MUNI
FI

Risk-Oriented Design for Forensic-Ready Software Systems

RNDr. Lukáš Daubner

Advisor: prof. RNDr. Tomáš Pitner, Ph.D.
Consultant: doc. Ing. RNDr. Barbora Bühnová, Ph.D.

Background

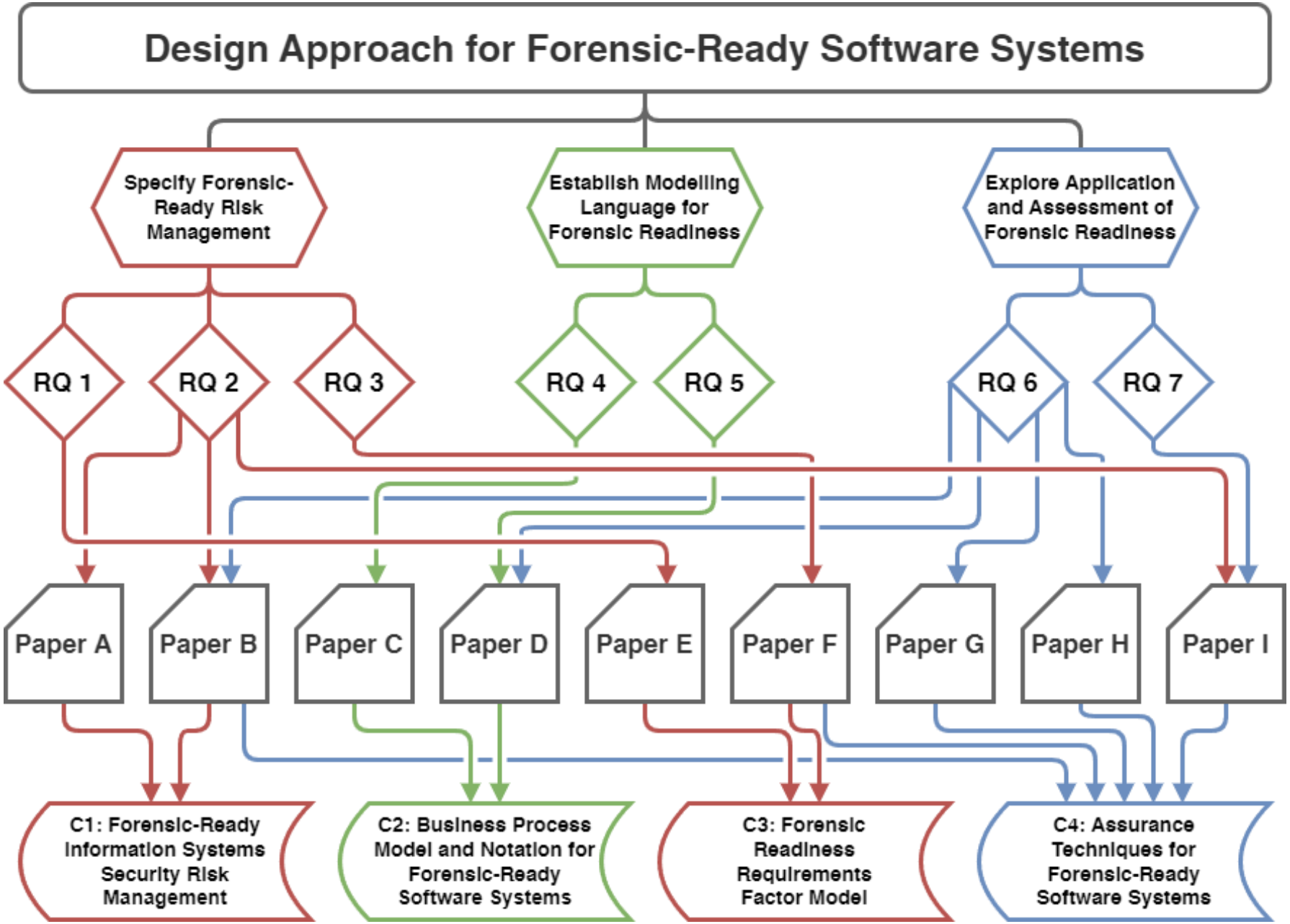
Forensic Readiness and Forensic-Ready Software Systems

