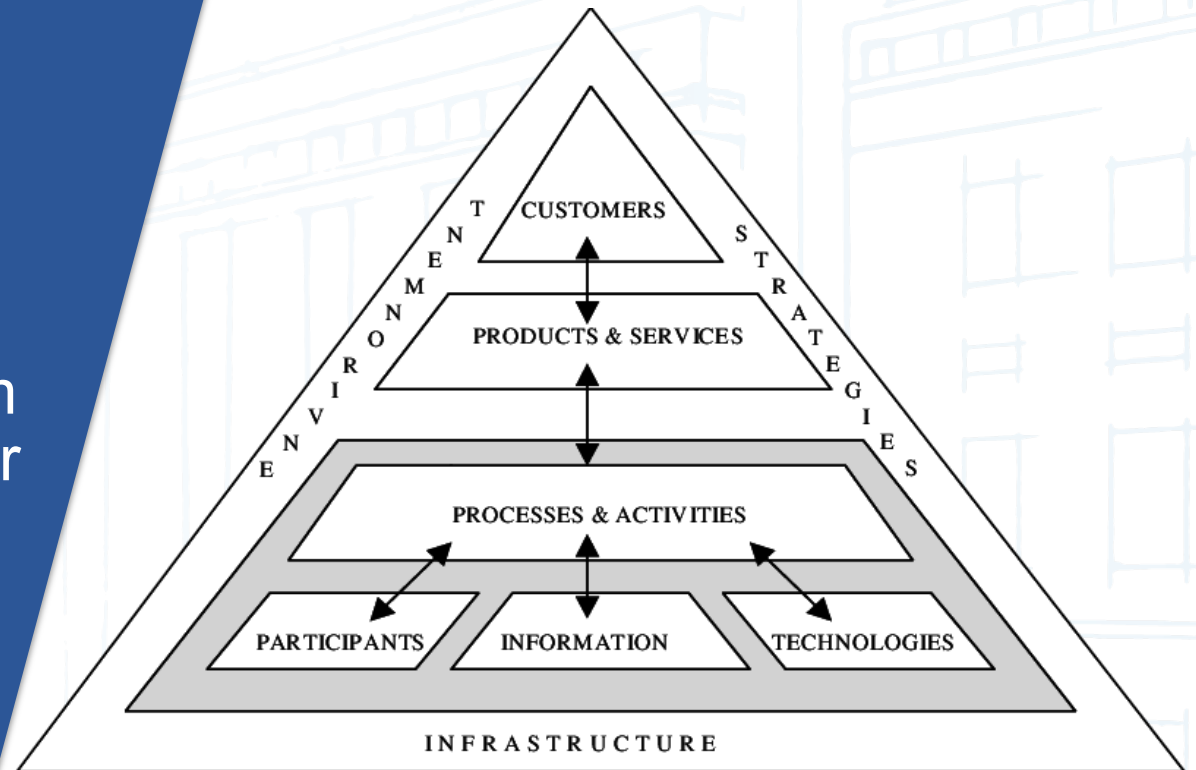
Functional security modelling through the FAST method

Emerging agentic architectures in conversational AI



Work System Theory

Explain how humans and technologies jointly perform work to produce services or products for customers



System in Context

- A1** Open System
- A2** Purposeful System
- A3** Stakeholders
- A4** Externalities

System Operation

- A5** Purposeful Activities
- A6** Resources
- A7** Regulation
- A8-A9** Interactions
- A10** Maintenance
- A11** System of Systems

Work System Axioms

Goal Attainment:

- A12** Goal Variety
- A13-A14** Alignment
- A15** Trade-offs
- A16** Operational Fit
- A17** Adaptability

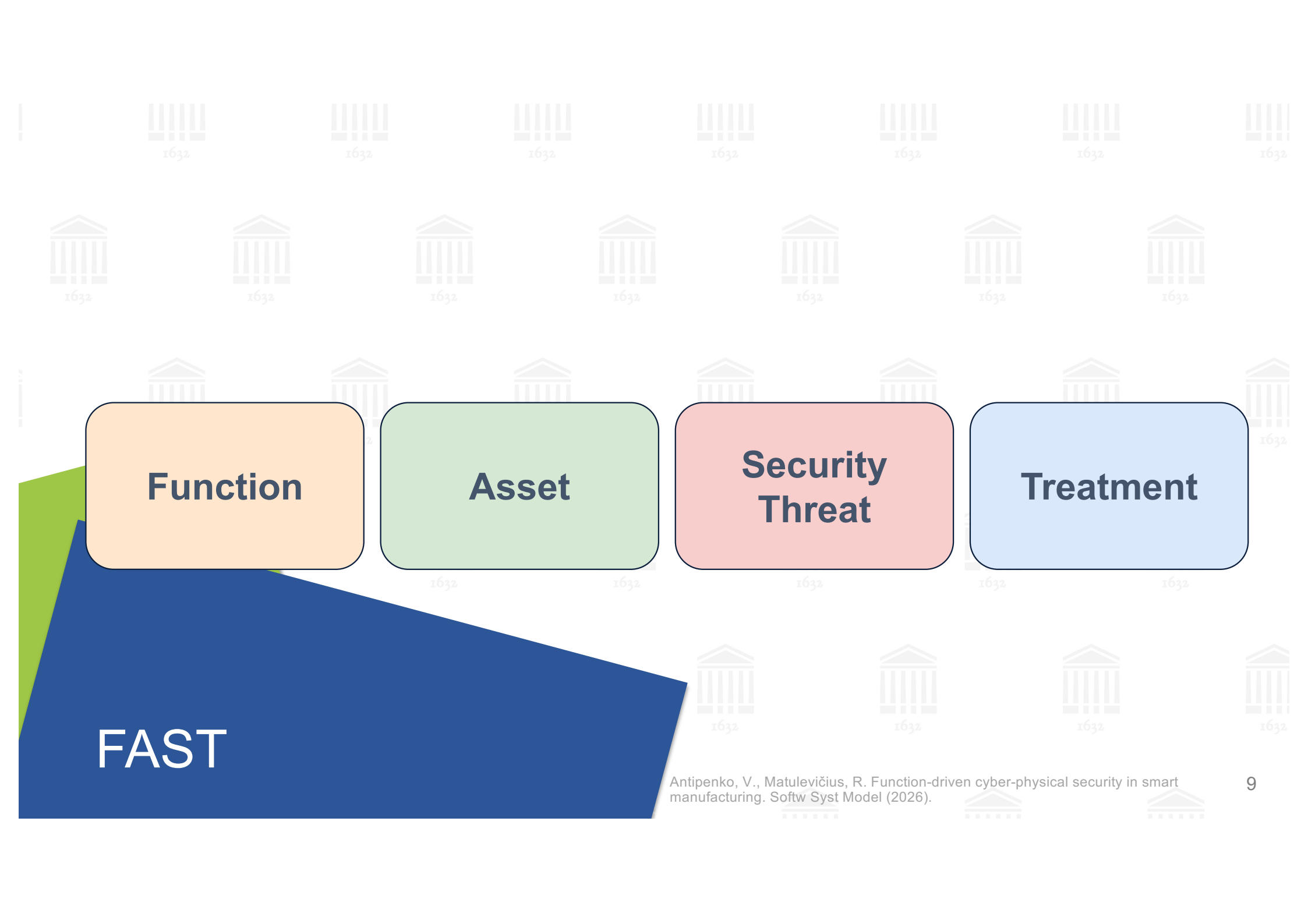
Operational Variability:

