Supporting Evolving Security Models for an Agile Security Evaluation

Wolfgang Raschke, Massimiliano Zilli, Philip Baumgartner
Johannes Loinig, Christian Steger, Christian Kreiner

TU Graz - Institute for Technical Informatics
NXP Semiconductors - Business Unit Identification (BUID)

David Project
Funded under the FIT-IT contract FFG 832171 by the Austrian Federal Ministry for Transport, Innovation, and Technology

Today‘s Java Card Applications

- E-money
- Credit card
- Transport
- Access Control
- Passport

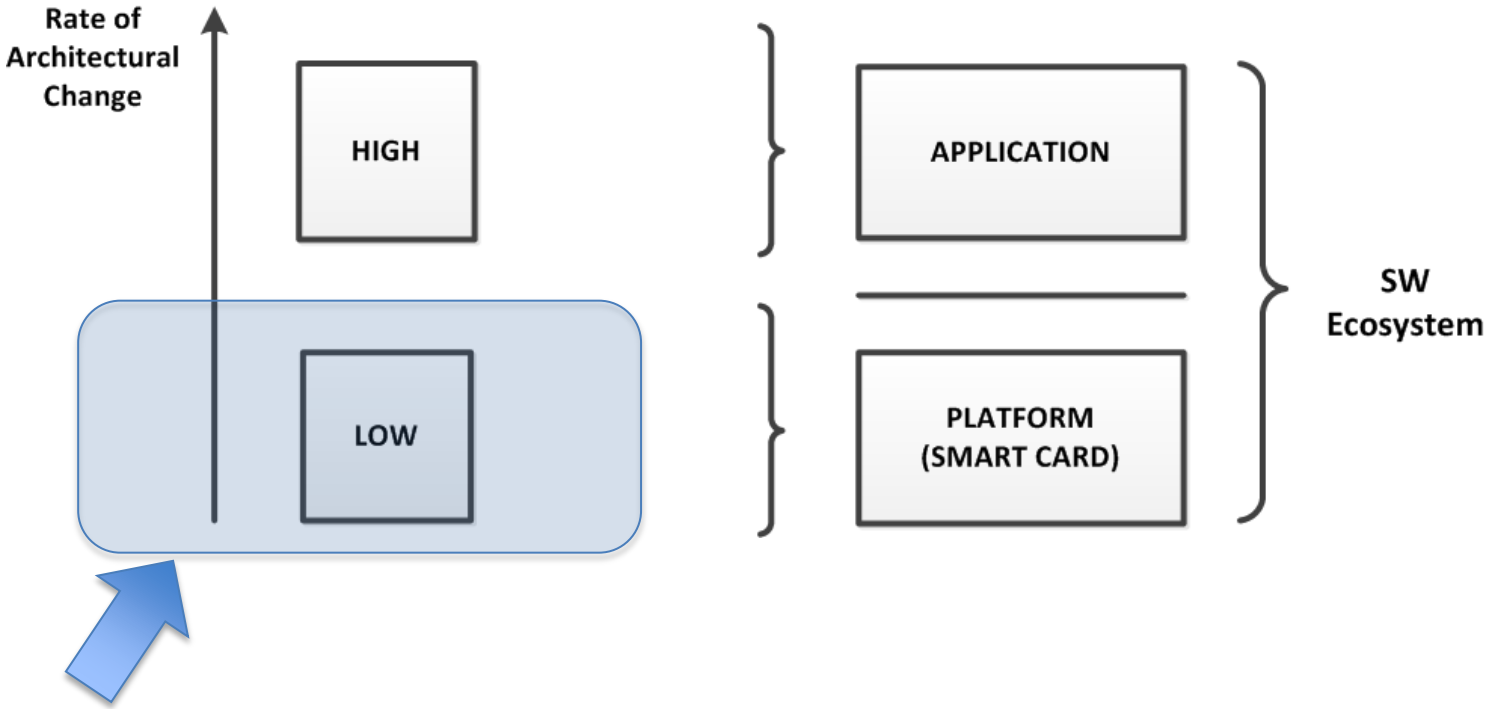
Market Volatility

- High rate of innovation (application scenarios)
- (Lead) customer interaction
- Time-to-market (Common Criteria)
- Early validation

Research Problem

- **Agile security** evaluation
- Evolution of **problem** and **solution** space
- How to support **evolution of a model**
  - Tools?
  - Processes?

