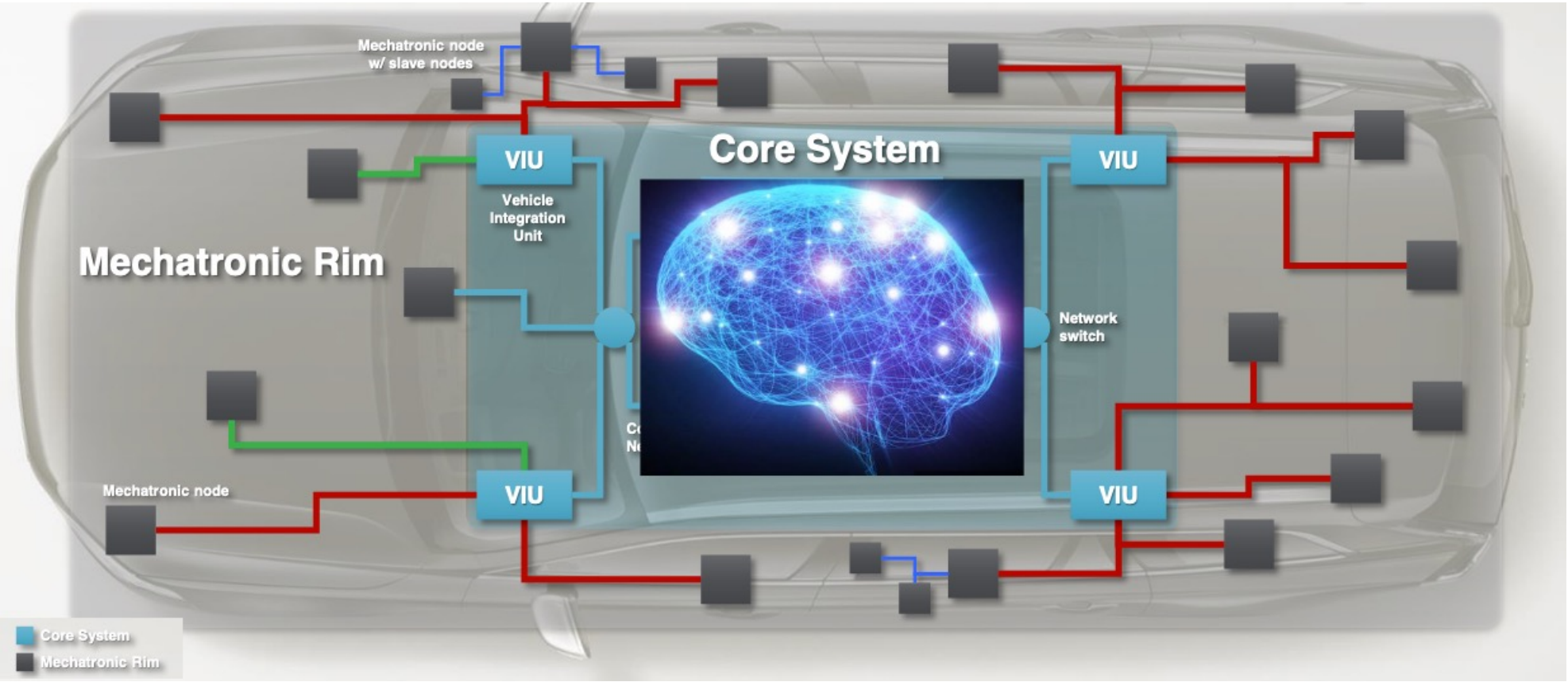
Cyber Resilience for Vehicles

REMIND: A Framework for the Resilient Design of Automotive Systems

Thomas Rosenstatter, Kim Strandberg, Rodi Jolak, Riccardo Scandariato, Tomas Olovsson

Published @ *IEEE SecDev 2020* | *here*

Centralised architecture



https://www.icse2018.org/getImage/orig/The+Car+%E2%80%93+computer+on+wheels.pdf

Resilience

Property of a system with the ability to maintain its intended operation in a dependable and secure way, possibly with degraded functionality, in the presence of faults and attacks.[1]

[1] *https://www.vinnova.se/en/p/cyrev-phase1---cyber-resilience-for-vehicles---cybersecurity-for-automotive-systems-in-a-changing-environment/*

REMIND: A Framework for the Resilient Design of Automotive Systems

→ Lead designers to the informed and optimal selection of resilience techniques to be implemented in an automotive system.