- Systematic preparation for (security) incident investigation
  - Proactively collect potential digital evidence
  - Ensure sound conduction of forensic processes
  - When security measures fail, reliably know Why? Who? How? When? Where?
- Designing software systems to include forensic readiness
  - A.k.a. forensic-by-design
  - High-level non-functional requirement
- Why are they important?
  - Enhancment of security posture – e.g., proving impact, addressing disputes
  - ISO/IEC 27001 – e.g., observability, incident response
  - GDPR – e.g., assess the scope of a data leak

Background

Gaps and Challenges for Forensic-Ready Software Systems

- Detailed guidelines
  - How does it expand on the secure design?
  - How to perform the risk assessment?
  - What are the goals, why should it be implemented in the system?
  - What are the specific requirements?
- Representation
  - How to capture the design into a model?
- Assessment
  - Is the design meeting its goals?

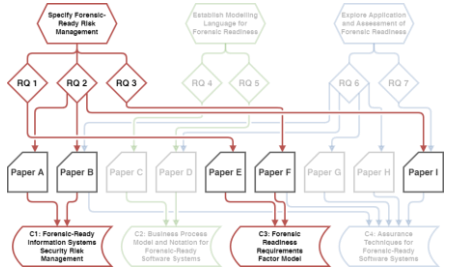

Design Approach for Forensic-Ready Software Systems
Specify Forensic-Ready Risk Management
Establish Modelling Language for Forensic Readiness
Explore Application and Assessment of Forensic Readiness
RQ 1
RQ 2
RQ 3
RQ 4
RQ 5
RQ 6
RQ 7
Paper A
Paper B
Paper C
Paper D
Paper E
Paper F
Paper G
Paper H
Paper I
C1: Forensic-Ready Information Systems Security Risk Management
C2: Business Process Model and Notation for Forensic-Ready Software Systems
C3: Forensic Readiness Requirements Factor Model
C4: Assurance Techniques for Forensic-Ready Software Systems

MUNI FI

Specify Forensic-Ready Risk Management

MUNI
FI

Specify Forensic-Ready Risk Management

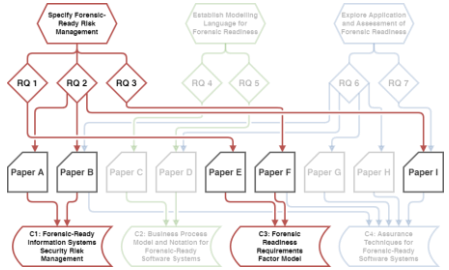


RQ1: What are the desired features of forensic-ready software systems?

- Performed a series of interviews with forensic investigators, lawyers, and researchers
  - About experiences and notion of a forensic-ready software system
- Gathered insights about desired features
  - E.g., tracing internal behaviour, correlation with other sources, precise time information
  - Systems aware of evidence-handling process
  - Being able to testify its reliability and correctness

MUNI FI

Specify Forensic-Ready Risk Management

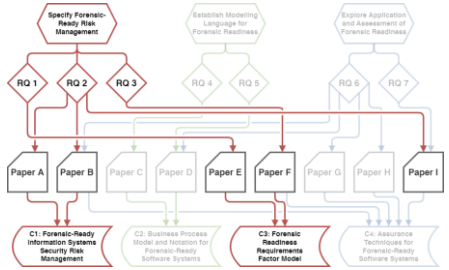


RQ2: How can a risk-oriented security design be enhanced with forensic readiness concepts?

- Organised common forensic readiness concepts
  - Based on major forensic readiness approaches
- Aligned the concepts with Information Systems Security Risk Management (ISSRM) domain model
  - Capturing relationship between security risk management and forensic readiness
  - Defined supplementary forensic-ready risk management process
- Validated through a case study, utilising the approach