Methodology: Limitations



Region of Applicability

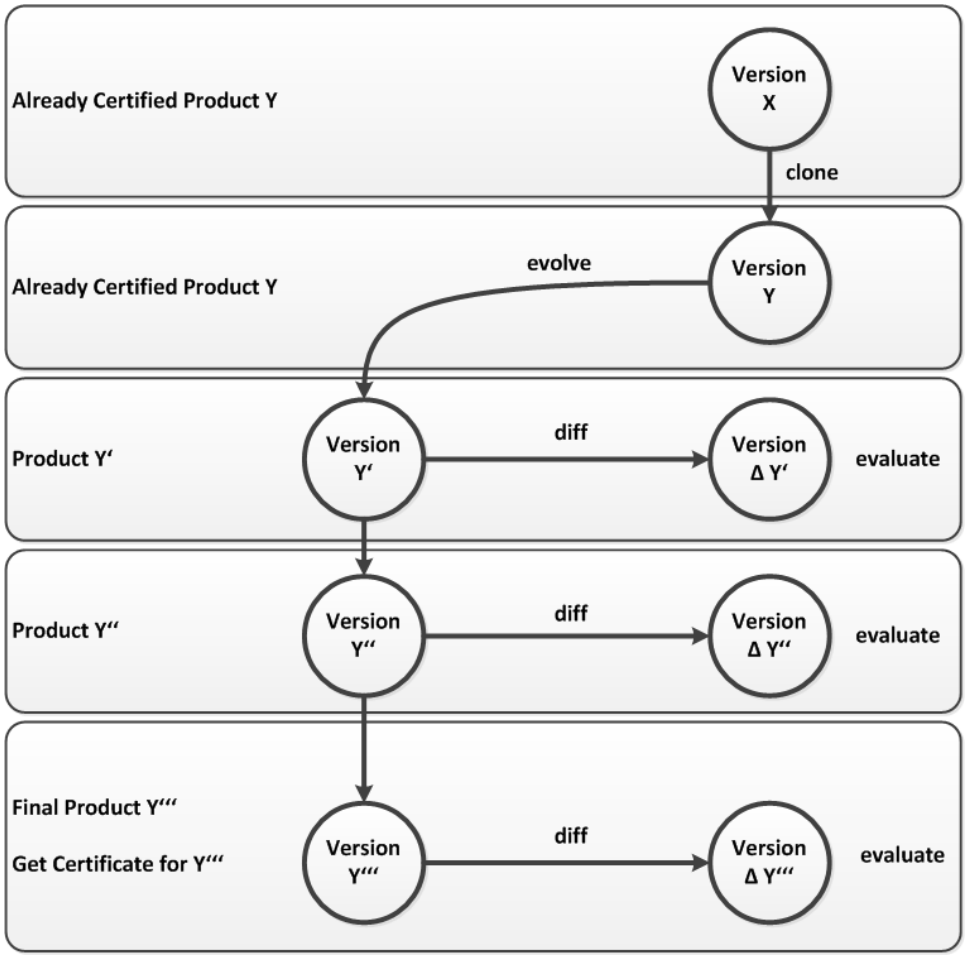
[Henderson1990] [Christensen2013] [Messerschmitt2005]