- A18** Agency
- A19** Compliance
- A20** Performance Uncertainty

System Change:

- A21** Design Incompletion,
- A22** Planned/ Unplanned Change,
- A23** Path Dependence,
- A24** Absorptive Capacity

Alter, S.: Can an LLM Use Work System Axioms When Describing Work Systems for Requirements Analysis? In: International Conference on Business Process Modeling, Development and Support. pp. 245–253. Springer (2025)



Function

Asset

**Security
Threat**

Treatment

FAST

Capturing information

- *Keyboard, bar code reader, digital camera*

Transmitting information

- *Wired-, Wireless connections*

Storing information

- *Hard disk, memory card, internet*

Processing of Information

Retrieving information

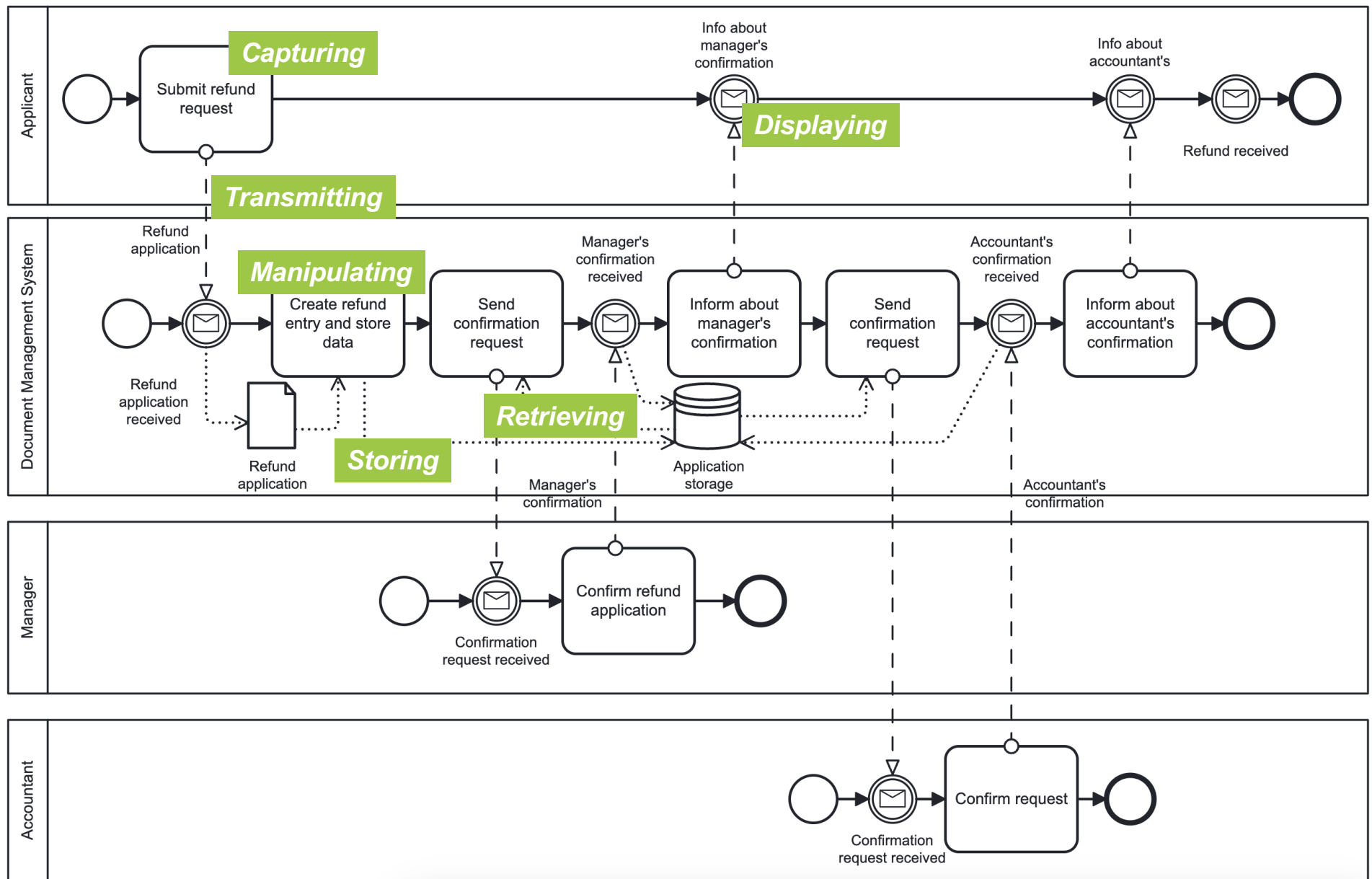
- *From any storage device*

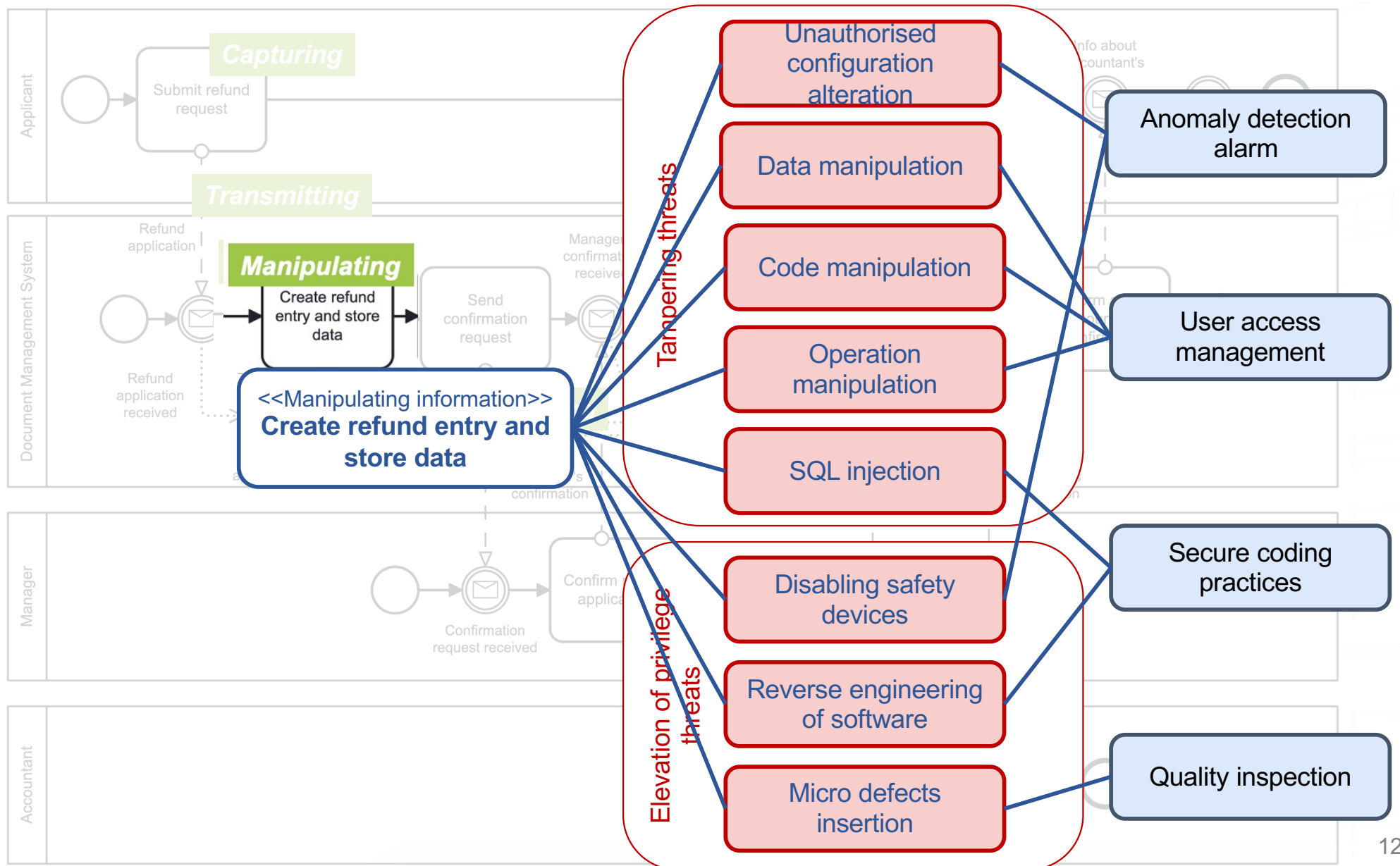
Manipulating information

- *Calculations, combinations of data*

Displaying information

- *Monitor, printer*





Large Language Models

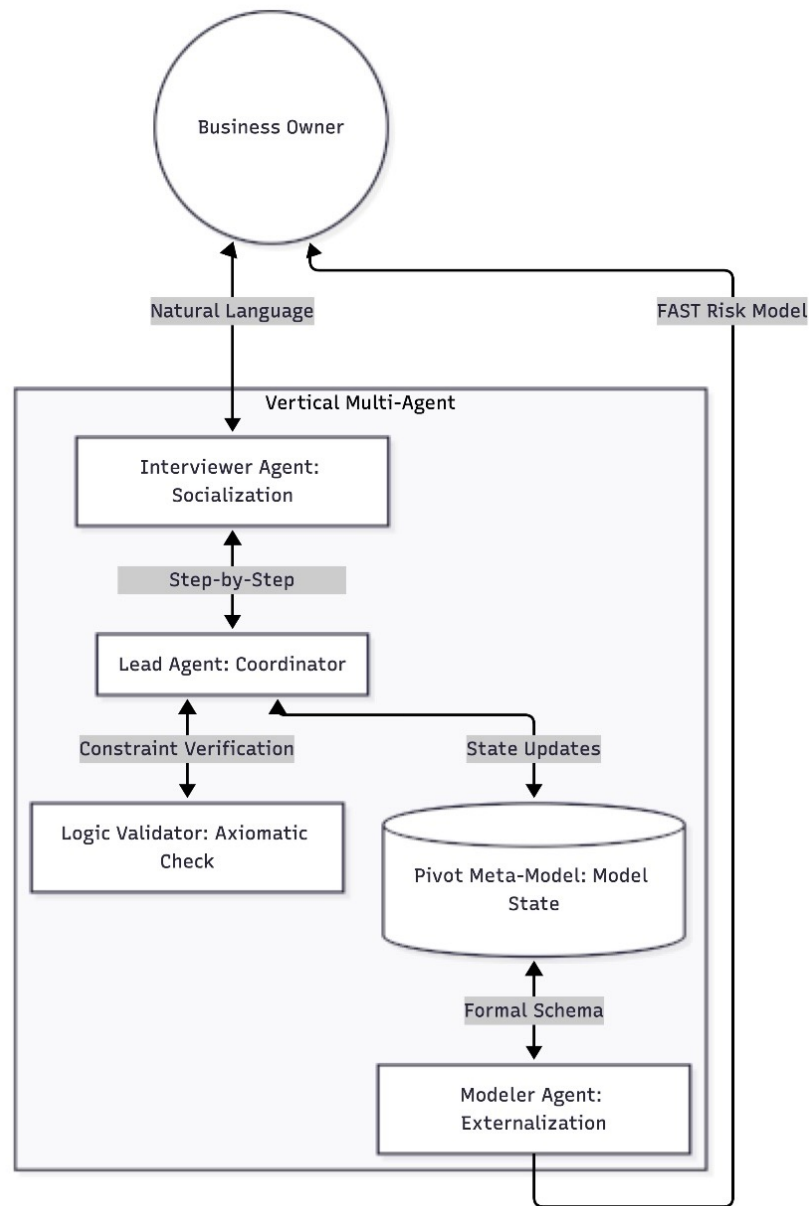
Conversational AI could help extract such knowledge

