MOBILITETSFORUM 09/11

Self-adaptation to withstand cyber attacks

Thomas Rosenstatter
thomas.rosenstatter@ri.se

Behrooz Sangchoolie

Pierre Kleberger

Self-Adaptation

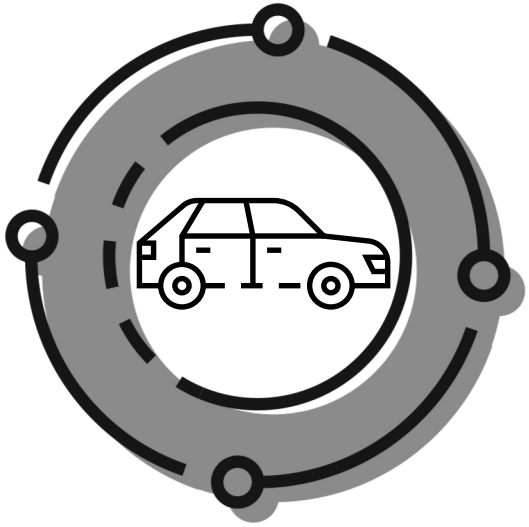
*Self-adaptation in a system is the capability to adapt to internal and external changes to maintain specific quality goals.**

Cyber Resilience

"The 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]

*Summary of various definitions found in publications [1] Definition from CyReV (phase 1) and used in T. Rosenstatter, K. Strandberg, R. Jolak, R. Scandariato and T. Olovsson, "REMIND: A Framework for the Resilient Design of Automotive Systems," *2020 IEEE Secure Development (SecDev)*, 2020, pp. 81-95.