1) Systematically identify resilience techniques
2) Taxonomy comprising of the four strategies: detection, mitigation, recovery, and endurance (REMIND)
3) Associate the identified technqiues to automotive assets
4) Guidelines for using this framework incl. trade-off discussion

Overview

Query scopus database

- Focus on **already performed** literature reviews and surveys
- Included
  - resilien* | survivability | attack recovery | error recovery | error handling | fault tolerance
  - software | system | network
  - published after 2010
  - written in English
- Excluded
  - hardware | fpga | memory | wireless | SDN
- Limited to subject areas *Computer Science* and *Engineering*

Overview

Query scopus database

Manual review of **200 most relevant publications** returned by scopus

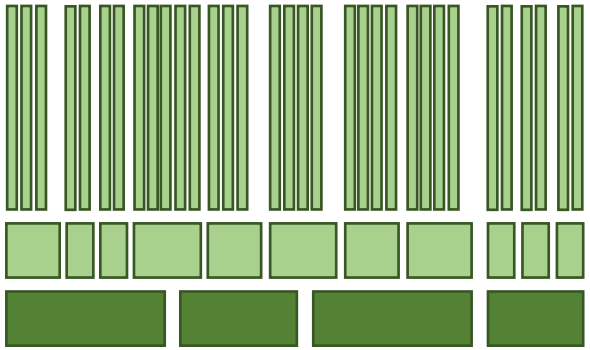
- Title and abstract screening and following full-text reading, we identified **8 relevant publications**
- **+ 3 additional publications and one NIST document**

Overview

Query scopus database

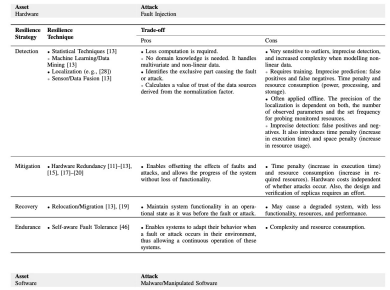
Manual review of 200 most relevant publications returned by scopus