MUNI FI

Specify Forensic-Ready Risk Management

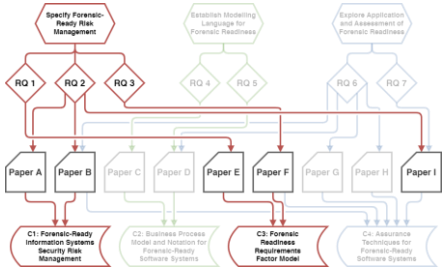


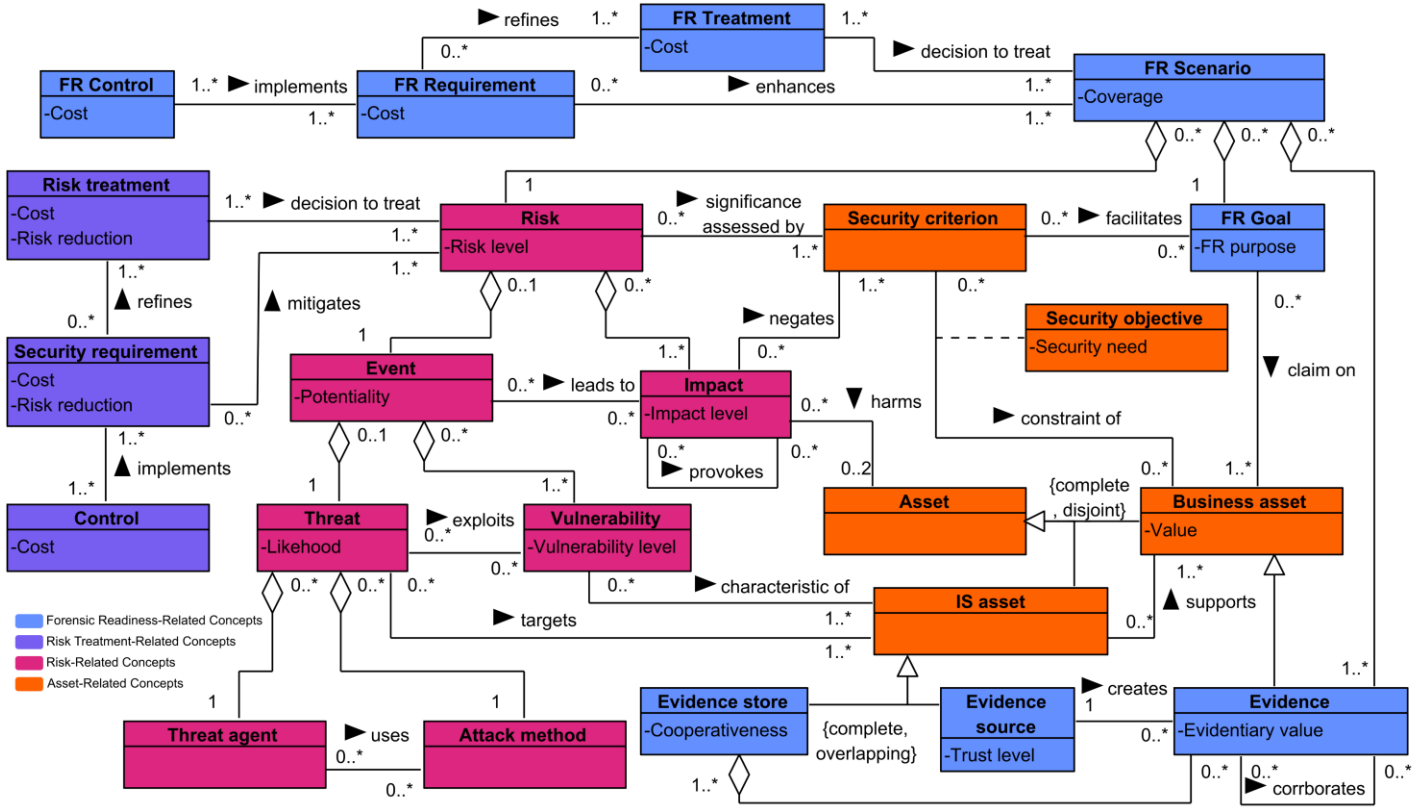
RQ3: What are the specific quality criteria making up the requirements for forensic-ready software systems?

