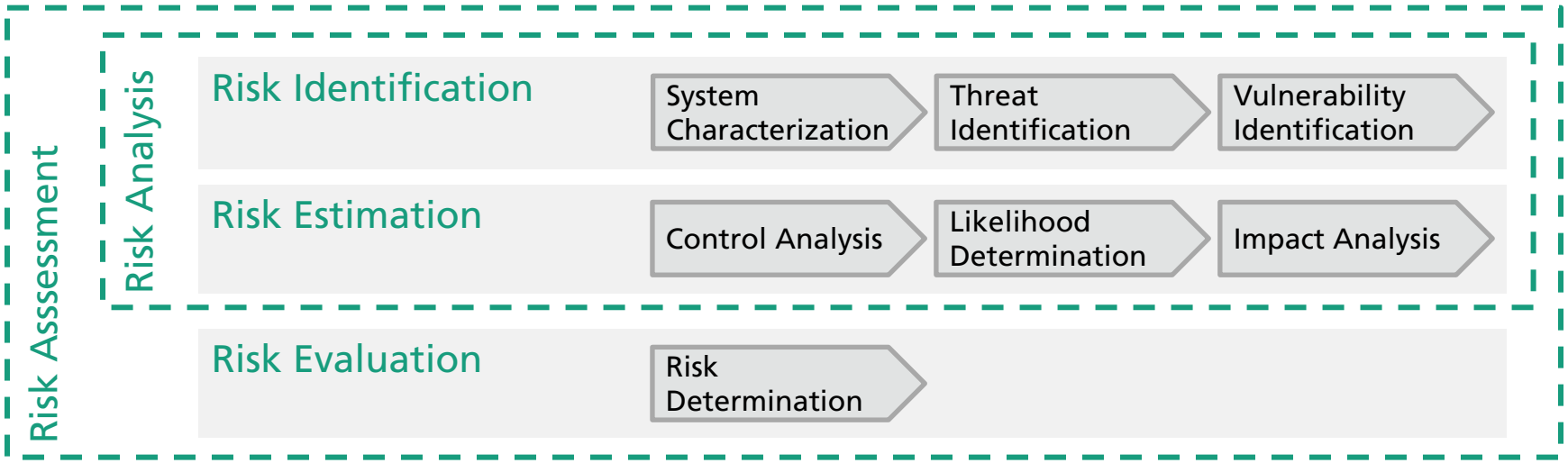
Selecting and Deploying Risk Assessment Methods for the Development Lifecycle