Taxonomy



Collection and classification of identified techniques in taxonomy

Guidelines



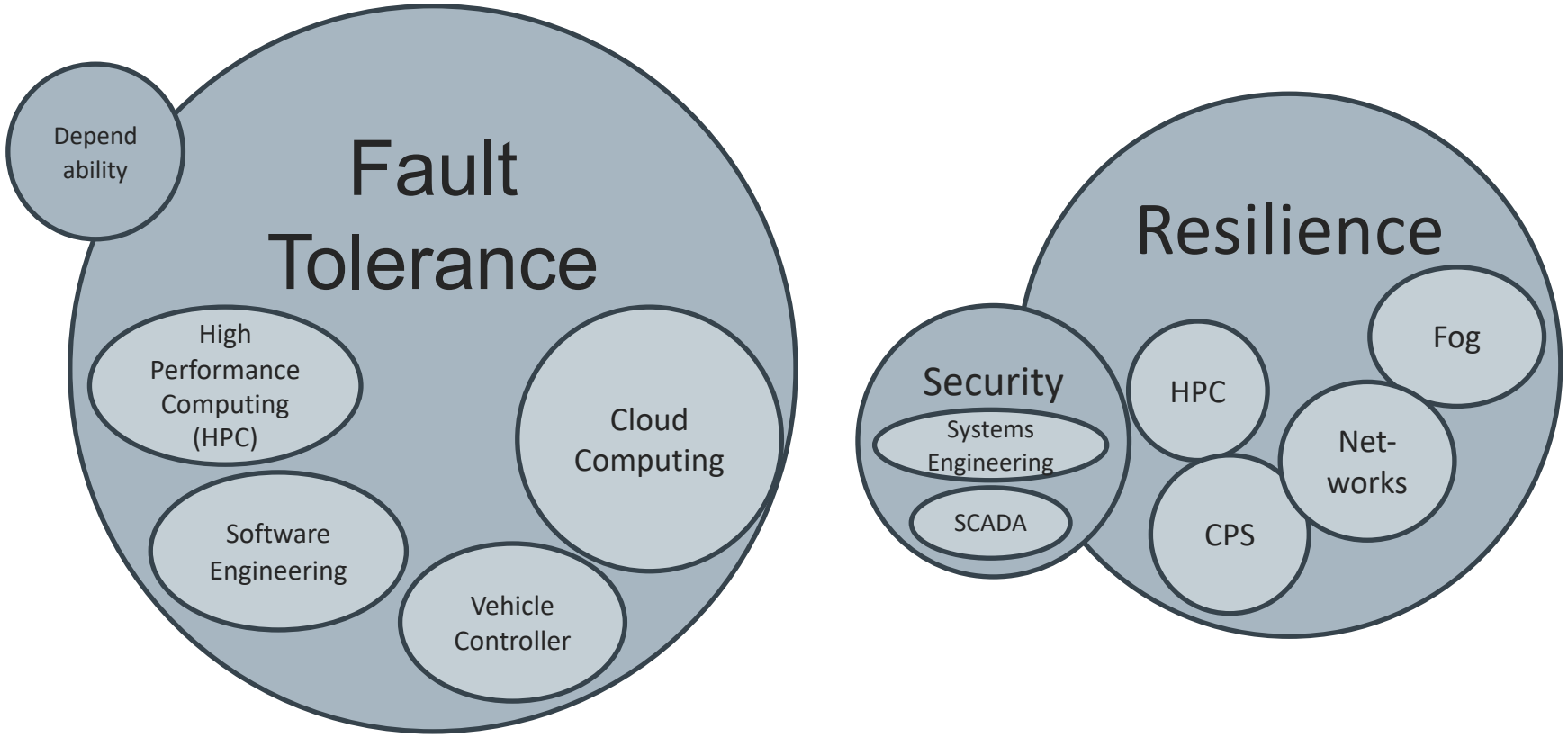
Asset	Attack
Hardware	Fault Injection

Resilience Strategy	Resilience Technique	Trade-off	
		Pros	Cons
Detection	• Statistical Techniques [13] - Machine Learning/Data Mining [13] • Localization (e.g., [28]) - Sensor/Data Fusion [13]	• Less computation is required. - No domain knowledge is needed. It handles multivariate and non-linear data. • Identifies the exclusive part causing the fault or attack. - Calculates a value of trust of the data sources derived from the normalization factor.	• Very sensitive to outliers, imprecise detection, and increased complexity when modelling non-linear data. - Requires training. Imprecise prediction: false positives and false negatives. Time penalty and resource consumption (power, processing, and storage). • Often applied offline. The precision of the localization is dependent on both, the number of observed parameters and the set frequency for probing monitored resources. - Imprecise detection: false positives and negatives. It also introduces time penalty (increase in execution time) and space penalty (increase in resource usage).