- Elicited forensic readiness qualitative factors
  - Based on the existing literature and the interviews
- Organised the factors into a hierarchical model
  - Adopting a quality criteria model
  - Facilitates formulation of verifiable forensic readiness requirements

MUNI FI

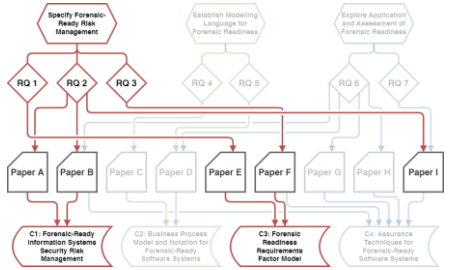
Forensic-Ready Information Systems Security Risk Management

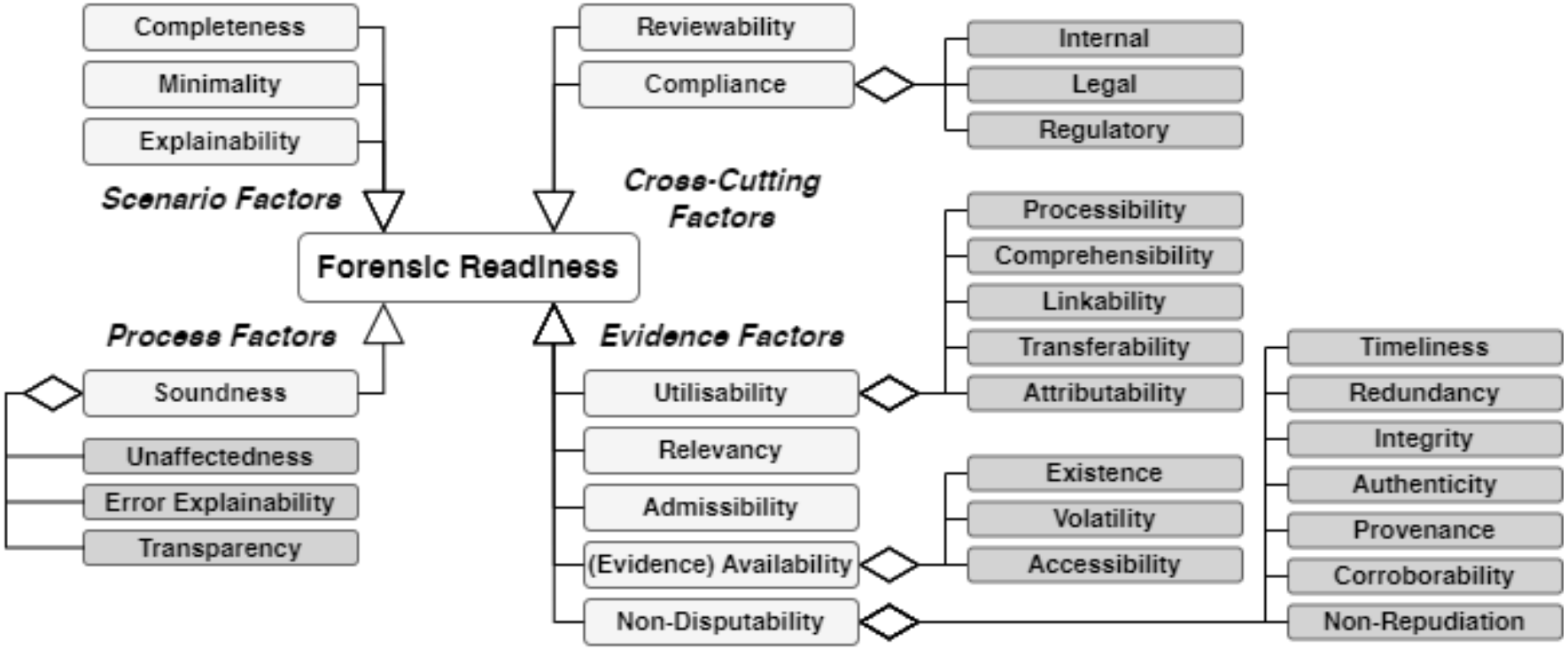




MUNI FI

Forensic Readiness Requirements Factor Model

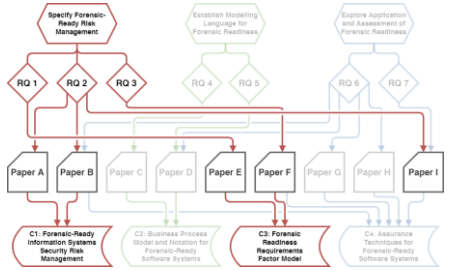




MUNI FI

Specify Forensic-Ready Risk Management

Publication Summary

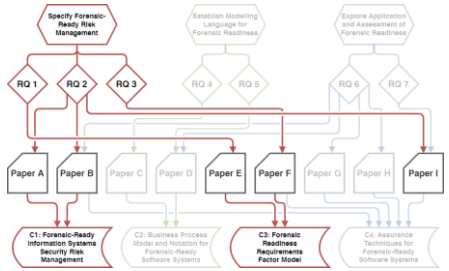


- Risk-Oriented Design Approach For Forensic-Ready Software Systems
  - **Lukas Daubner** and Raimundas Matulevičius
  - ARES, 2021
  - *Proposes the idea of considering forensic readiness within security risk management*

- Addressing insider attacks via forensic-ready risk management
  - **Lukas Daubner**, Martin Macak, Raimundas Matulevičius, Barbora Buhnova, Sofija Maksović, and Tomas Pitner
  - JISA, 2023 **[IF 5.6][SJR Q1]**
  - *Describes a risk management approach to derive the forensic readiness requirements*

MUNI FI

Specify Forensic-Ready Risk Management



Publication Summary