Lack mechanisms to ensure that extracted information is internally consistent, complete, or grounded in formal system principles

Organisational knowledge is treated as unstructured text

The relational and rule-based nature of socio-technical systems is not taken into account

Agentic FAST Assessor



- Lead agent: coordinator
- Interviewer agent: Socialization
- Pivot meta-model: Model state
- Logic validator: Axiomatic check
- Modeler Agent: Externalisation

Stakeholder scenario

“Well, usually our suppliers just send the invoices as PDFs to our general office email. Once I see them, I download the file and put it into a folder on our shared office drive so the accountant can look at it later.”

Stakeholder scenario

**Capturing
information**

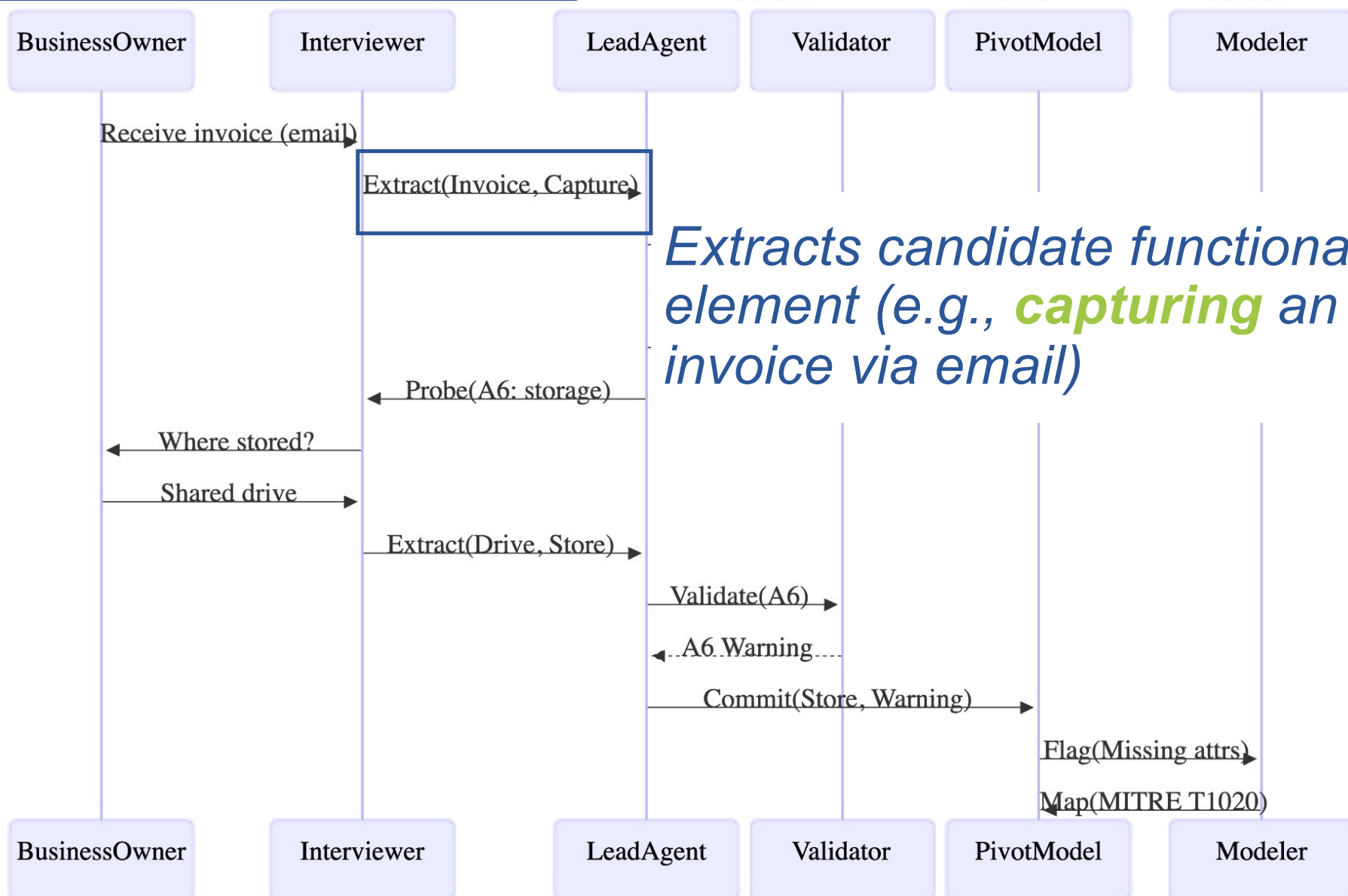
**Transmitting
information**

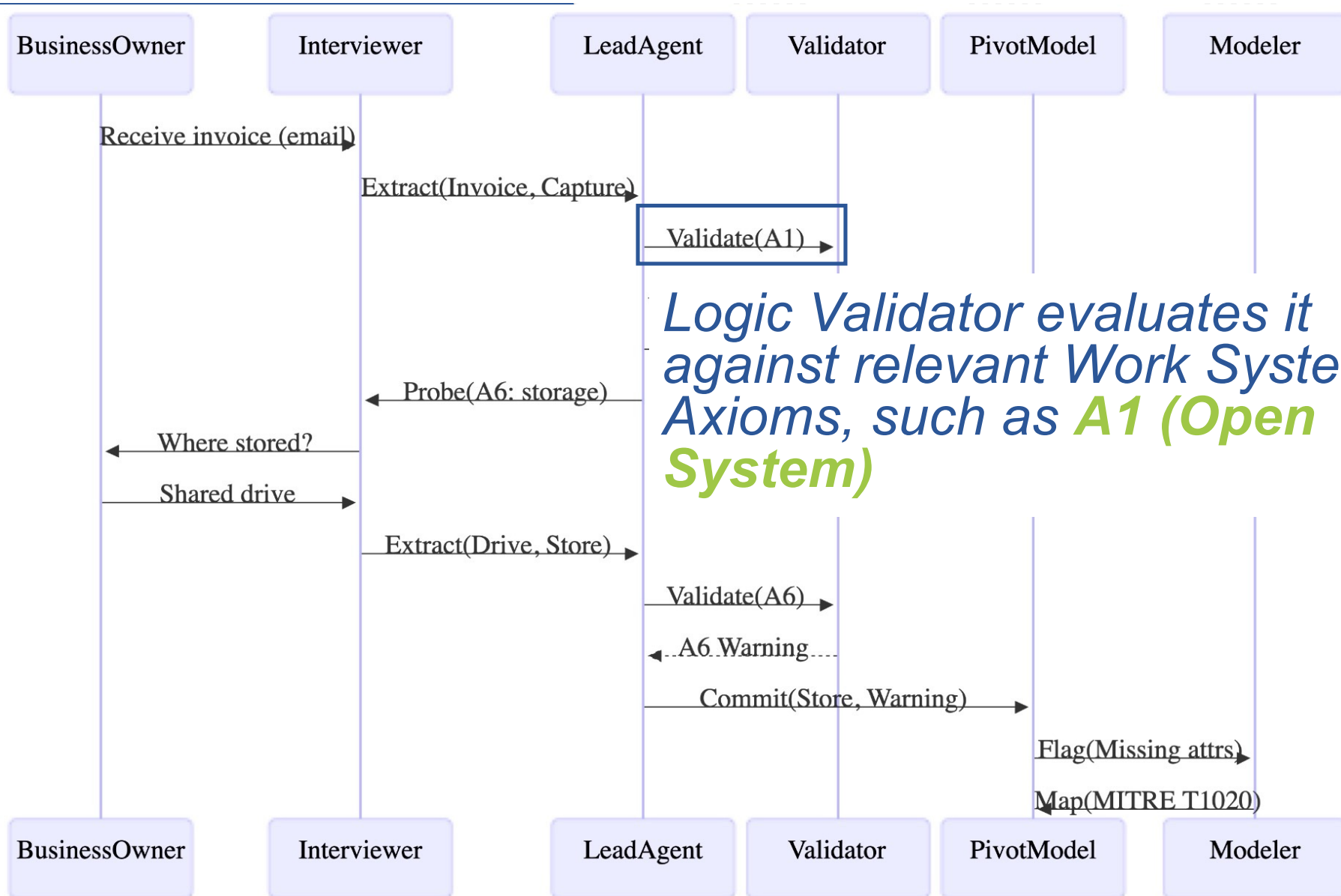
“Well, usually our suppliers just send the invoices as PDFs to our general office email. Once I see them, I download the file and put it into a folder on our shared office drive so the accountant can look at it later.”