Single System Development vs. Clone and Own

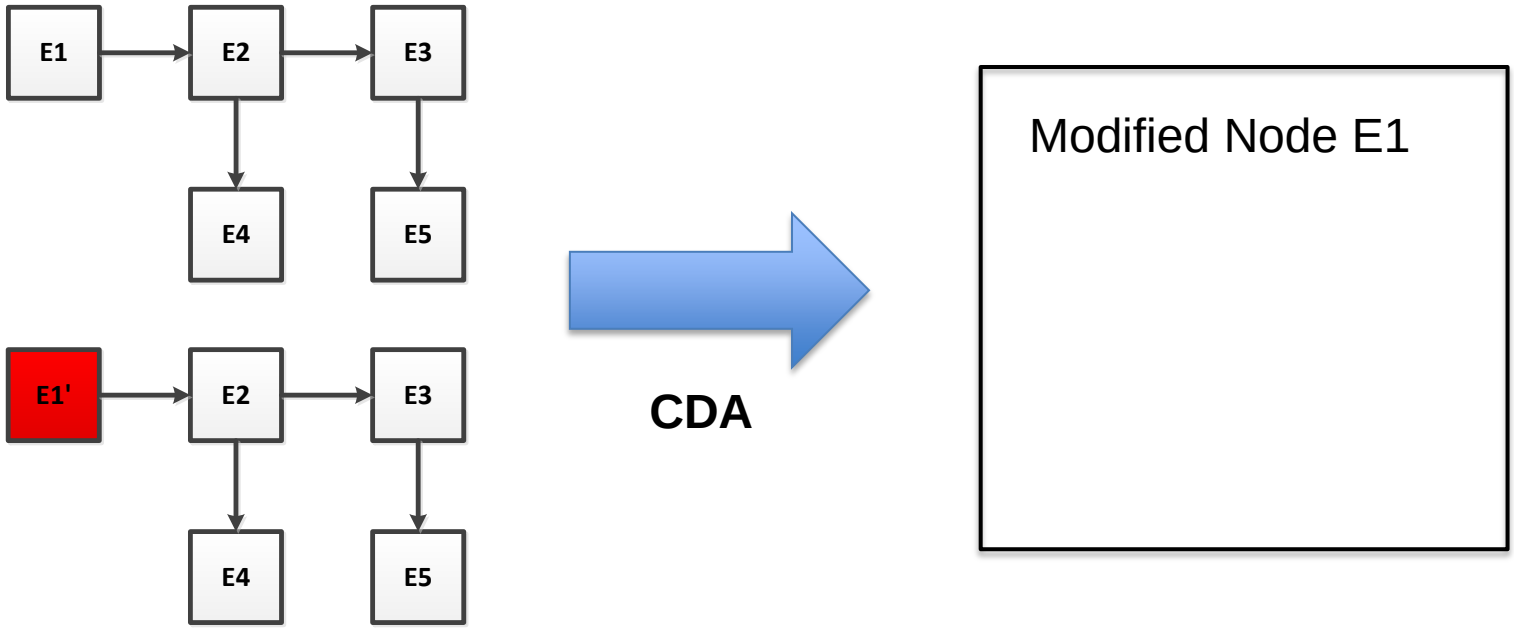
- Single system development
  - Completely new requirements
  - Always start from scratch
  - Architectural evolution
  - Radical evolution
- Clone & Own
  - Copy and adapt to new requirements
  - Often used in practice
  - Incremental evolution
  - Modular evolution