- Forensic experts' view of forensic-ready software systems: A qualitative study
  - **Lukas Daubner**, Barbora Buhnova, and Tomas Pitner
  - JSME, 2023 **[IF 2.0][SJR Q2]**
  - *Conducts an empirical qualitative study identifying the problems and needs of forensic readiness and framing the notion of an ideal forensic-ready software system*

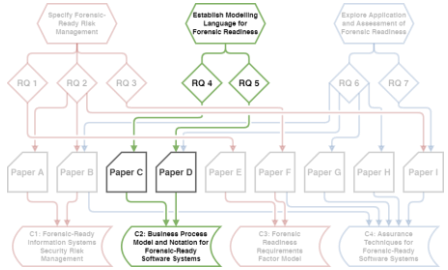
- A Model of Qualitative Factors in Forensic-Ready Software Systems
  - **Lukas Daubner**, Raimundas Matulevičius, and Barbora Buhnova
  - RCIS, 2023 **[CORE B]**
  - *Describes a forensic readiness qualitative factor reference model facilitating the formulation of specific requirements for forensic-ready software systems*

MUNI FI

Establish Modelling Language for Forensic Readiness

MUNI
FI

Establish Modelling Language for Forensic Readiness

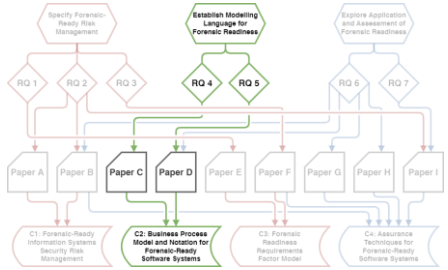


RQ4: How to capture the dynamics of the potential evidence within the forensic-ready software systems?

- Representing the system as a process model
  - Capturing system's dynamics in a scenario-like manner
  - Emphasis on potential evidence lifecycle and relationships
- Utilised in multiple settings to support forensic-ready design
  - Model running scenarios
  - Capture and reason about system within a case study