Mitigation	• Hardware Redundancy [11]–[13], [15], [17]–[20]	• Enables offsetting the effects of faults and attacks, and allows the progress of the system without loss of functionality.	• Time penalty (increase in execution time) and resource consumption (increase in required resources). Hardware costs independent of whether attacks occur. Also, the design and verification of replicas requires an effort.
Recovery	• Relocation/Migration [13], [19]	• Maintain system functionality in an operational state as it was before the fault or attack.	• May cause a degraded system, with less functionality, resources, and performance.
Endurance	• Self-aware Fault Tolerance [46]	• Enables systems to adapt their behavior when a fault or attack occurs in their environment, thus allowing a continuous operation of these systems.	• Complexity and resource consumption.

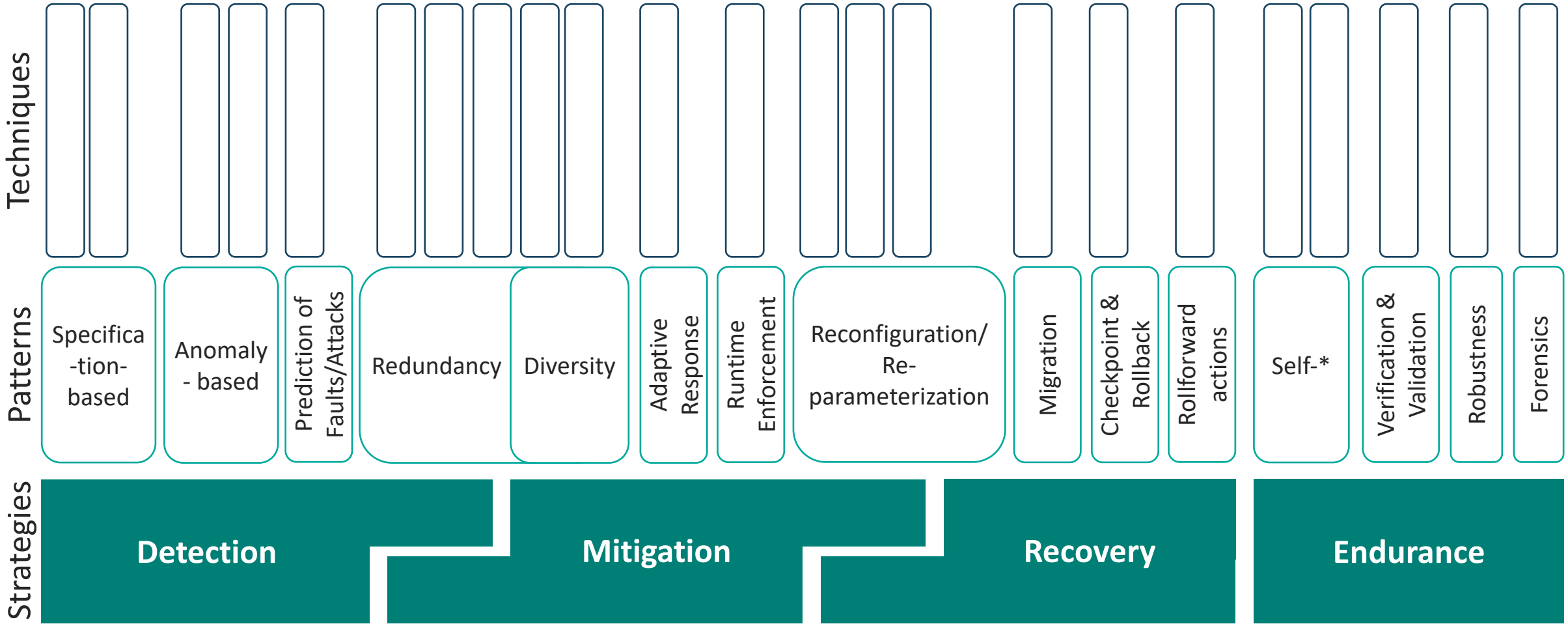
Asset	Attack
Software	Malware/Manipulated Software