Challenges



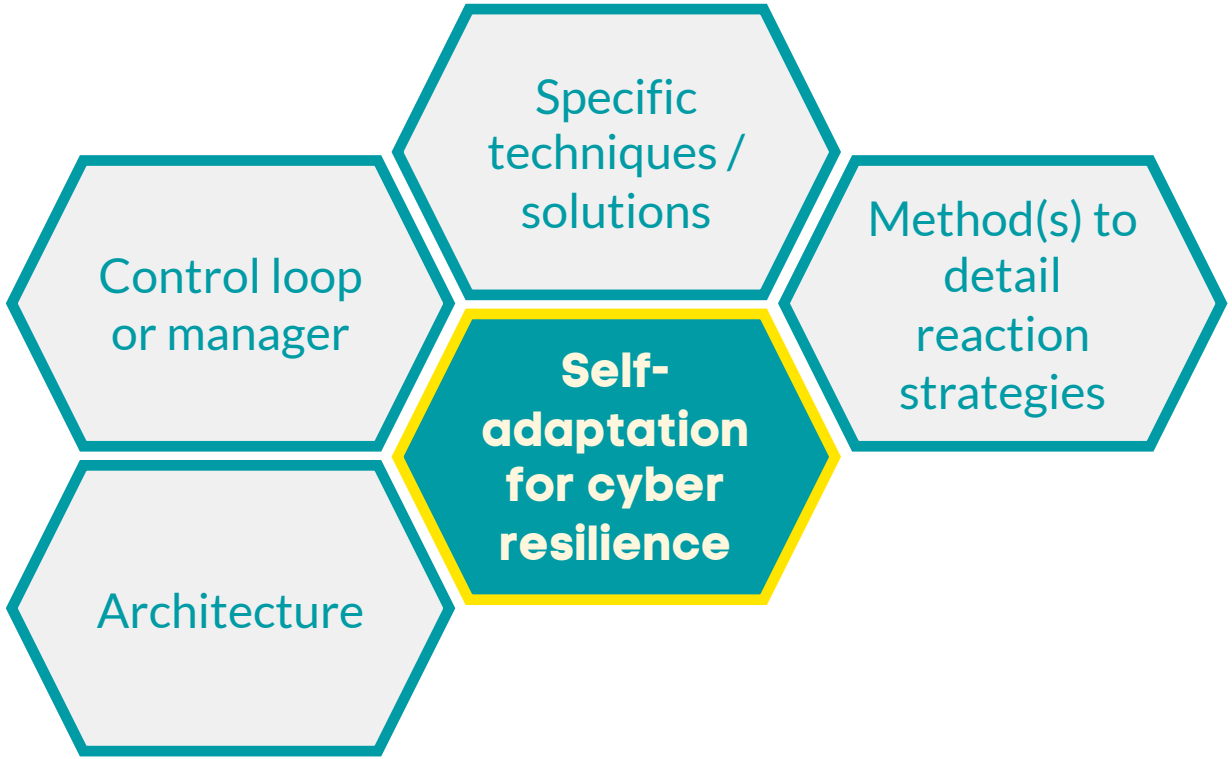
C.1 Safety restrictions

C.2 Support for self-adaptation

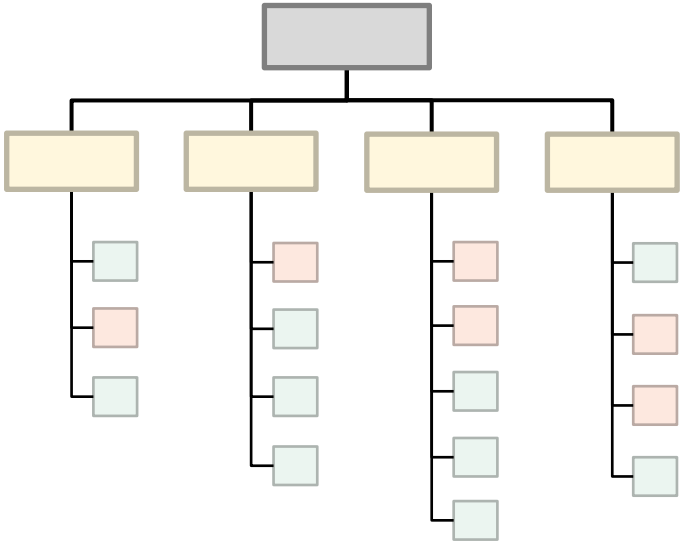
C.3 Identification of security control parameters.

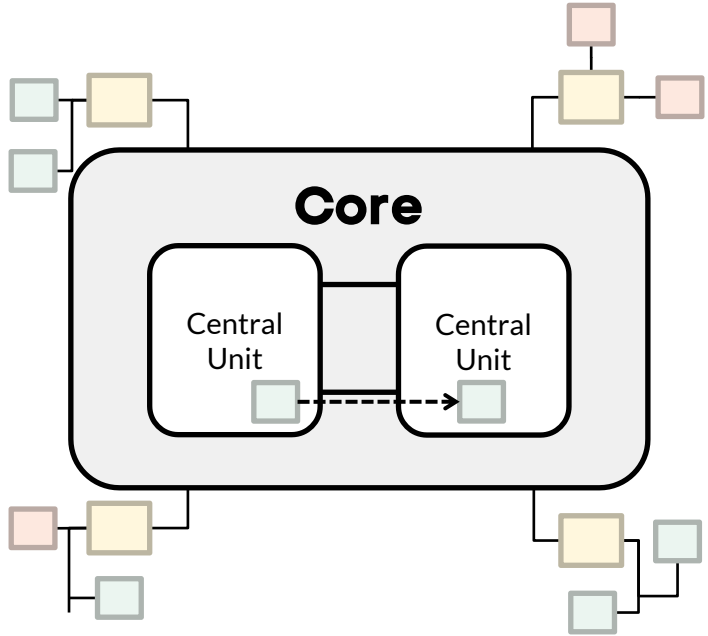
C.4 How to adapt and configure the techniques?