SASSI-Workshop Berlin

2015-09-16, Dr. Jörn Eichler

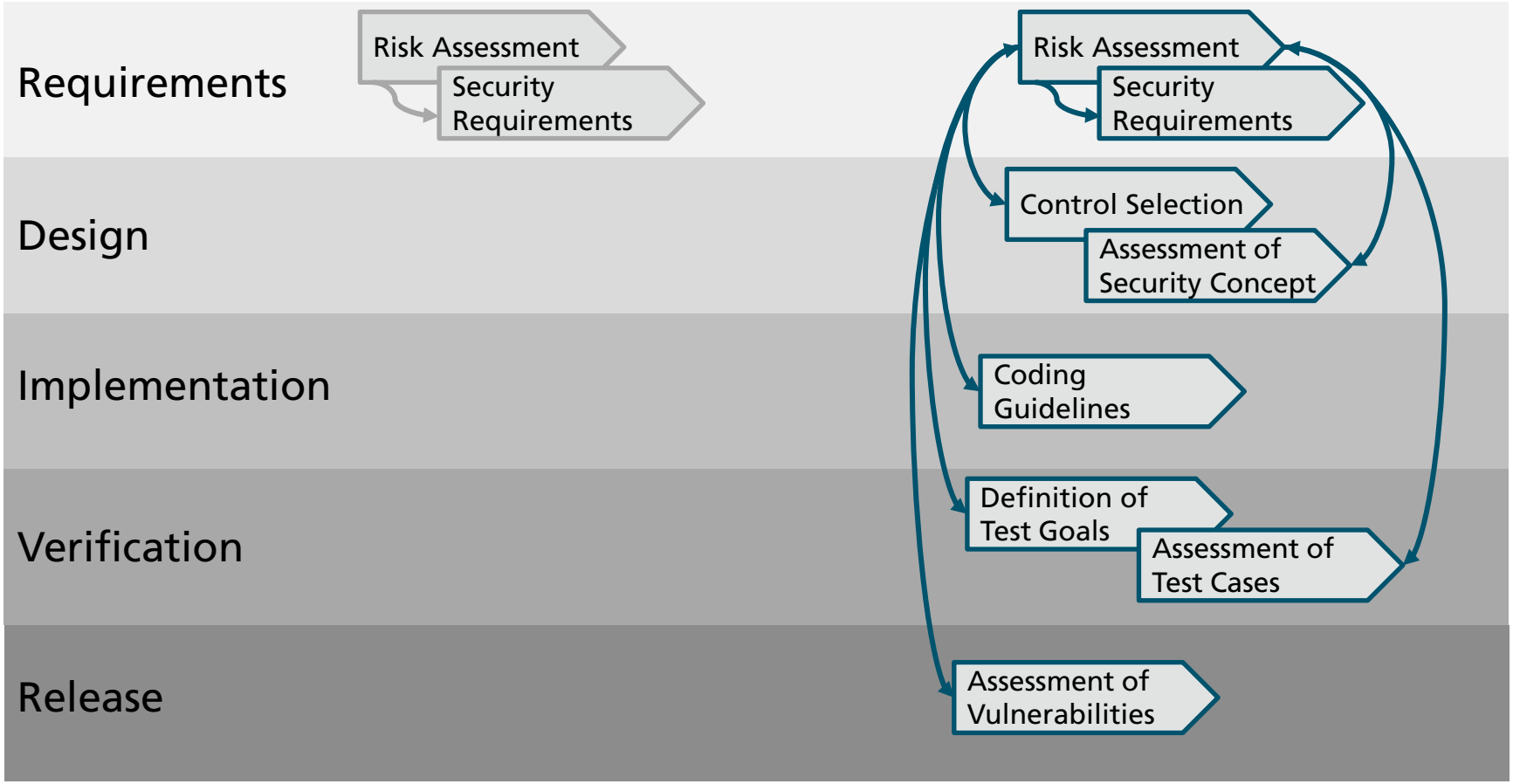


Fraunhofer AISEC

AGENDA

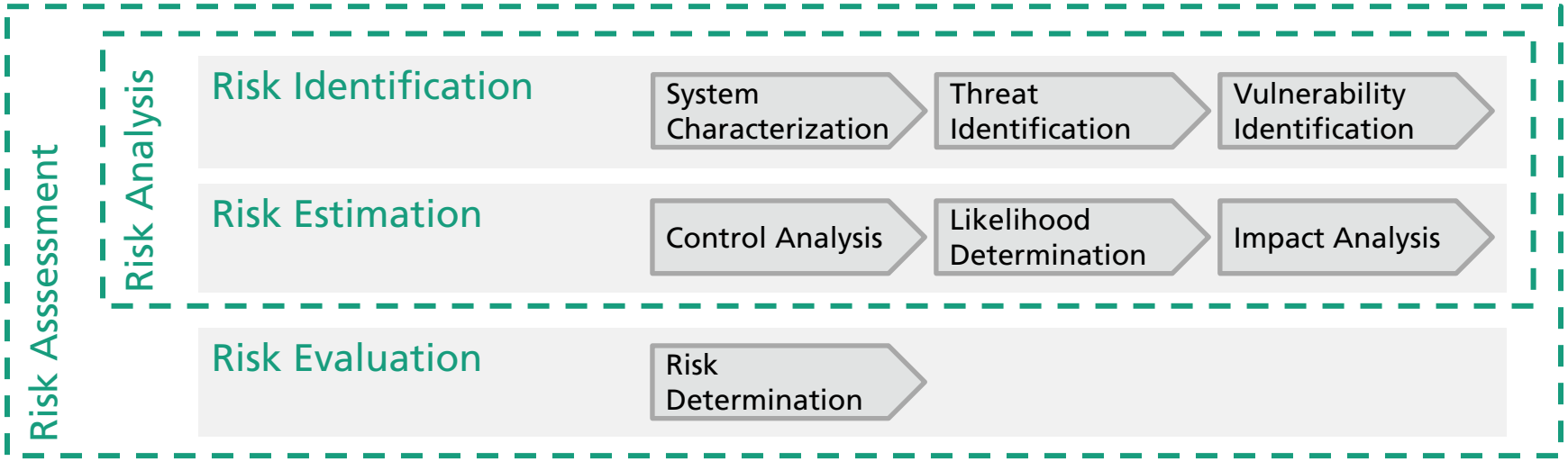
- Motivation
- Essentials
- Comparing approaches
- Tailoring approaches
- Summary