Guidelines to show how these techniques can be combined

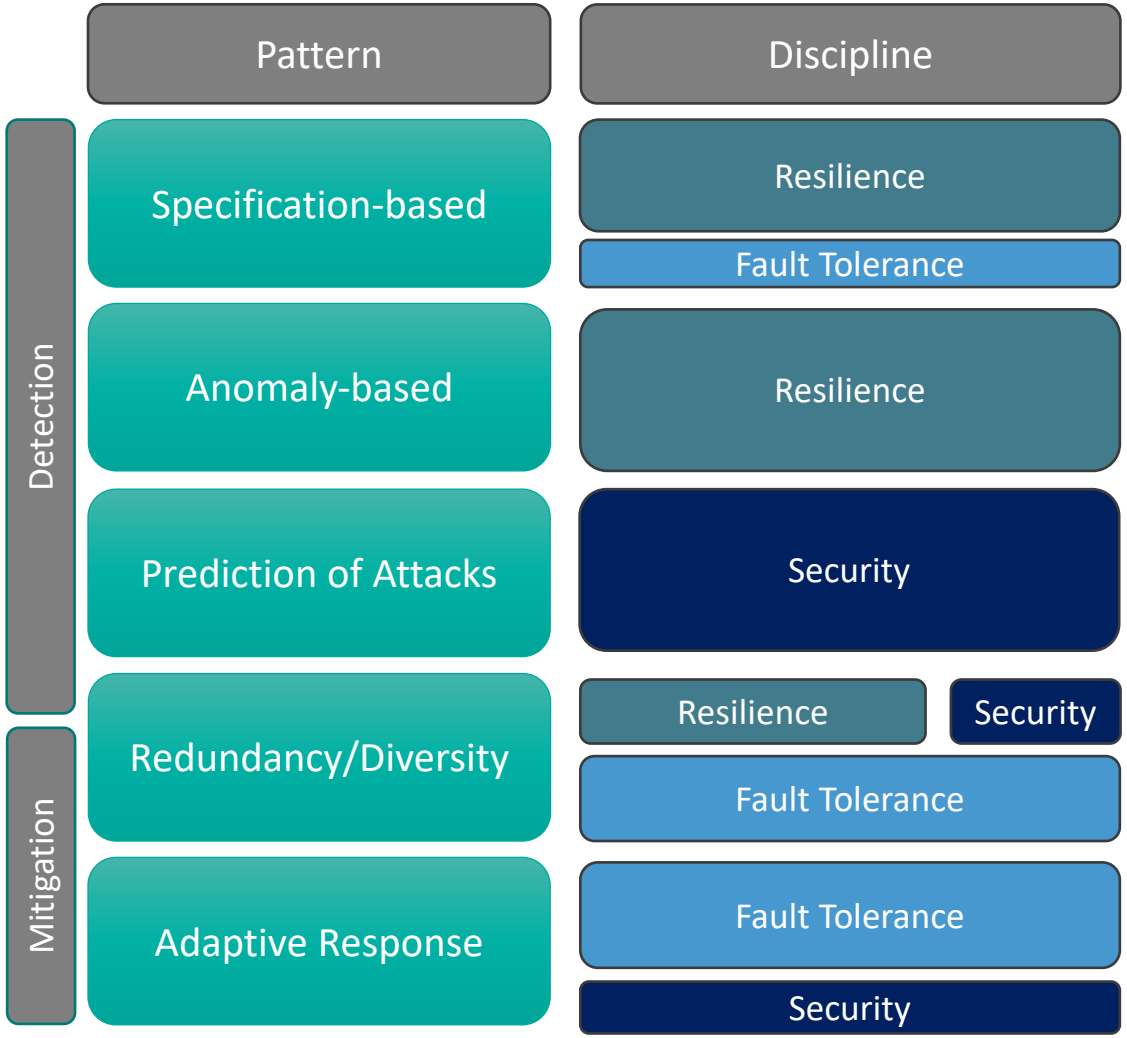
Disciplines of the selected publications