MUNI FI

Establish Modelling Language for Forensic Readiness

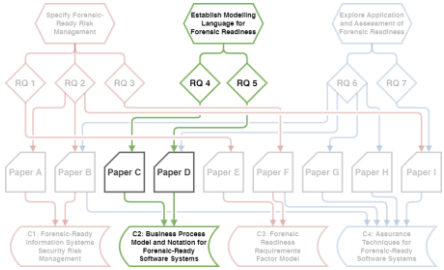


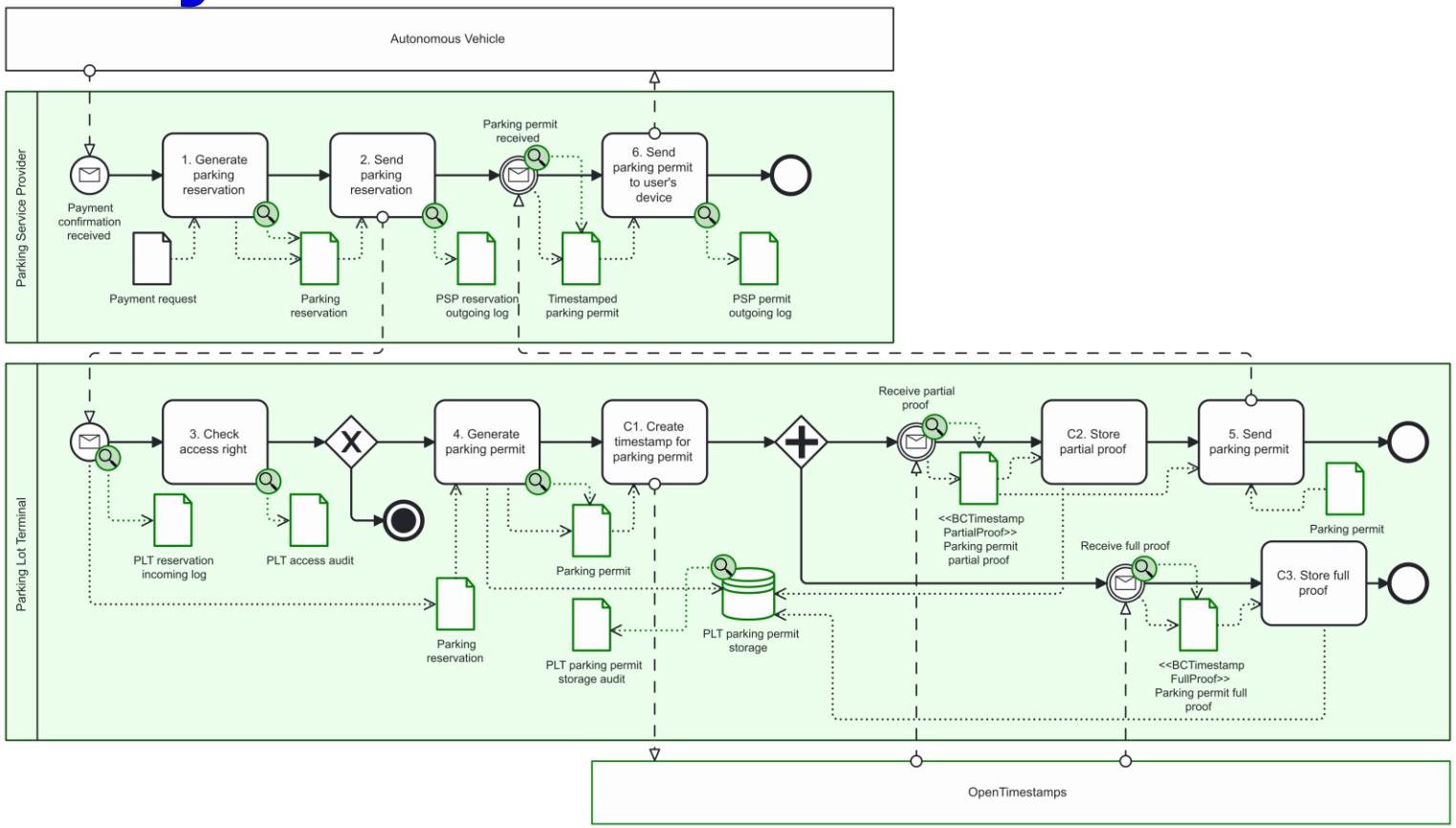
RQ5: How can be the concepts of forensic-ready risk management represented as models?