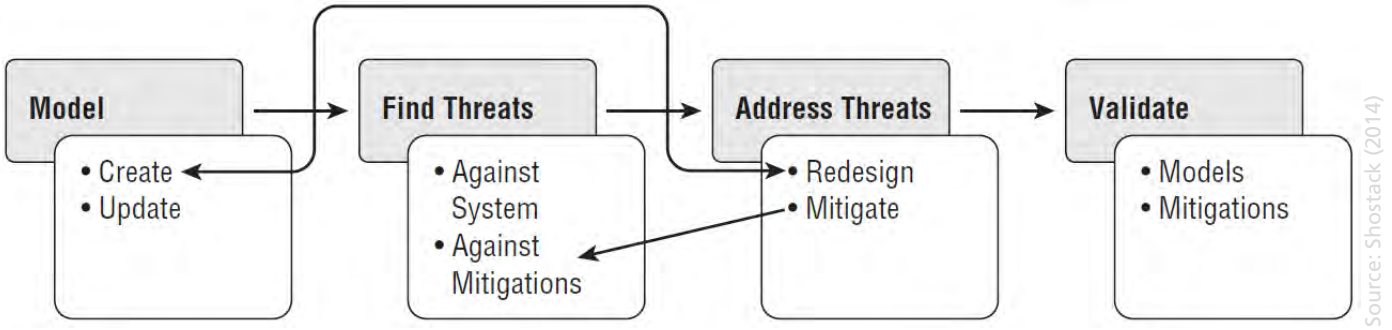
Motivation: The Case for Risk Assessment



Fraunhofer AISEC

Risk Assessment: Essentials





Fraunhofer AISEC

Evaluating Methods for Risk Assessment
(Köster et al. 2009)

Aspect	Criteria	Example: Microsoft
Audience	• Developer and architects • "Real world" environments	Addresses practitioners, rich application experience
Abstraction level	• Different level of abstraction	Multiple levels of data flow diagrams (DFDs)
Collaboration support	• Role model • Asynchronous execution • Knowledge sharing	Supports templates but provides no defined roles and no knowledge base
Evaluation target	• Quantification not required • Ongoing assessments	Focus on concrete scenarios, estimation very weakly supported
Models and techniques	• Specified data structure and notation • Intended vs. current level of security • Reuse of existing model information	DFD and templates provided but intended/current level is not clearly distinguished
Validation and plausibility	• Verification of results • Explication of assumptions • Metrics for assurance level • Tool support with audit trail	Tool provided and assumptions are explicated but verification, assurance level, and audit trail not really

Source: Köster et al. (2009)

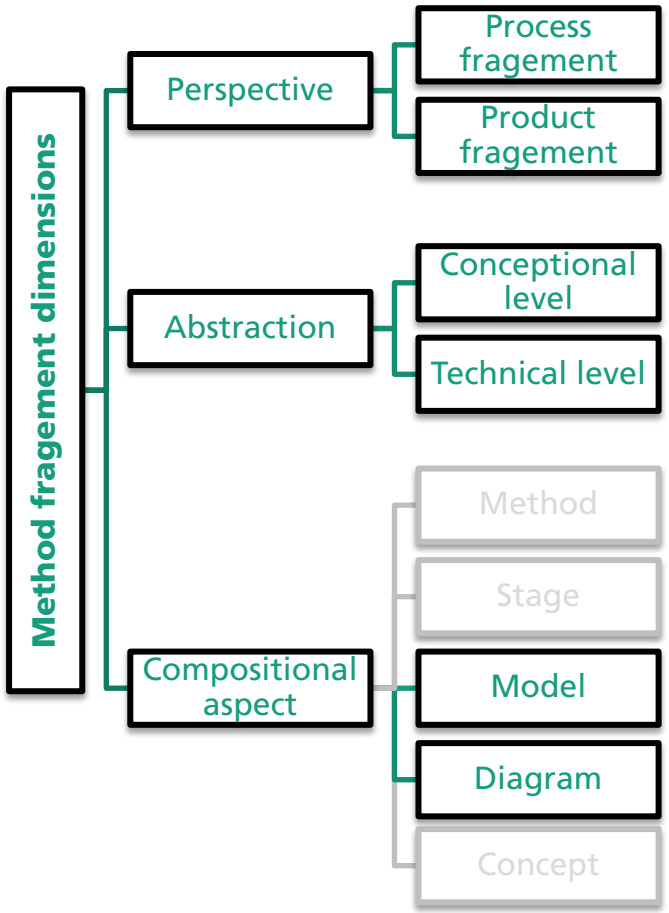
Exemplary Evaluation of Multiple Methods
(Köster et al. 2009)