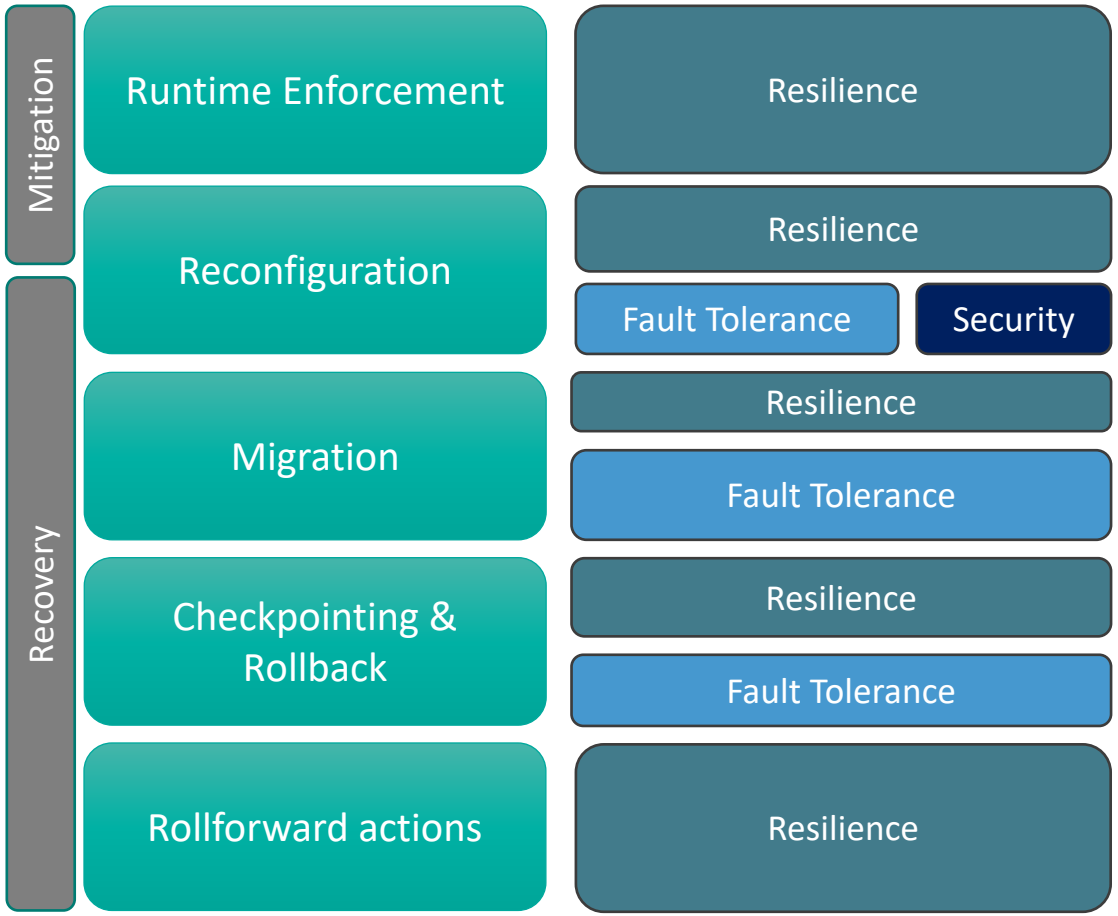


Taxonomy



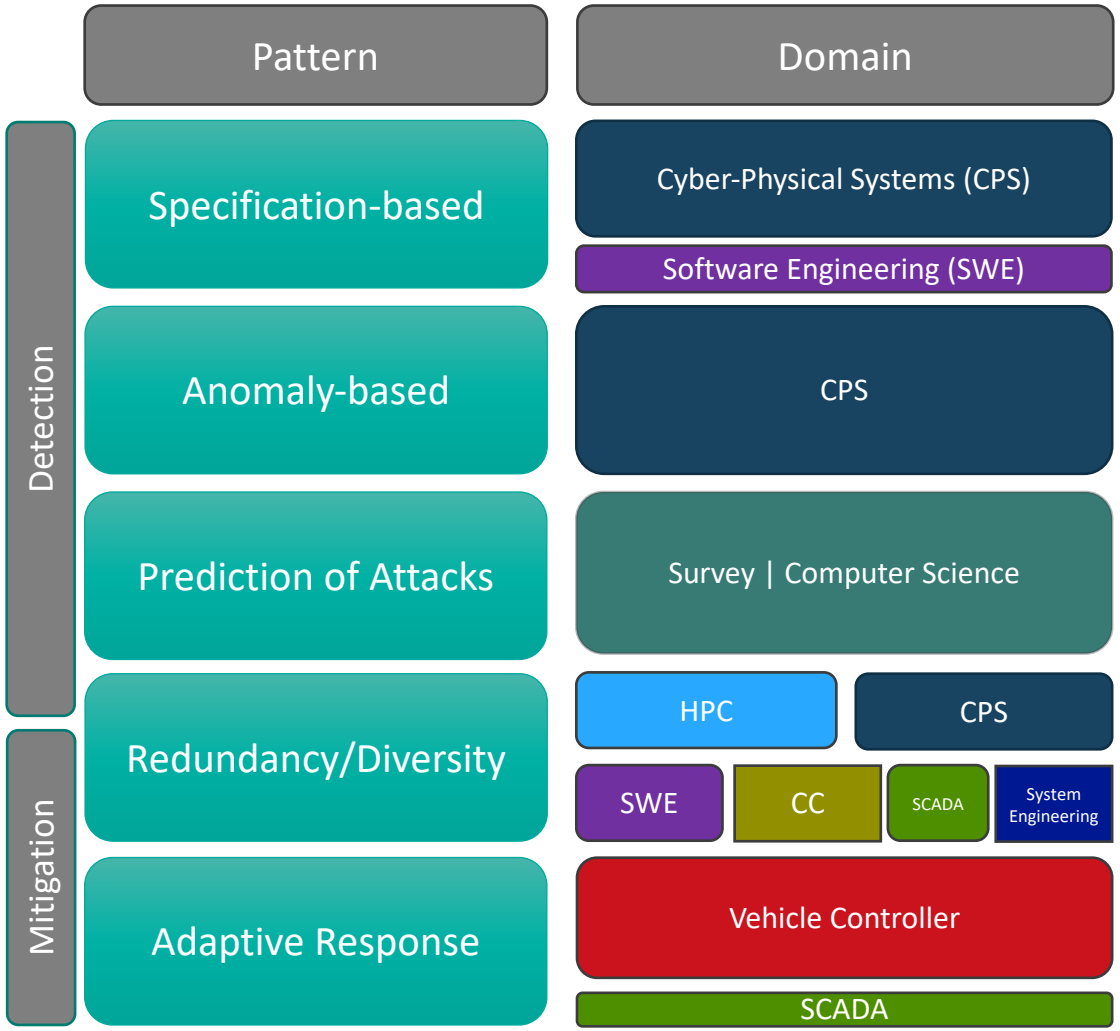
Disciplines of existing work identifying relevant techniques