Region of Applicability

Model Evolution: Clone and Own

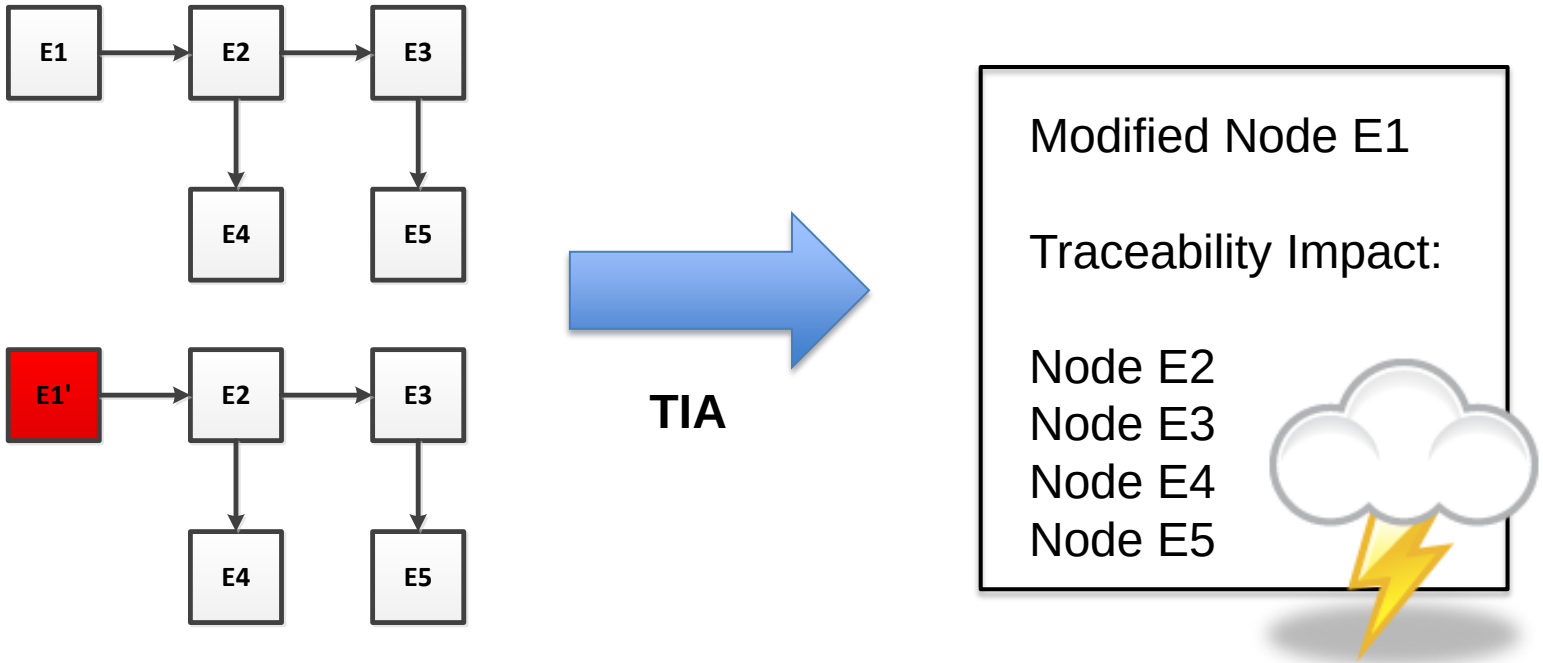


Change Detection Analysis



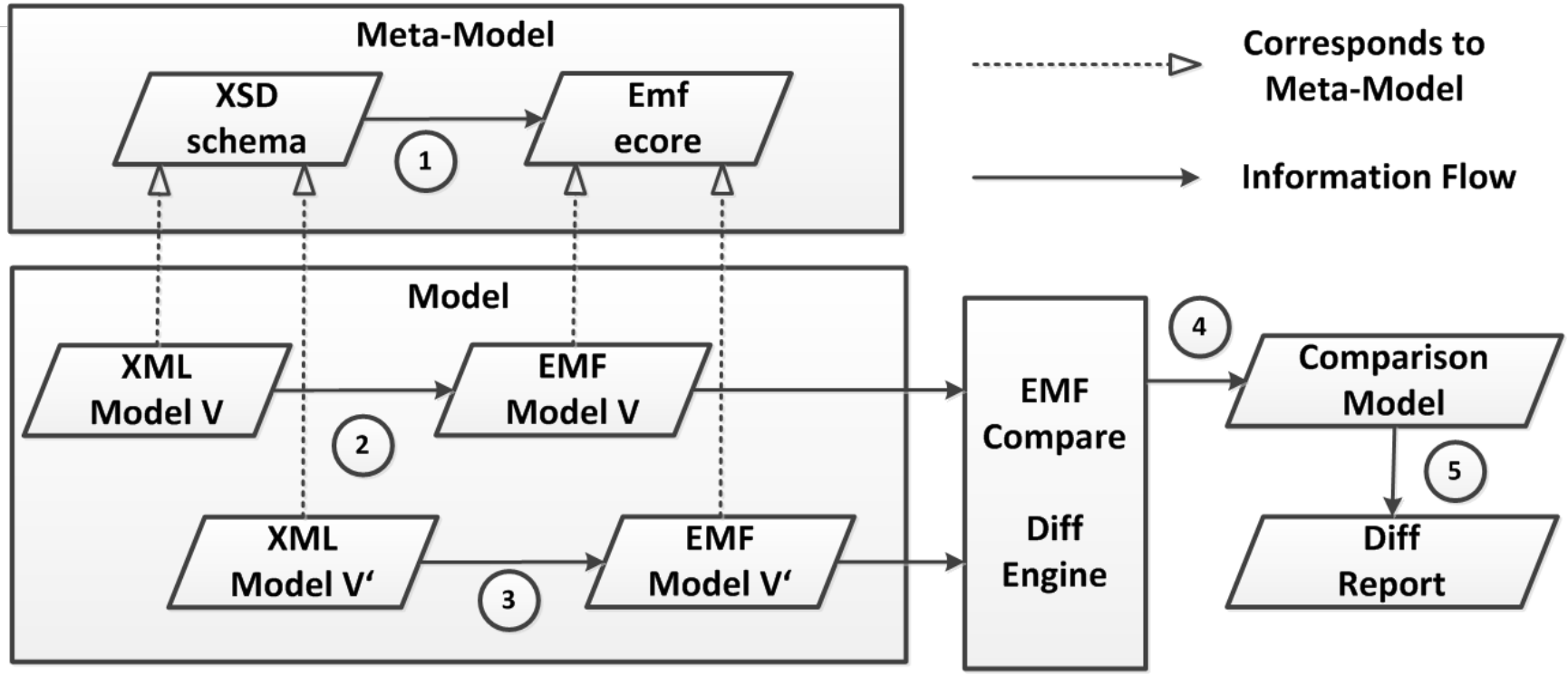
[Altmanninger2009] [Brun2008]

