IARIA

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

The Eighteenth International Conference on Emerging Security Information, Systems and Technologies
SECURWARE 2024

ALEXANDER LAWALL

Securing Enterprise Applications:

Security Models and Adaptive Access Control for Consistent Access Rights in Dynamic Environments

Keynote
Nice, November 2024

PROF. DR. ALEXANDER LAWALL

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Academic Roles

- Program Director, B.Sc. & M.Sc. Cyber Security and Cyber Security Management
- Professor in Cyber Security (Distance & On-site Learning)

Expertise

- System & Network Security
- Web Application & Cloud Security
- IoT and Industrial IT Security

Professional Affiliations

- Leadership Committee, "Management of Information Security" (Society for Informatics, GI)
- Professional Lead, "Security & GRC in IT" (Summit Leipzig)
- Member, Association of Cyber Forensics and Threat Investigators (ACFTI)
- Member, Zentrum Digitalisierung Bayern (ZD.B)

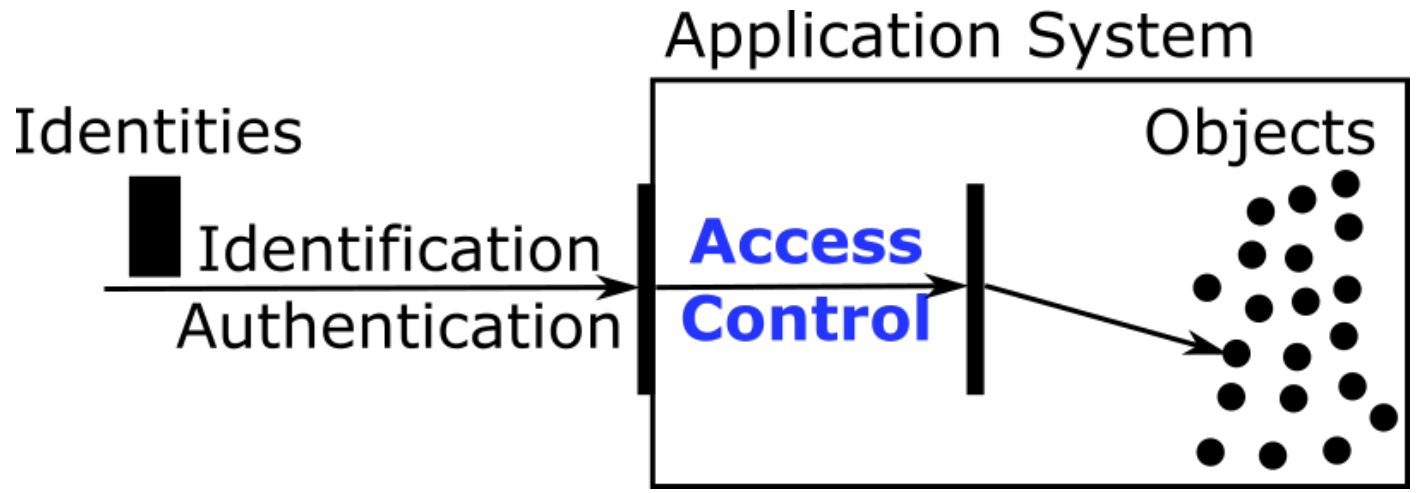
Research & Publications

- Focus Areas: Cyber Security, Information Security, Industry 4.0/5.0, IoT, Rights Management
- Publications in national/international Journals and Conferences
- Keynote Speaker, Program Chair, Panel Expert of International Conferences