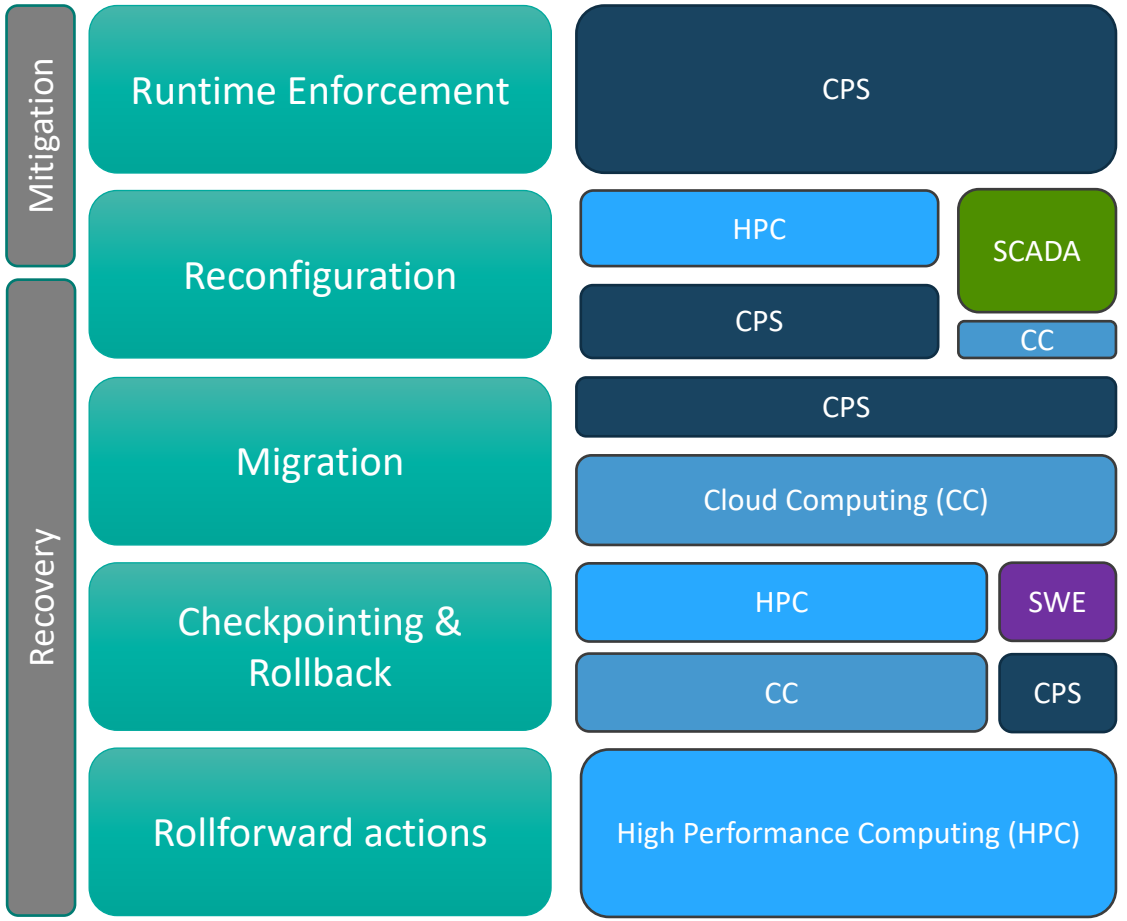




* Not all identified patterns are shown.

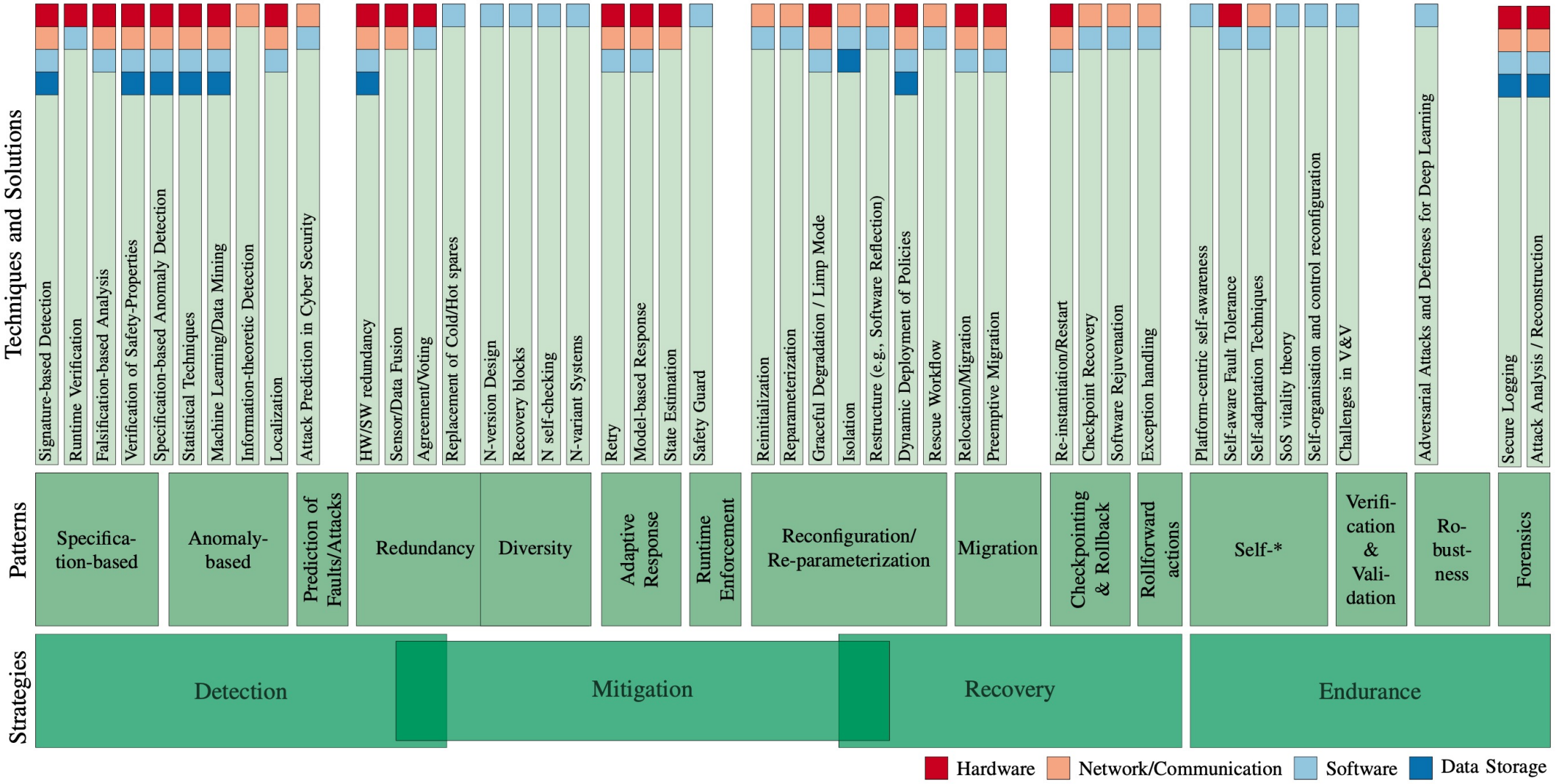
Domains of existing work identifying relevant techniques





* Not all identified patterns are shown.