Traceability Impact Analysis

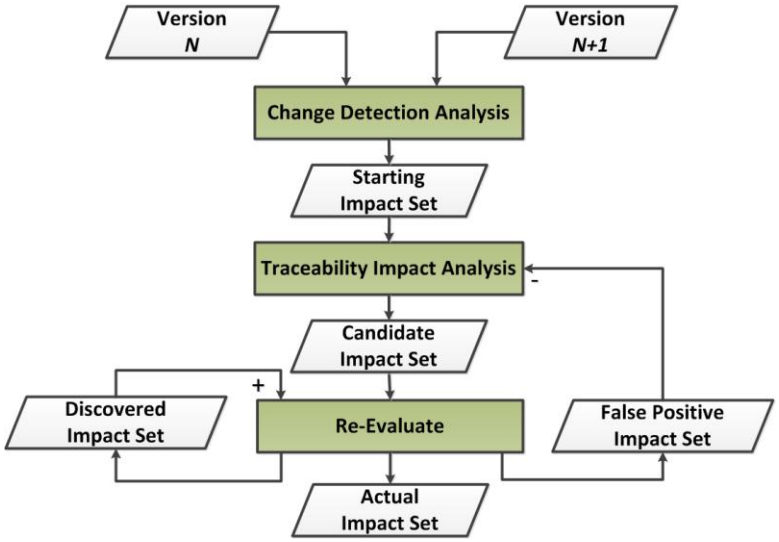


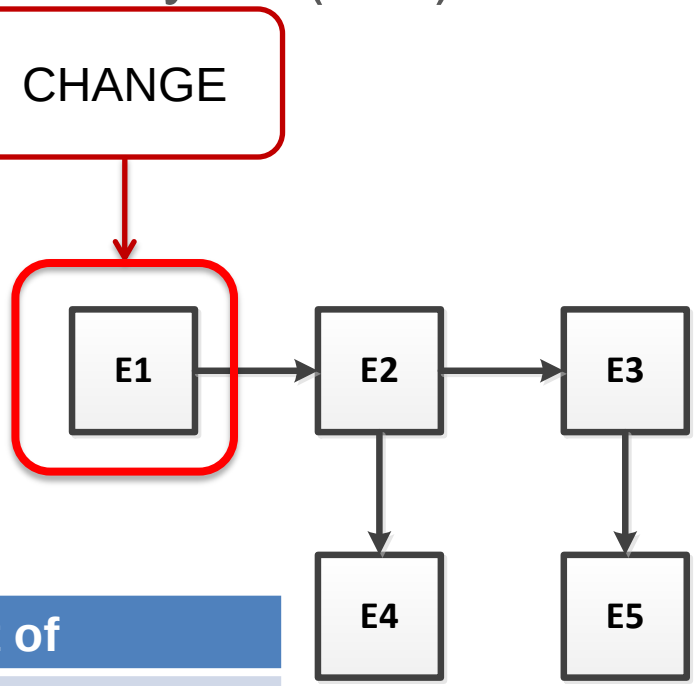
[Bohner2002]