AGENDA

INTRODUCTION AND RESEARCH SUBJECT

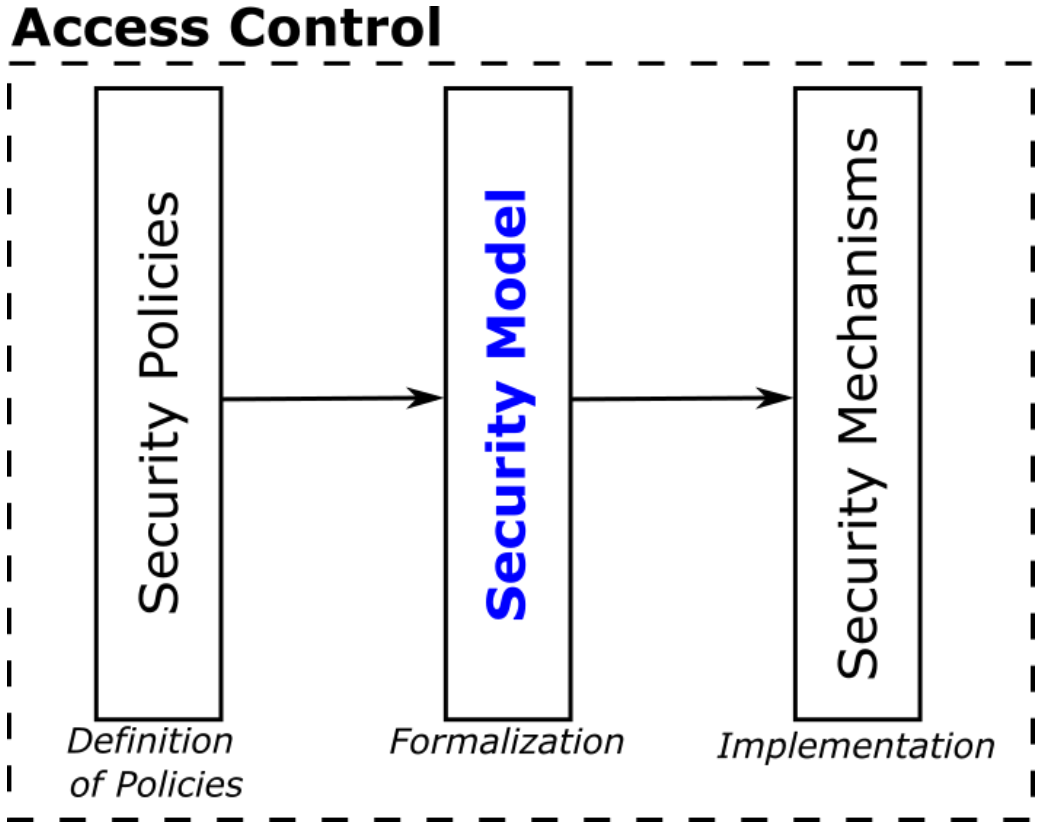
Access Control & Permissions



[cf. Seufert 2002 & Moschgath 2003]

INTRODUCTION AND RESEARCH SUBJECT

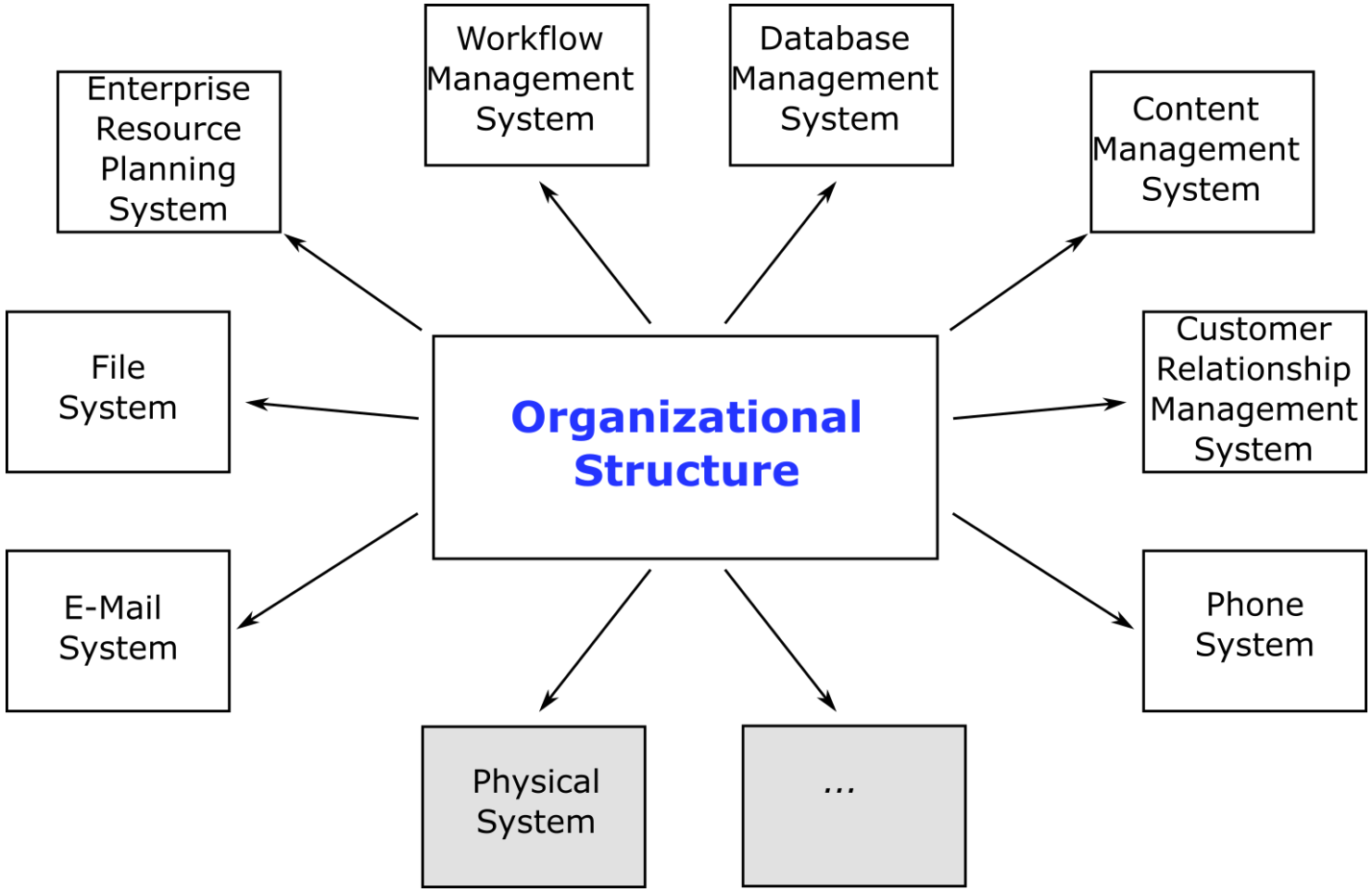
Phases of Access Control



[cf. Hansen, Mendling and Neumann 2015]

INTRODUCTION AND RESEARCH SUBJECT

Basis of Security Models



[cf. Ferraiolo, Kuhn and Chandramouli 2003; Hildmann 2010 & Goldstein and Frank 2012]