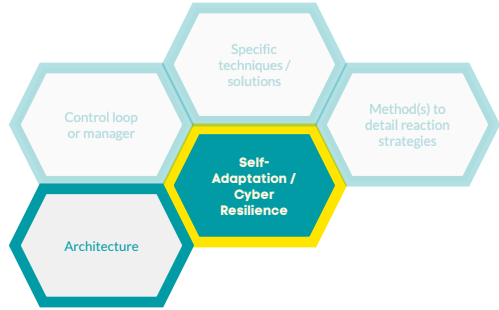
What are the puzzle bits for self-adaptation in vehicles?



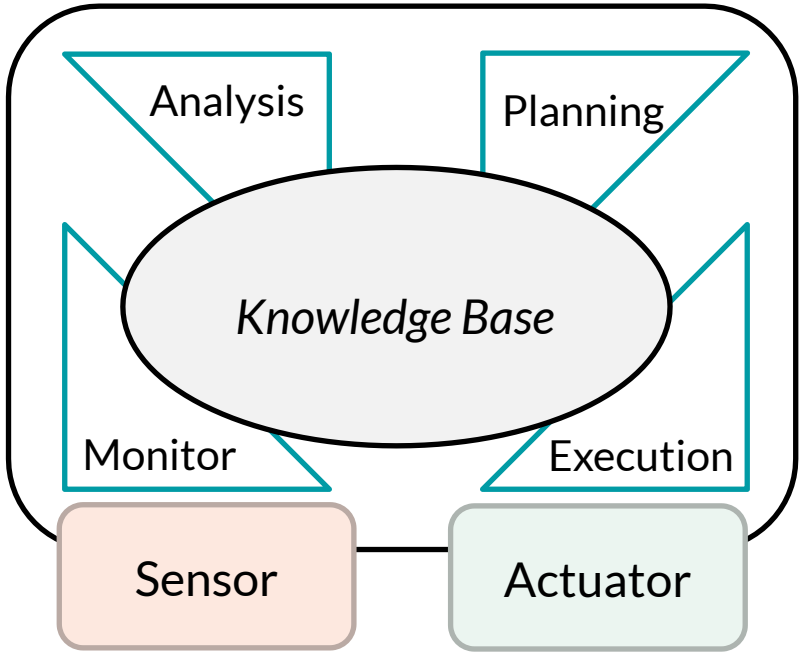
Architecture



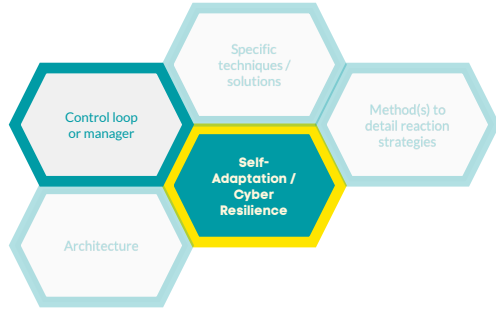




Control loop / manager

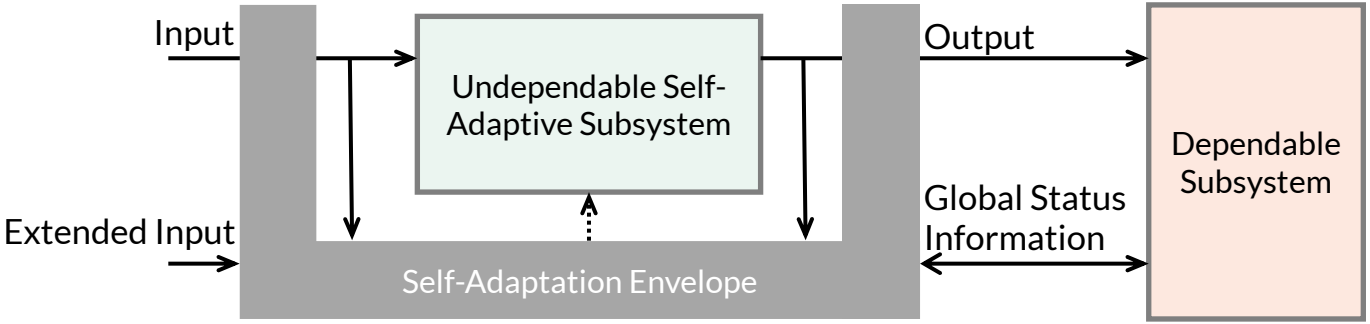


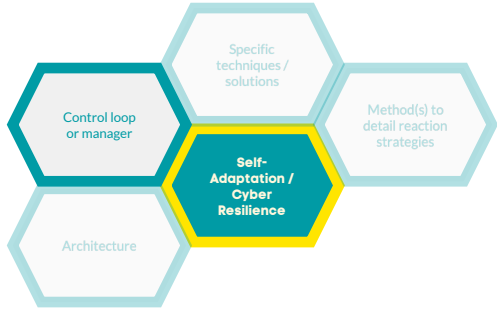
MAPE-K[3]



[3]J. O. Kephart and D. M. Chess, "The vision of autonomic computing," in Computer, vol. 36, no. 1, pp. 41-50, Jan. 2003, doi: 10.1109/MC.2003.1160055.