- Clarification of model's semantics
- Aligned the model with FR-ISSRM
  - The risk management concepts can be instantiated and used in the process
  - Allows for model-based assessment
- Joint representation with Security risk-oriented BPMN

MUNI FI

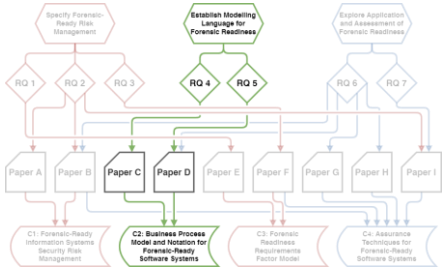
BPMN for Forensic-Ready Software Systems





MUNI FI

Establish Modelling Language for Forensic Readiness



Publication Summary

- Business Process Model and Notation for Forensic-Ready Software Systems
  - **Lukas Daubner** and Raimundas Matulevičius
  - ENASE, 2022 **[CORE B]**
  - *Introduces a novel modelling notation: BPMN for Forensic-Ready Software Systems*

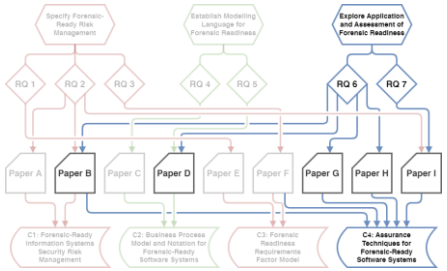
- BPMN4FRSS: An BPMN Extension to Support Risk-Based Development of Forensic-Ready Software Systems
  - **Lukas Daubner**, Raimundas Matulevičius, Barbora Buhnova, and Tomas Pitner
  - ENASE, **Selected Papers**, 2023 **[CORE B]**
  - *Provides more details on semantics, clarifies requirements and controls representation*

MUNI FI

Explore Application and Assessment of Forensic Readiness

MUNI
FI

Explore Application and Assessment of Forensic Readiness

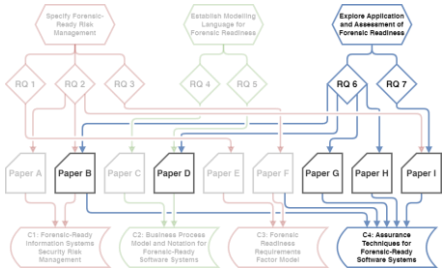


RQ6: What are the evaluation techniques of forensic-ready software systems utilising models?

- Explored the required evaluation target
- Forensic readiness metrics
  - Used within forensic-ready risk management
  - For establishing state of the system and to verify the requirements
- Model rules
  - Defining what is not allowed in the design
  - Hinting towards improvements

MUNI FI

Explore Application and Assessment of Forensic Readiness

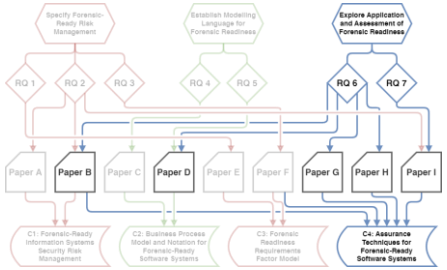


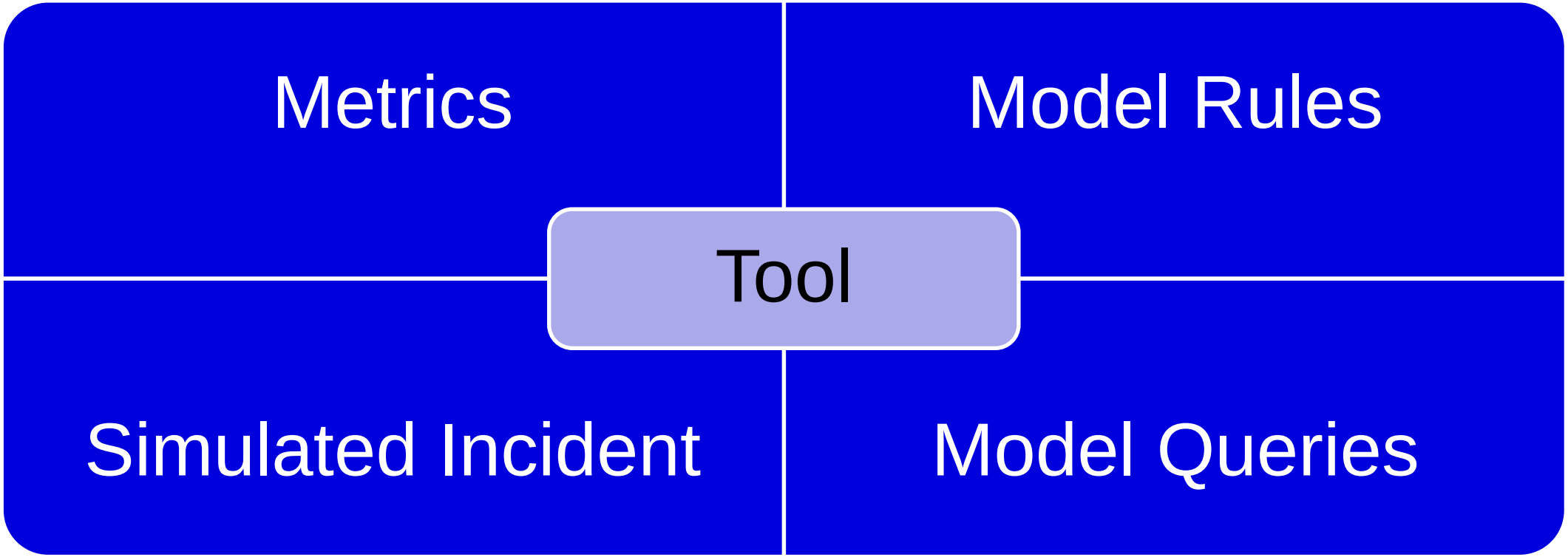
RQ7: How can the forensic readiness of a system be evaluated by utilising empirical knowledge?