INTRODUCTION AND RESEARCH SUBJECT

Direct Assignment of Identities

Objects / Identities	Object 1	Object 2	…	Object n
Identity 1	Operations	Operations	…	Operations
Identity 2	Operations	Operations	…	Operations
…	…	…	…	…

[cf. Bell and La Padula 1976; Sandhu 1992 & Ferstl and Sinz 2013]

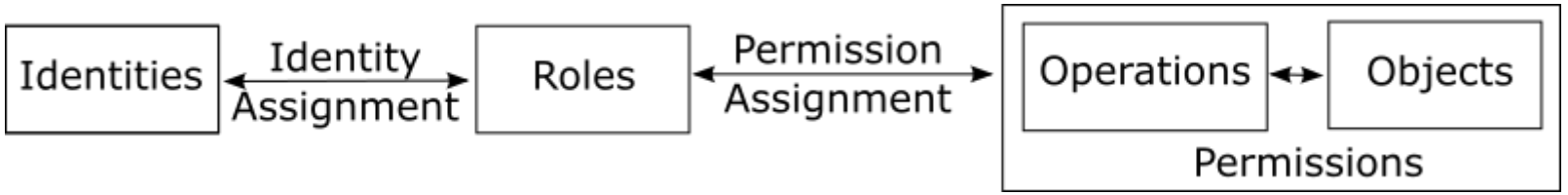
INTRODUCTION AND RESEARCH SUBJECT

Direct Assignment of Identities

Identities \ **Objects**	File **Report**	Table **Salary**	…	Workflow **Order**
Meier	{read, write}	{insert, change}	…	{create, execute}
Lawall	{read}		…	{execute}
…	…	…	…	…

INTRODUCTION AND RESEARCH SUBJECT

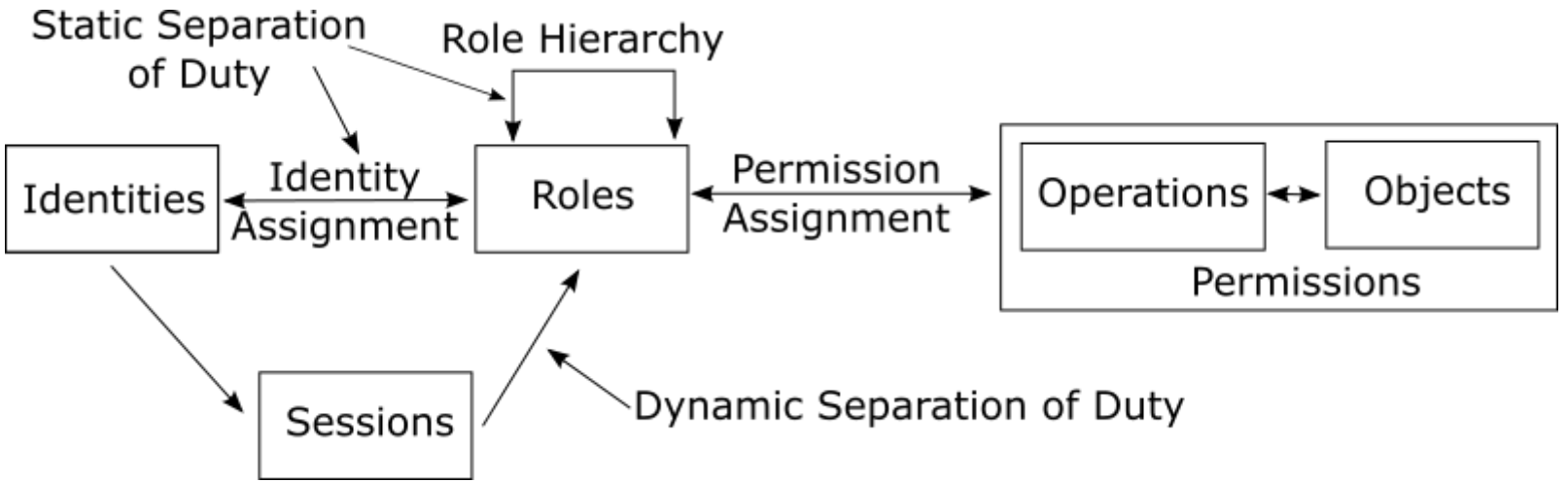
Role-based Assignment of Identities (RBAC)



[cf. Ferraiolo and Kuhn 1995 & Sandhu et al. 1996]