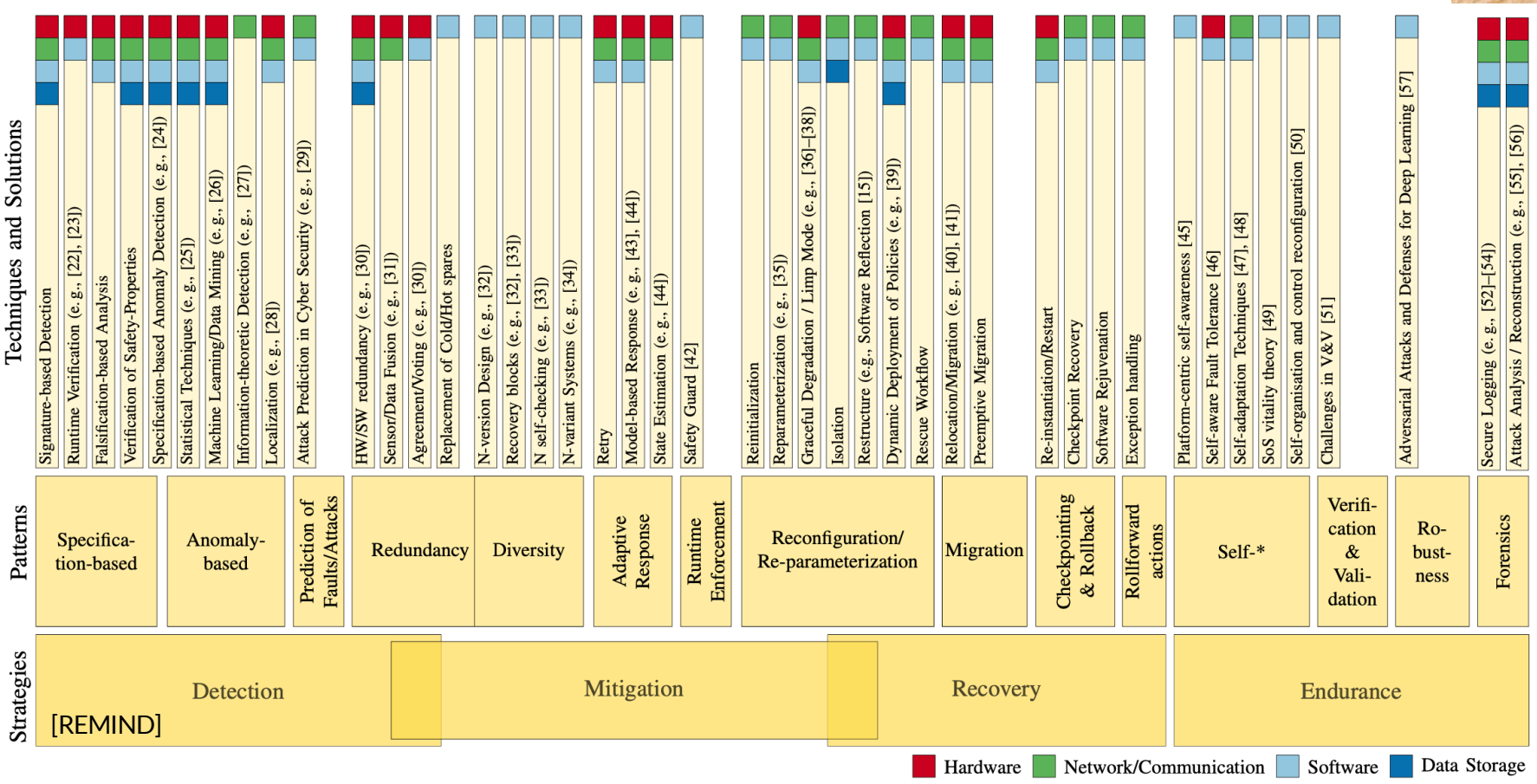
Control of dependable systems





[4]G. Weiss, P. Schleiss, D. Schneider, and M. Trapp. 2018. Towards integrating undependable self-adaptive systems in safety-critical environments. In Proceedings of the 13th International Conference on Software Engineering for Adaptive and Self-Managing Systems (SEAMS '18). Association for Computing Machinery, New York, NY, USA, 26–32.

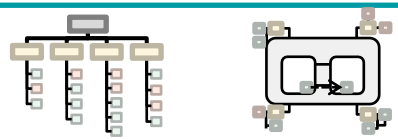
Specific techniques/solutions



[REMIND]

Techniques and Solutions
Patterns
Strategies
Specification-based Anomaly Detection
Agreement/Voting
Reinitialisation
Graceful Degradation
Relocation/Migration
How to piece everything together and configure them?
Signature-based Detection
Runtime Verification (e. g., [22], [23])
Verification of Safety-Properties
Information-theoretic Detection (e. g., [27])
Localization (e. g., [28])
Attack Prediction in Cyber Security (e. g., [29])
HW/SW redundancy (e. g., [30])
Sensor/Data Fusion (e. g., [31])
N-version Design (e. g., [32])
Recovery blocks (e. g., [32], [33])
N self-checking (e. g., [33])
N-variant Systems (e. g., [34])
Retry
Model-based Response (e. g., [43], [44])