Aspect	CORAS	OCTAVE	Trike	EBIOS	Microsoft
Audience	◒	◒	○	○	●
Abstraction level	●	○	●	○	●
Collaboration support	◒	◒	○	◒	◒
Evaluation target	◒	◒	◒	○	○
Models and techniques	●	○	●	◒	◒
Validation and plausibility	◒	○	◒	◒	◒

Source: Köster et al. (2009)

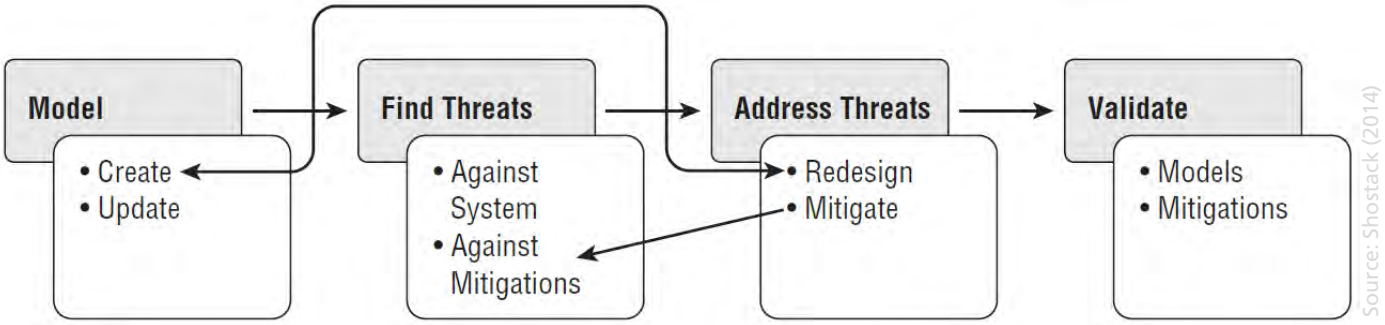
Analyzing and Decomposing Methods
Applying a Method Engineering Framework

- A method
  - is a repeatable procedure
  - that specifies the steps
  - involved in solving a specific problem
- Method Engineering
  - *Selection and assembly* of method fragments to provide adequate methods
  - Situational method engineering "encompasses all aspects of creating a development method for a specific situation" (Brinkkemper 1996)



Fraunhofer AISEC

Exemplary Method Analysis: SDL/A Threat Modeling



Source: Shostack (2014)

Fragment	Short name	Dimensions	Method chunks
F1.1	Diagram creation	pro / conc / dia	C1.1
F1.2	Threat identification	pro / conc / mod	C1.2
F1.3	Selection of mitigations	pro / conc / mod	C1.3
F1.4	Identification of update needs	pro / conc / mod	C1.4
F1.5	Model validation	pro / conc / mod	C1.5
WP1.1	DFDs	prd / conc / dia	C1.1, C1.2, C1.3, C1.4, C1.5
WP1.2	Threats	prd / conc / mod	C1.2, C1.3, C1.4, C1.5
WP1.3	Mitigations	prd / conc / mod	C1.3, C1.4, C1.5
T1.1	Threat modeling tool	prd / tech / mod	(C1.1), (C1.2), (C1.3), (C1.4), (C1.5)