INTRODUCTION AND RESEARCH SUBJECT

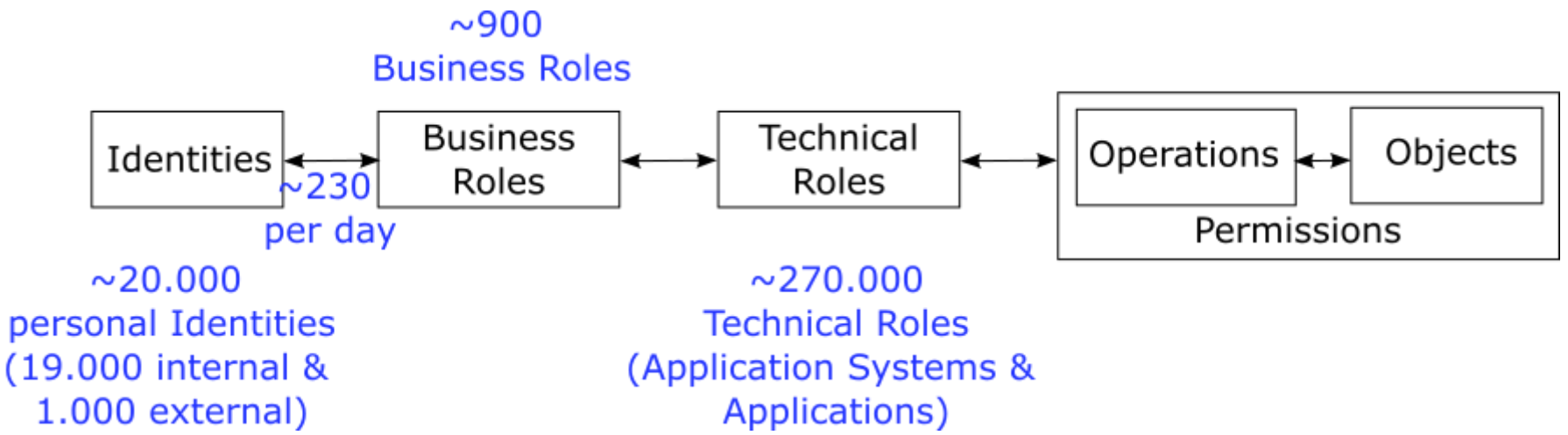
Role-based Assignment of Identities (RBAC)



[cf. Ferraiolo and Kuhn 1995 & Sandhu et al. 1996]

INTRODUCTION AND RESEARCH SUBJECT

(Enterprise) Role-based Assignment of Identities (ERBAC)



INTRODUCTION AND RESEARCH SUBJECT

Attribute-based Assignment of Identities (ABAC)

Attributes

- User Attributes (who is accessing the resource)
  - *Job title (e.g., doctor, nurse, admin)*
  - *Department (e.g., cardiology, pediatrics)*
  - *Clearance level (e.g., high, medium, low)*

- Resource Attributes (the data/resource being accessed)
  - *Data sensitivity (e.g., confidential, restricted)*
  - *Record type (e.g., patient notes, lab results)*

- Environmental Attributes (conditions for access)
  - *Time of access (e.g., business hours only)*
  - *Location (e.g., access allowed only on hospital premises)*
  - *Emergency status (e.g., relaxed rules during emergencies)*

[cf. Batth et al. 2021)

PROBLEM STATEMENT, RESEARCH GOAL & QUESTIONS

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Core Problem: *Inconsistent Assignment of Identities*

Partial Problem 1 (PP1): *Assignment through Full Enumeration*

- High susceptibility to changes

cf. Herwig and Schlabitz 2004, p. 290 & Linkies and Off 2006, p. 22

Partial Problem 2 (PP2): *Variety of Variants (structural-organizational and application-specific influencing factors)*

cf. Fischer 2015, p. 3

Partial Problem 3 (PP3): *Inadequacy (capability of the meta-model and relevance of the model)*

- Maintenance-intensive assignment of identities and discrepancy with reality

cf. Feng et al. 2004, p. 357; Strembeck and Neumann 2004, p. 393; Vahs 2007; Sinz et al. 2012; Eymann 2013

Key Consequences of Organizational Changes (Hiring, Moving, and Departure of Identities)

- *Anomalies in Access Rights/Permission*
- *Violations of Security Policies*
- *Lack of Compliance*

PROBLEM STATEMENT, RESEARCH GOAL & QUESTIONS

INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Research Goal: Development of a *meta-model for intra- and inter-organizational structures* and the *declarative* assignment of identities in business application systems

RQ1: *What elements are required for a structural-organizational meta-model?*

RQ2: *How are organizational identities declared in business application systems?*

RQ3: *What impact does the structural-organizational meta-model, including the declarative query language, have on maintenance effort?*

RQ4: *To what extent can change-related issues (e.g., anomalies, inconsistencies) in business application systems be reduced?*

RQ5: *Is the meta-model with the query language practically implementable?*

DEVELOPMENT OF THE ARTEFACT ($C\text{-}ORG$)

(Meta-)Model for Organizational Structures

Entity Types (+ Attribute Types $\mathcal{ATT}$ [cf. Lawall et al. 2015])

Organizational Units

- $O^{\mathcal{T}}$ at the template level [cf. Lawall et al. 2014c]
- O (intra-organizational O^{i} & inter-organizational O^{e}) [cf. Lawall et al. 2014a]

Functional Units

- $\mathcal{F}^{\mathcal{T}}$ at the template level [cf. Lawall et al. 2014c]
- F (intra-organizational F^{i} & inter-organizational F^{e}) [cf. Lawall et al. 2014a]

Identities (personnel & machine-based)

- A (intra-organizational A^{i} & inter-organizational A^{e}) [cf. Lawall et al. 2013a; Lawall et al. 2014a]

Relationship Types (+ Attribute Types $\mathcal{ATT}$)

Structural Relationships $\mathcal{R}_{s}$ (primary and secondary organization) [cf. Lawall et al. 2014a, Lawall et al. 2014c, Lawall et al. 2014, Lawall et al. 2015]

Organization-Specific Relationships $\mathcal{R}_{o}$ (reporting, supervisor, deputy relationships) [cf. Lawall et al. 2014a, Lawall et al. 2014c]