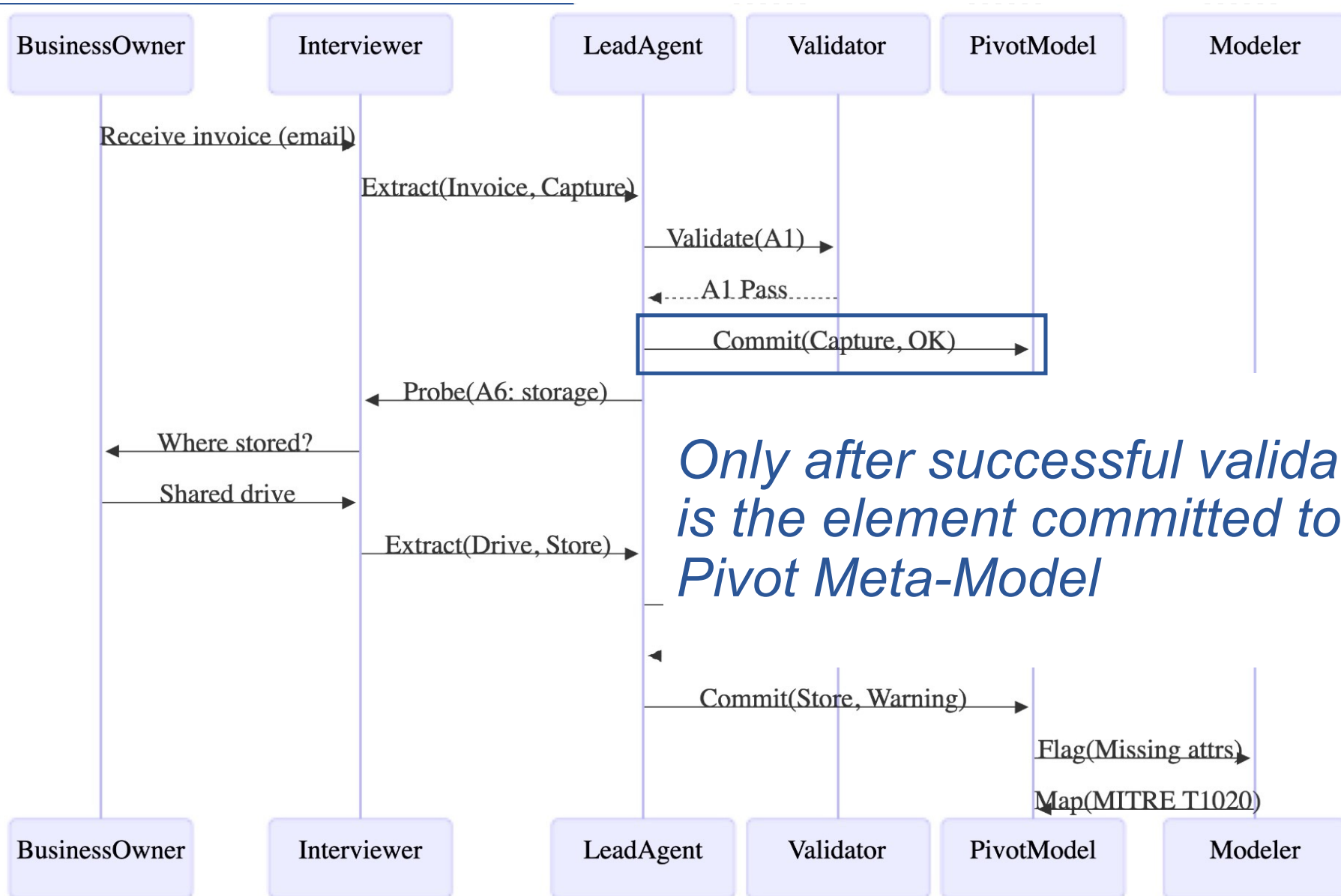
**Storing
information**

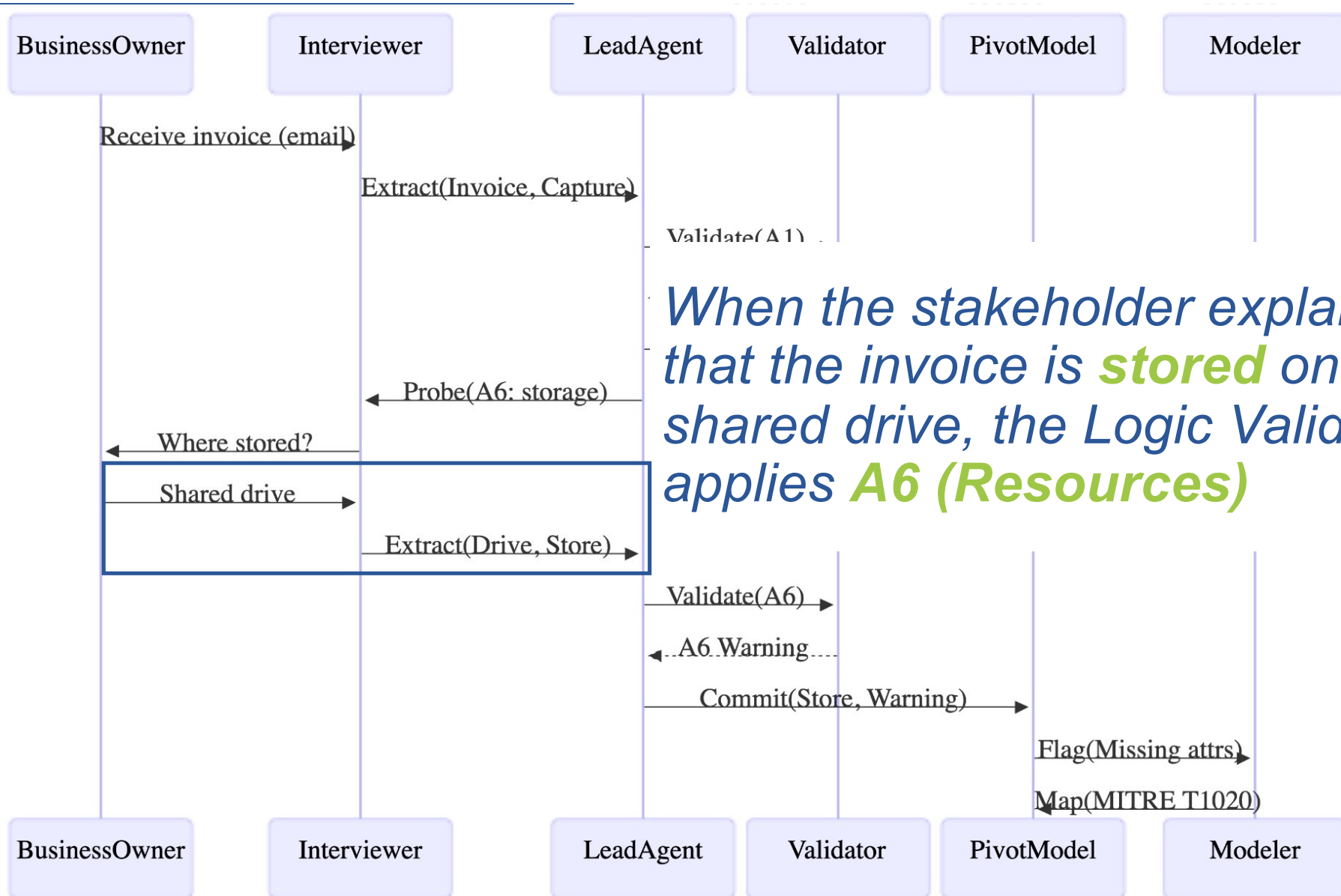
**Displaying
information**

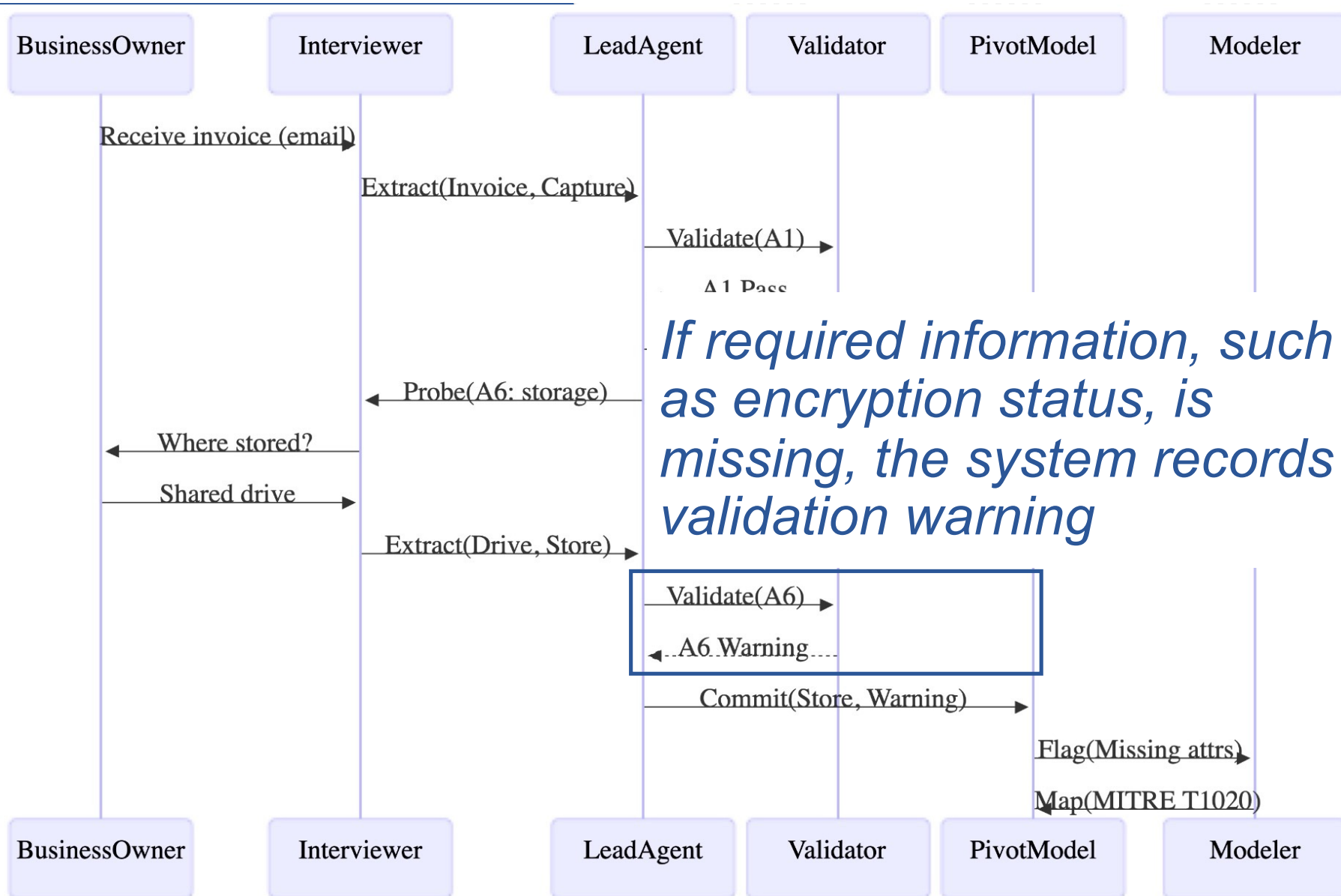
**Retrieving
information**

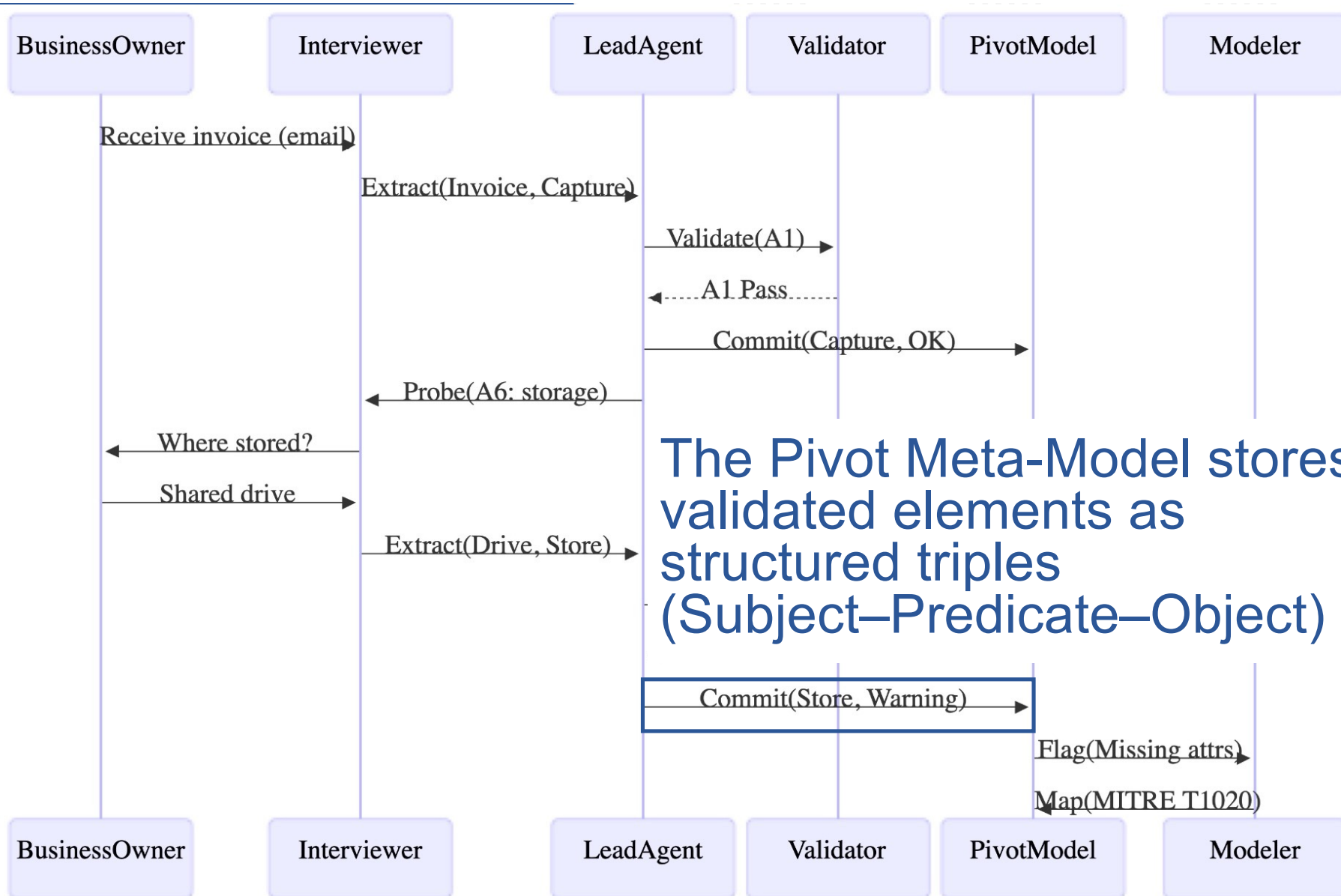


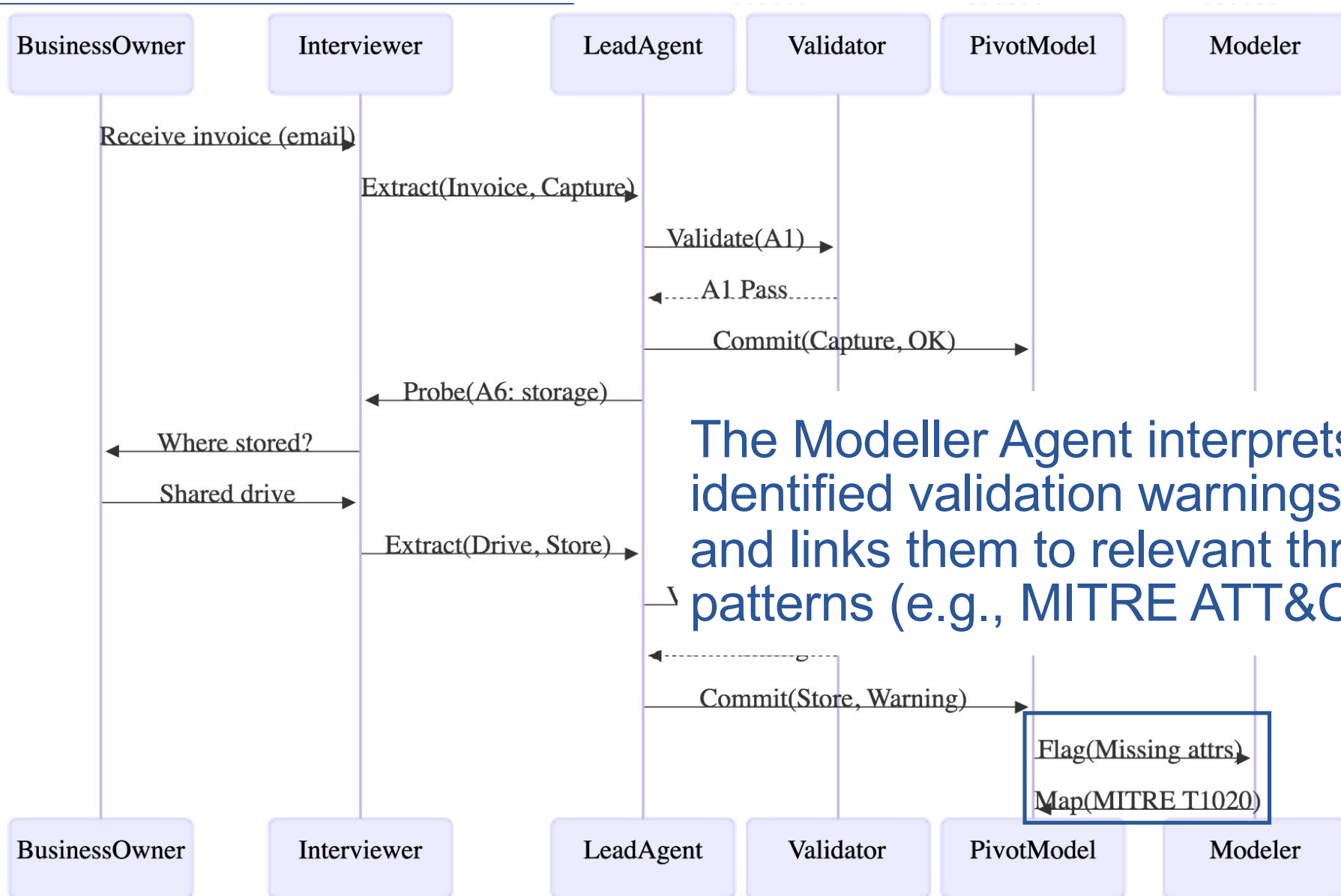












The Modeller Agent interprets identified validation warnings and links them to relevant threat patterns (e.g., MITRE ATT&CK)

Concluding remarks

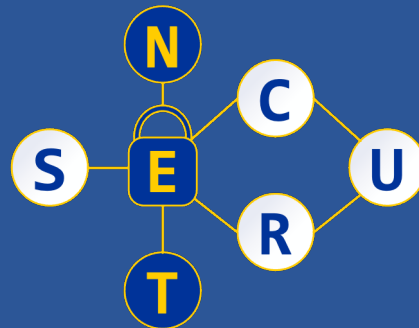
Architecture separates risk elicitation, axiomatic validation and model state management

Contribution specifies a constraint-aware design that integrates Works System Axioms and FAST functional modelling





Cyber-security Excellence Hub in
Estonia and South Moravia



Enhancing Cross-Sectoral Collaboration
in Cybersecurity in Estonia, Czechia,
Lithuania, Ukraine, and the Netherlands