- Planned and performed a case study involving an existing system
  - Established model based on risk management protocol and stakeholder engagement
- Simulated incident investigation
  - Evaluating the system in near-realistic scenario
  - Combining technology, people, and processes
  - Hands-on experience for stakeholders
  - Findings translated into forensic readiness requirements

MUNI FI

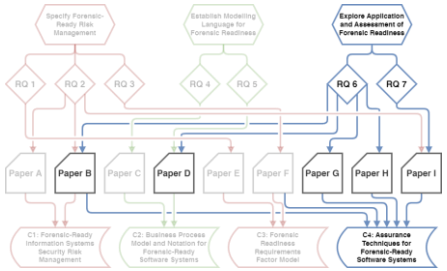
Assurance Techniques for Forensic-Ready Software Systems





MUNI FI

Explore Application and Assessment of Forensic Readiness



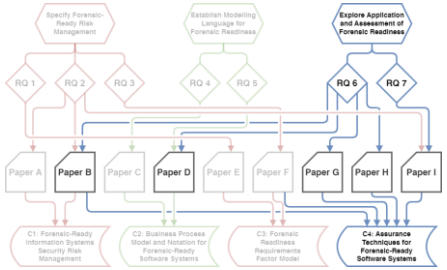
Publication Summary

- Verification of Forensic Readiness in Software Development: A Roadmap
  - **Lukas Daubner**, Martin Macak, Barbora Buhnova, and Tomas Pitner
  - SAC, 2020 **[CORE B]**
  - *Presents the problem of forensic-ready software systems verification, together with its objectives*

- Towards verifiable evidence generation in forensic-ready systems
  - **Lukas Daubner**, Martin Macak, Barbora Buhnova, and Tomas Pitner
  - Big Data, 2020
  - *Organises the challenges of verifying of potential evidence generation and discusses the approaches to designing, developing, and refining a verification method*

MUNI FI

Explore Application and Assessment of Forensic Readiness



Publication Summary

- A Case Study on the Impact of Forensic-Ready Information Systems on the Security Posture
  - **Lukas Daubner**, Raimundas Matulevičius, Barbora Buhnova, Matej Antol, Michal Růžička, and Tomas Pitner
  - CAiSE, 2023 **[CORE A]**
  - *Conducts a case study of integrating forensic readiness capabilities into an existing information system, and reports lessons learned in a practical implementation of a forensic-ready system*

MUNI FI

Conclusion

- Forensic-Ready Information Systems Security Risk Management
  - Forensic readiness domain model and risk management process
  - Supported by Forensic Readiness Requirements Factor Model
- BPMN for Forensic-Ready Software Systems
  - Modelling support for the design and risk assessment
- Assurance and assessment
  - Metrics, Rules, Simulated incident
- Approach successfully applied on an existing system