User-Defined Relationships $\mathcal{R}_{u}$ [cf. Lawall et al. 2014a, Lawall et al. 2014c, Lawall et al. 2014d]

Extensional Relationships $\mathcal{R}_{e}$ [cf. Lawall et al. 2014c]

Permission-Specific Relationships $\mathcal{R}_{p}$ (+ $\mathcal{L}_{\mathcal{M}}$) [cf. Lawall et al. 2014, Lawall 2015]

DEVELOPMENT OF THE ARTEFACT ($C\text{-}ORG$)

(Meta-)Model for Organizational Structures

Knowledge Hierarchy [cf. Lawall et al. 2014c]

$O^{\mathcal{T}}{}_{kl4}$, $\mathcal{F}^{\mathcal{T}}{}_{kl4}$ (template level)
O_{kl3} (organizational units level)
F_{kl2} (functional units level)
A_{kl1} (identities level)

Prioritization of Identities [cf. Lawall et al. 2014c]

Knowledge Hierarchy of the Organizational Model (“Level Algorithm”)

Limitation of Validity of Relations

Predicates on Relations ($\mathcal{L}_{\mathcal{P}}$) [cf. Lawall et al. 2014a, Lawall et al. 2014d]

Functional Unit Dependent Restrictions

- Hyperedge on Functional Unit from $r \in \mathcal{R}_o$ and $r \in \mathcal{R}_u$:
  $r = (A_1, A_2)$ with $A_1 \neq A_2$ or $A_1 = A_2$, respectively, or $r = (A, F)$ [cf. Lawall et al. 14a]

DEVELOPMENT OF THE ARTEFACT (*C-ORG*)

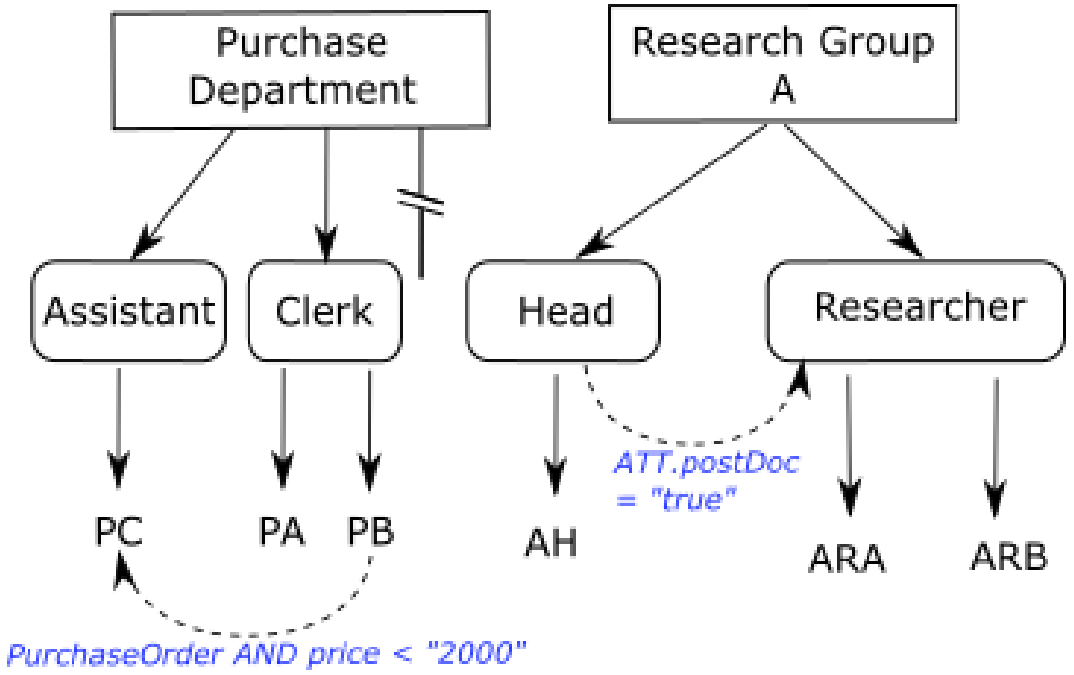
Language for Predicates ($\mathcal{L}_{\mathcal{P}}$)

Restriction of the Validity of Relations $\mathcal{R}_o$, $\mathcal{R}_u$ [cf. Lawall et al. 2014a , Lawall et al. 2014d]

Context from Application System (CONTEXT from $\mathcal{L}_{\mathcal{A}} \equiv \mathcal{L}_{\mathcal{P}}$)

Parameters from Application System (WITH clause in $\mathcal{L}_{\mathcal{A}}$ $(\equiv)$ $\mathcal{L}_{\mathcal{P}}$)

Attribute (in the Organizational Model)