State Estimation (e. g., [44])
Safety Guard [42]
Graceful Degradation / Limp Mode (e. g., [36]–[38])
Dynamic Deployment of Policies (e. g., [39])
Preemptive Migration
Re-instantiation/Res
Checkpoint Reco
Software Rejuve
Exception hand
Platform-cent
Self-aware F
Self-adaptati
SoS vitality
Self-organisa
Challenges in
Adversarial Atta
Learning [57]
Secure Logging (e. g., [52]
Attack Analysis / Reconstruction (e. g., [55], [56])
Specifica-tion-based
Anomaly-based
Prediction of Faults/Attacks
Redundancy
Diversity
Adaptive Response
Runtime Enforcement
Reconfiguration/ Re-parameterization
Migration
Checkpointing & Rollback
Rollforward actions
Self-*
Verifi-cation & Vali-dation
Ro-bust-ness
Forensics
Detection
Mitigation
Recovery
Endurance
Hardware
Network/Communication
Software
Data Storage

Decision framework for detailing reaction strategies

- Architecture 
- Granularity 
- Required resources 
- Evaluation of the technique 
- Duration of effectiveness **short-term / long-term**
- STRIDE threats 
- Time to adapt 
- ...

MOBILITETSFORUM 09/11

Self-adaptation to withstand cyber attacks

Thomas Rosenstatter
thomas.rosenstatter@ri.se

Behrooz Sangchoolie

Pierre Kleberger

RI.SE