Implementation Model-Diff



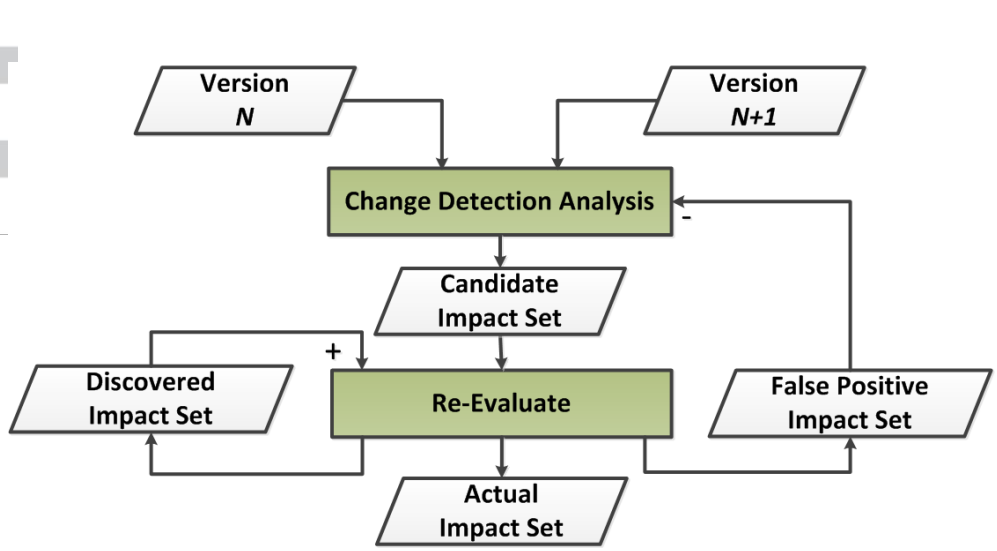
Process with Traceability Impact Analysis (TIA)

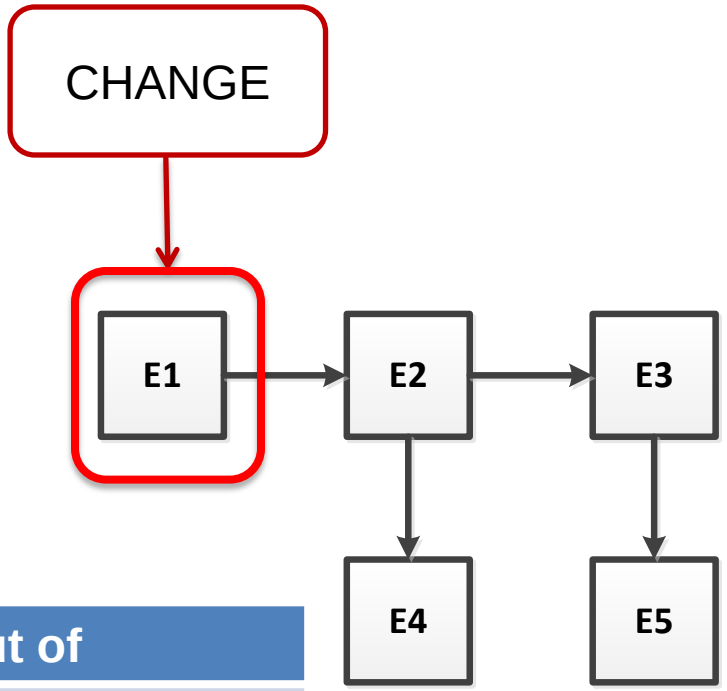




	Set	Output of
Starting Impact Set	{E1}	CDA
Candidate Impact Set	{E1,E2,E3,E4,E5}	TIA
Discovered Impact Set	{}	re-evaluation
False Positive Impact Set	{E3,E4,E5}	re-evaluation
Actual Impact Set	{E1,E2}	re-evaluation