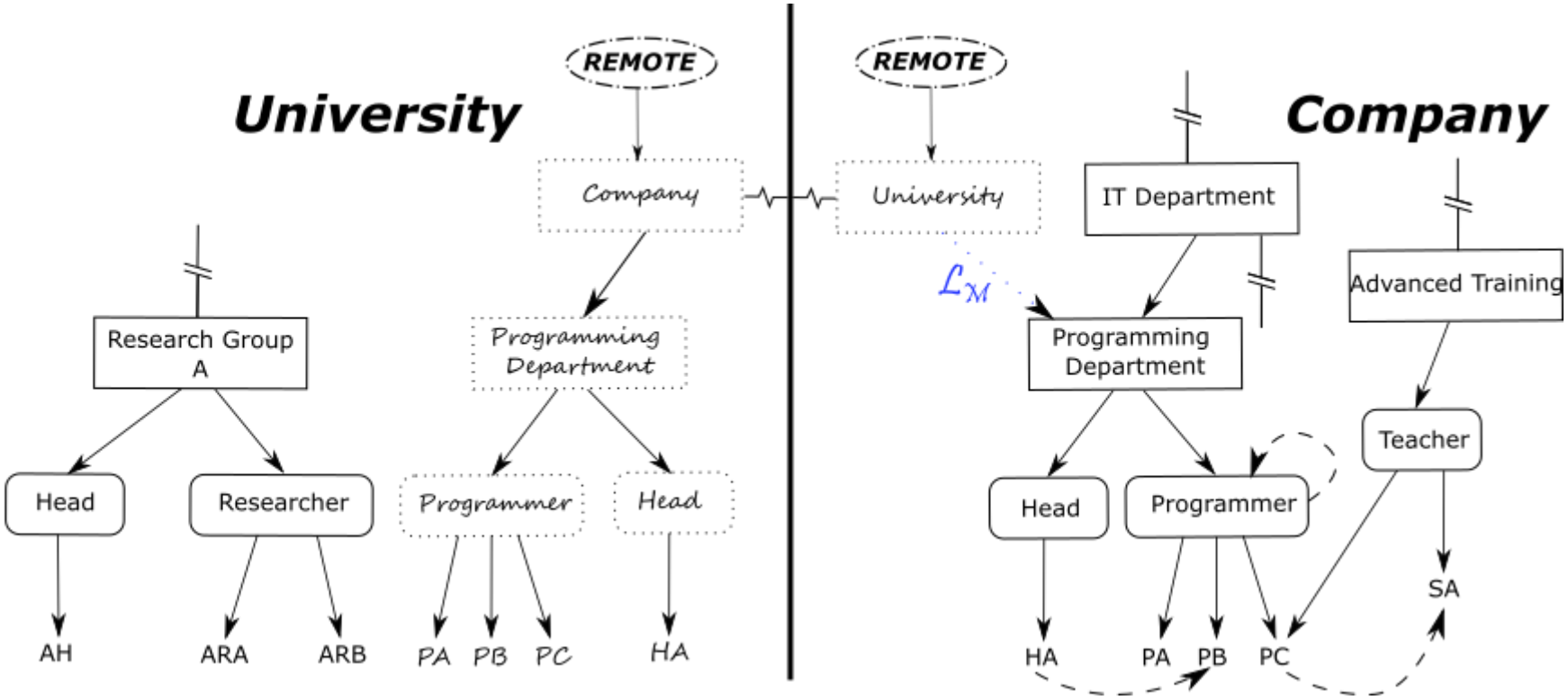


DEVELOPMENT OF THE ARTEFACT ($C\text{-}ORG$)

Language for Model Elements ($\mathcal{L}_{\mathcal{M}}$)

Expressions on Relations $\mathcal{R}_{\mathbf{p}}$ [cf. Lawall et al. 2014]

Propagation of Model Elements (including inter-organizational structures)



Example: $\mathcal{L}_{\mathcal{M}}$ = ENT.O OR ENT.F OR ENT.A OR REL.Structural OR ATT.name

DEVELOPMENT OF THE ARTEFACT (*C-ORG*)

Declarative Query Language ($\mathcal{L}_{\mathcal{A}}$) [Excerpt]

Declaration of Identities based on
Entities/Identities (e.g., "Lawall")
Relationships (e.g., SUPERVISOR OF (Researcher(Security)))
Attributes (e.g., Researcher(*).ATT.postdoc = "true")

Consideration of the Acting Functional Unit
Explicit: A AS F, e.g., "Lawall" AS Lecturer
Implicit: i.e., F(O), e.g., Researcher(Security)

Separation of Duty (e.g., Researcher(Security) NOT <Requester>)

Parameters from Application Systems (e.g., Researcher(Security) WITH price="20")

Prioritization of Identities
- FALLBACKTO: e.g., Researcher(Security) FALLBACKTO Head of(Security)
- Configuration of the Knowledge Hierarchy Levels, e.g., DEGREE = 0,F; DEGREE != 0

Combination of Language Expressions (i.e., AND | OR)

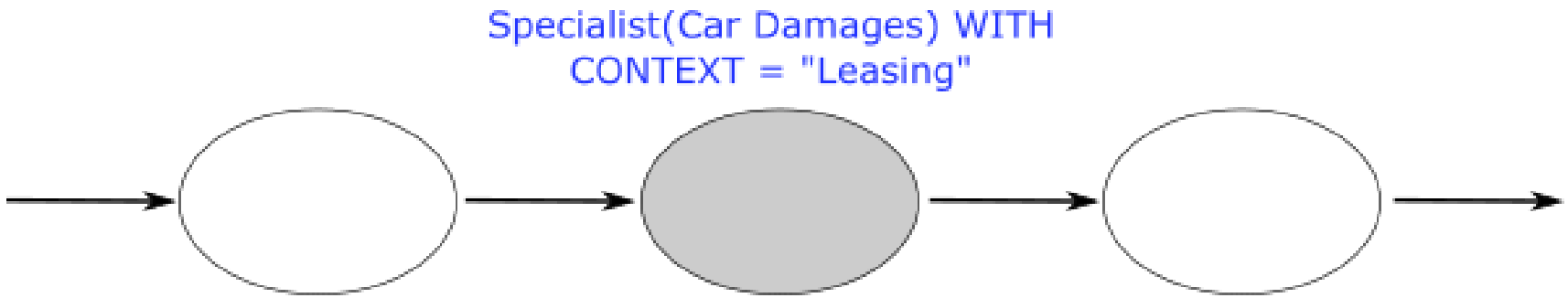
DEVELOPMENT OF THE ARTEFACT (*C-ORG*)