REMIND Resilience Techniques



REMIND: A Framework for the Resilient Design of Automotive Systems

→ Lead designers to the informed and optimal selection of resilience techniques to be implemented in an automotive system.

1) Systematically identify resilience techniques proposed in literature
2) Taxonomy comprising of the four strategies: detection, mitigation, recovery, and endurance (REMIND)
3) Associate the identified technqiues to automotive assets
4) Guidelines for using this framework including trade-off discussion

RI. SE
Thomas Rosenstatter, Researcher, RISE
thomas.rosenstatter@ri.se

Publications providing an overview or a collection of relevant techniques

Discipline	Existing Work	Domain
Resilience	[Chang2015]	Cloud Computing
	[Hukerikar2017]	High Performance Computing
	[NIST 800-160v2]	Systems Engineering
	[Ratasich 2019]	Cyber-Physical Systems
	[Sterbenz 2010]	Networks
Security	[Segovia2019]	SCADA Systems
Dependability	[Bakhshi2019]	Fog Computing
Fault Tolerance	[Egwutuoha2013]	High Performance Computing
	[Kumari2018]	Cloud Computing
	[Mukwevho2018]	Cloud Computing
	[Slåtten2013]	Software Engineering
	[Wanner2012]	Vehicle Controller

References

[Chang2015] Victor Chang, Muthu Ramachandran, Yulin Yao, Yen-Hung Kuo, and Chung-Sheng Li. A resiliency framework for an enterprise cloud. International Journal of Information Management, 36(1):155 – 166, 2016.

[Hukerikar2017] Saurabh Hukerikar and Christian Engelmann. Resilience design patterns: A structured approach to resilience at extreme scale. arXiv preprint arXiv:1708.07422, 2017.

[NIST 800-160v2] Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid. Developing cyber resilient systems:: a systems security engineering approach. Technical Report NIST SP 800-160v2, National Institute of Standards and Technology, Gaithersburg, MD, November 2019.

[Ratasich2019] Denise Ratasich, Faiq Khalid, Florian Geissler, Radu Grosu, Muhammad Shafique, and Ezio Bartocci. A Roadmap Toward the Resilient Internet of Things for Cyber-Physical Systems. IEEE Access, 7:13260–13283, 2019.

[Sterbenz2010] James PG Sterbenz, David Hutchison, Egemen K. Cetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Schöller, and Paul Smith. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks, 54(8):1245 – 1265, 2010. Resilient and Survivable networks.

[Sterbenz2014] James PG Sterbenz, David Hutchison, Egemen K. Cetinkaya, Abdul Jabbar, Justin P Rohrer, Marcus Schöller, and Paul Smith. Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance invited paper. Telecommunication Systems, 56(1):17–31, 2014.

References

[Segovia2019] Mariana Segovia, Ana Rosa Cavalli, Nora Cuppens, and Joaquin Garcia- Alfaro. A study on mitigation techniques for scada-driven cyber-physical systems (position paper). In Nur Zincir-Heywood, Guillaume Bonfante, Mourad Debbabi, and Joaquin Garcia-Alfaro, editors, Foundations and Practice of Security, pages 257–264, Cham, 2019. Springer International Publishing.

[Bakhshi2019] Zeinab Bakhshi, Guillermo Rodriguez-Navas, and Hans Hansson. De- pendable Fog Computing: A Systematic Literature Review. In 2019 45th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), pages 395–403, 2019.

[Egwutuoha2013] Ifeanyi P Egwutuoha, David Levy, Bran Selic, and Shiping Chen. A survey of fault tolerance mechanisms and checkpoint/restart imple- mentations for high performance computing systems. The Journal of Supercomputing, 65(3):1302–1326, 2013.

[Kumari2018] Priti Kumari and Parmeet Kaur. A survey of fault tolerance in cloud computing. Journal of King Saud University - Computer and Information Sciences, 2018.

[Mukwevho2018] Mukosi A. Mukwevho and Turgay Celik. Toward a smart cloud: A review of fault-tolerance methods in cloud systems. IEEE Transactions on Services Computing, pages 1–1, 2018.

[Slåtten2013] Vidar Slåtten, Peter Herrmann, and Frank Alexander Kraemer. Chapter 4 - model-driven engineering of reliable fault-tolerant systems—a state- of-the-art survey. In Atif Memon, editor, Advances in Computers, volume 91 of Advances in Computers, pages 119 – 205. Elsevier, 2013.

[Wanner2012] Daniel Wanner, Annika Trigell, Lars Drugge, and Jenny Jerrelind. Survey on fault-tolerant vehicle design. World Electric Vehicle Journal, 5(2):598–609, Jun 2012.