Source: Renatus et al. (2015)

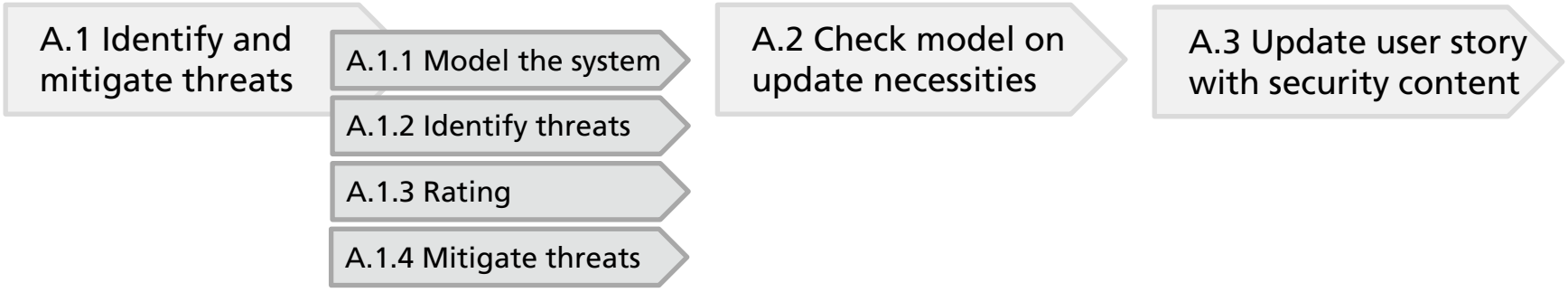
Method Comparison Based on Decomposition

	SDL/A Threat Modeling	AVS Threat Modeling	Threat Modeling Express
Non-Monolicithy	● (5)	● (5)	○ (2)
Segmentation of product fragments	◒	●	○
Additional artifacts	●	●	●
Policies / guidelines	●	◒	○
Scrum modifications: activities / work products	● / ○	○ / ●	○ / ○
Estimations	◒	◒	○

Source: Renatus et al. (2015)

Fraunhofer AISEC

Method Tailoring Based on Decomposition



Chunk	Short name	Process fragment	Work products	Related chunks
C.1	Model system	A.1.1	WP.1	C1.1
C.2	Identify threats	A.1.2	WP.1, WP.2	C1.2
C.3	Mitigate threats	A.1.4	WP.1, WP.2, WP.3	C1.3
C.4	Check update necessities	A.2	WP.1, WP.2	C1.4, C2.2
C.5	Update user story	A.3	WP.1, WP.2, WP.3, WP.4	C2.1
C.6	Rating	A.1.3	WP.1	C2.4

Source: Renatus et al. (2015)

Fraunhofer AISEC

Summary

- Risk assessment is a cornerstone for secure software
- Many activities depend on up-to-date risk assessments
- Therefore, choose your risk assessment method wisely
  - Understand differences between existing approaches
  - Investigate your internal requirements
- COTS methods do not always fit your needs
  - Tailoring increases acceptance and benefit
  - Systematic approaches for analysis and tailoring provide means for streamlined adoption

Contact

Fraunhofer Institute for
Applied and Integrated Security (AISEC)

Parkring 4, 85748 Garching near Munich
Alexanderstr. 9, 10178 Berlin (Berlin Office)

Dr. Jörn Eichler

Head of Department „Secure Software Engineering“

Tel.: +49 89 32299 86-152
Fax: +49 89 32299 86-299

joern.eichler@aisec.fraunhofer.de
http://www.aisec.fraunhofer.de/

References

ISO (2008)	ISO 27005: Information technology — Security techniques — Information security risk management
Köster et al. (2009)	Information security assessments for embedded systems development: An evaluation of methods. *Proceedings of 8th Annual Security Conference*
NIST 800-30 (2002)	Risk Management Guide for Information Technology Systems
Renatus et al. (2015)	Method Selection and Tailoring for Agile Threat Assessment and Mitigation. *Proceedings of the First International Workshop on Agile Secure Software Development (ASSD)*
Shostack (2014)	Threat Modeling: Designing for Security. *Wiley*