Application Scenarios

Definition of Access Rights

Objects / Identities	Object 1	Object 2	…	Object 3
President(University X) OR Professor(*)	{read, write}	{insert, change}	…	{create, execute}
…	…	…	…	…

Definition of Actors/Task Carriers



DEVELOPMENT OF THE ARTEFACT (*C-ORG*)

Application Scenarios

Definition of Recipients (e.g., functional mail addresses)

researcher-RG-security@uni.org

→ Researcher(Security)

apprentice-year-2@company.com

→ Apprentice(*).ATT.(Now() – Startdate) = “2”

Definition of Content

Attribute	Value
name	ATTRIBUTE name OF Head(Security)
email	ATTRIBUTE email OF Head(Security)
…	…

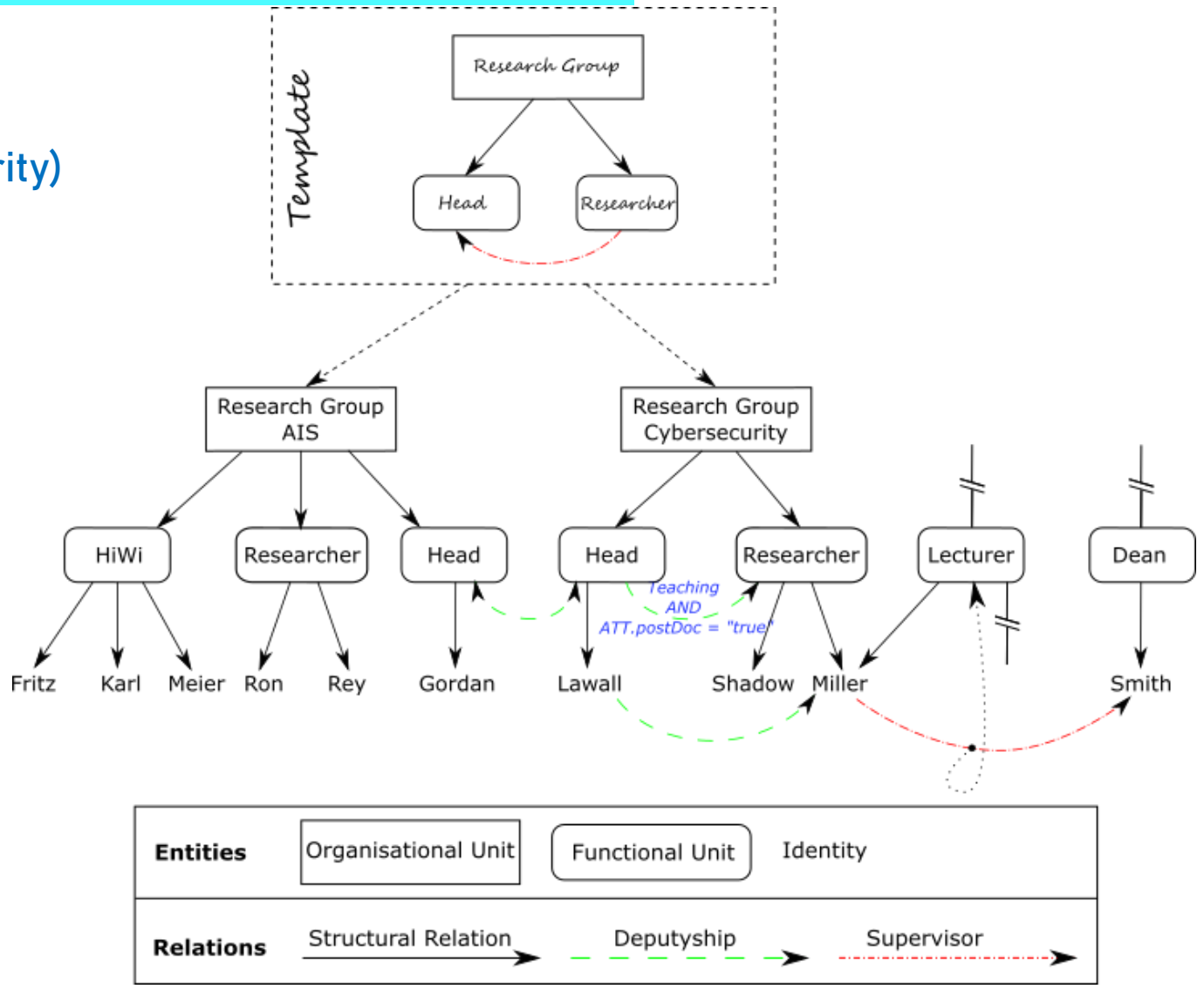
DEVELOPMENT OF THE ARTEFACT (*C-ORG*)