Process With Experiential Impact Analysis (EIA)



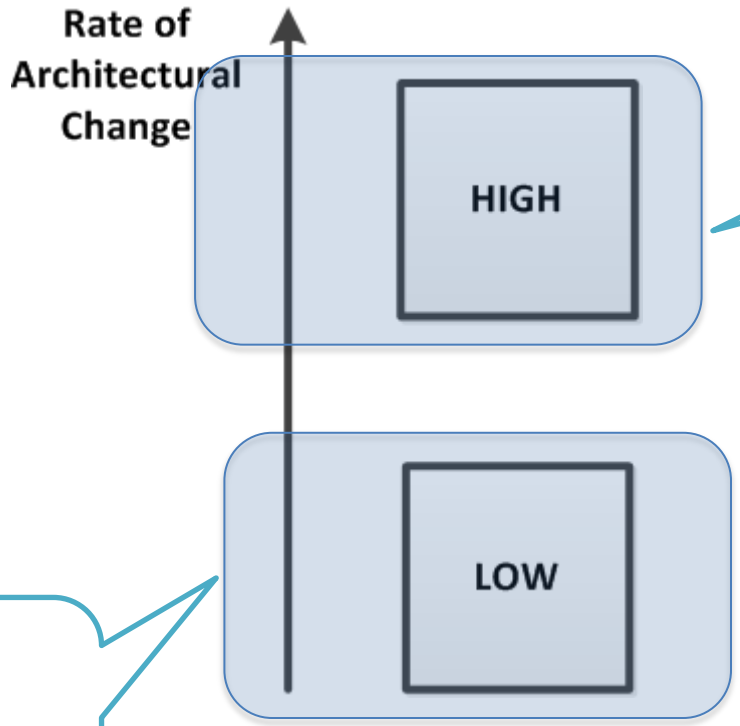


	Set	Output of
Candidate Impact Set	{E1}	CDA
Discovered Impact Set	{E2}	re-evaluation
False Positive Impact Set	{}	re-evaluation
Actual Impact Set	{E1,E2}	re-evaluation

Conclusions

	TIA Process	EIA Process
Affinity	Delta Evaluation	Agile Evaluation
Process	Formal	Informal
Focus On	Formal Correctness	Human Experience
Presumed Experience	LOW	HIGH
Validation Principle	Opt Out	Opt In
Iteration Cycle	Months/Years	Weeks
Time-to-Market	-	+
DIS	SMALL	LARGE
FPIS	LARGE	SMALL

Future Work



FUTURE:
How can security evaluation be tailored to support this area?

CURRENT: Region of Applicability

Implications for Security Evaluation?

Thank you!

wolfgang.raschke@tugraz.at
https://www.iti.tugraz.at/

References

[Henderson1990] Henderson R.M., Clark K.B. (1990). Architectural innovation: the reconfiguration of existing product technologies and the failure of established firms. Administrative science quarterly, 9-30.

[Christensen2013] Christensen, C. (2013). The innovator's dilemma: when new technologies cause great firms to fail. Harvard Business Review Press.

[Messerschmitt2005] Messerschmitt, D. G., & Szyperski, C. (2005). Software ecosystem: understanding an indispensable technology and industry. MIT Press Books, 1.

[CC2009] Common Criteria (2009). Common Criteria for Information Technology Security Evaluation – Part 1-3. Version 3.1, Revision 3 Final

[Altmanninger2009] Altmanninger, K., Brosch, P., Kappel, G., Langer, P., Seidl, M., Wieland, K., & Wimmer, M. (2009, October). Why model versioning research is needed!? an experience report. In Proceedings of the MoDSE-MCCM 2009 Workshop@ MoDELS (Vol. 9).

[Brun2008] Brun, C., & Pierantonio, A. (2008). Model differences in the eclipse modeling framework. UPGRADE, The European Journal for the Informatics Professional, 9(2), 29-34.

[Bohner2002] Bohner, S. A. (2002, December). Extending software change impact analysis into cots components. In Software Engineering Workshop, 2002. Proceedings. 27th Annual NASA Goddard/IEEE (pp. 175-182). IEEE.