Identification of Identities in the Organizational Model

$\mathcal{L}_{\mathcal{A}}$ from Application System:

Head(Research Group Cybersecurity)

WITH CONTEXT = “Teaching”



CONCLUSION

Summary

(Meta-)Model & Formal Languages

- Representation of Organizational Structures (intra- & inter-organizational)
  [Meta-Model, Language for Predicates $\mathcal{L}_{\mathcal{P}}$, Language for Model Elements $\mathcal{L}_{\mathcal{M}}$]
- Consistent Assignment of Identities
  [Declarative Query Language $\mathcal{L}_{\mathcal{A}}$]

RQ1: *What elements are required for a structural-organizational meta-model?*

RQ2: *How are organizational identities declared in business application systems?*

RQ3: *What impact does the structural-organizational meta-model, including the declarative query language, have on maintenance effort?*

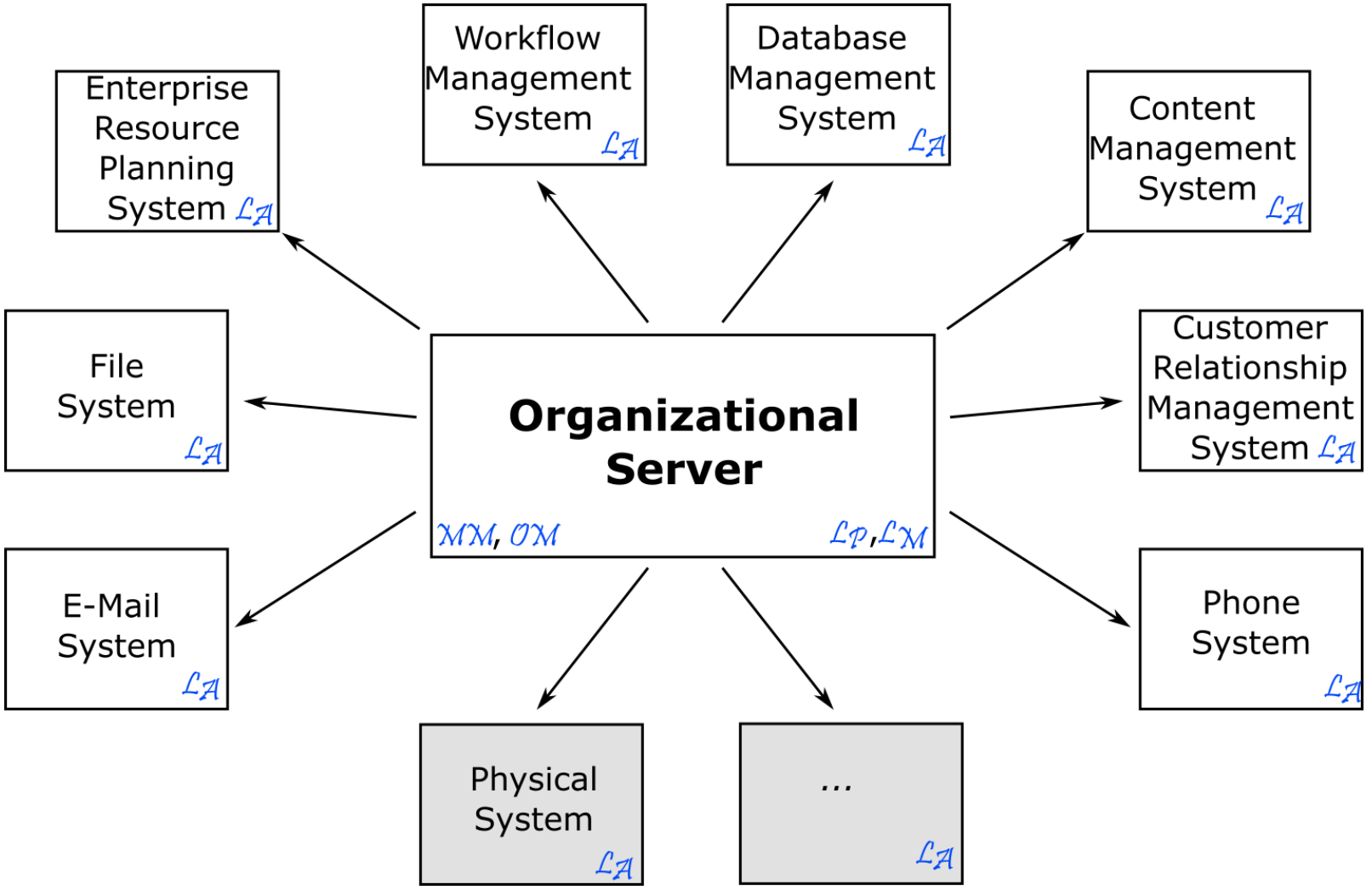
RQ4: *To what extent can change-related issues (e.g., anomalies, inconsistencies) in business application systems be reduced?*

RQ5: *Is the meta-model with the query language practically implementable?*

- No maintenance effort in application systems in case of organizational changes (join, move, leave of identities)
- Consistent Access Rights (i.e., Task Assignments, Recipients, Content)
- No violations of Security Policies

CONCLUSION

(New) System Landscape



INTERNATIONAL UNIVERSITY OF APPLIED SCIENCES

Discussion with

PARTICIPANTS(*)

Prof. Dr. Alexander Lawall
alexander.lawall@iu.org