Projects Overview

TUM Chair of IT Security

Computer Science Department

Huang Xiao (I20)

xiao@sec.in.tum.de

Overview

- BMBF Project: ARAMiS
- Anomaly Detection with Machine Learning

ARAMiS

AUTOMOTIVE · RAILWAY · AVIONICS MULTICORE SYSTEMS aramis

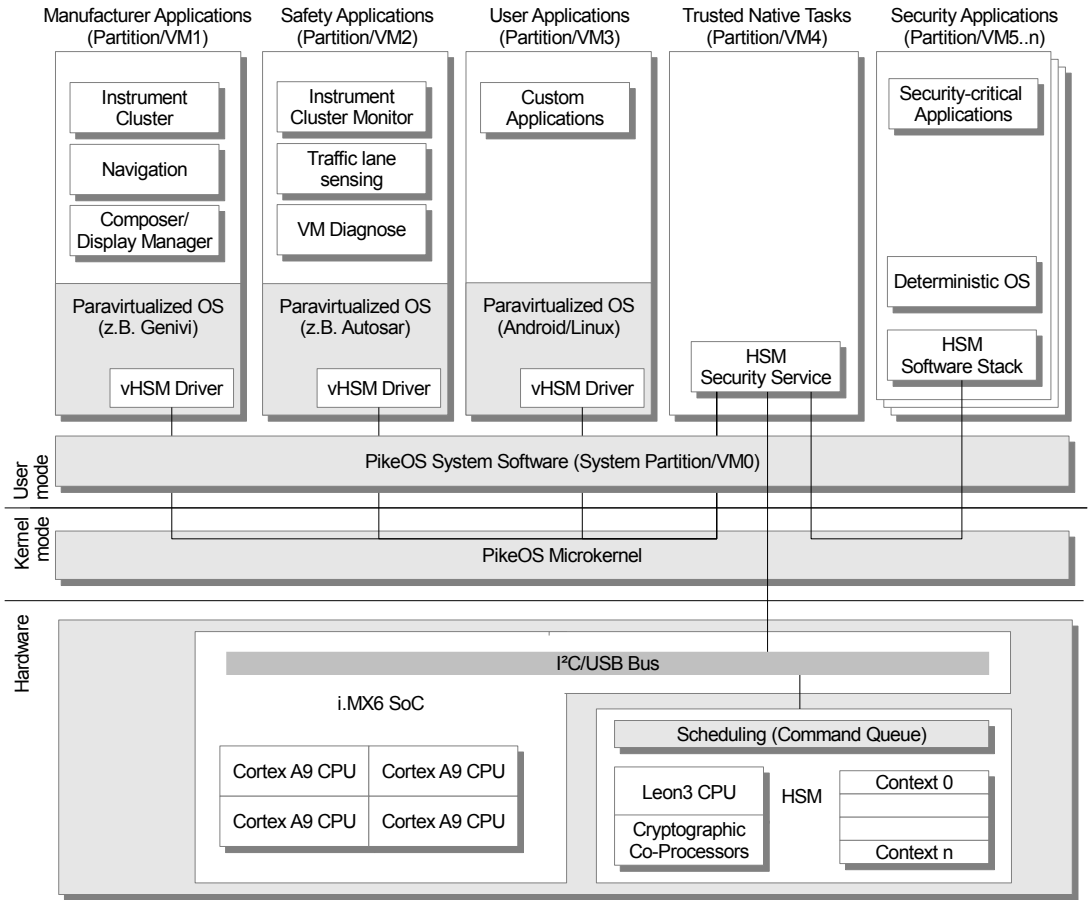
- **ARAMiS** stands for Automotive, Railway and Avionics Multicore Systems.
- **Goal**: *Multicore adaption of current existing embedded systems to increase system security, safety and efficiency in automotive, railway and avionics domains.*
- **Importance**: Fundament of networking embedded systems and Cyber Physical Systems.
- **Funded** by BMBF for three years.
- **Project consortium** includes the most influential partners in both industry and academy. E.g., BMW, EADS, Siemens, Infienon, TUM, Fraunhofer (32 Partners overall)
- **Results**: Realization of MC-OS (Multicore Operating System) for various mobility domains, project documents, Scientific publications, books, articles, organization of speicial sessions (e.g., workshops).
- TUM Chair of IT Security: Security components in ARAMiS MC-OS.

ARAMiS (Cont.)

AUTOMOTIVE · RAILWAY · AVIONICS MULTICORE SYSTEMS

aramis

System architecture (via PikeOS)



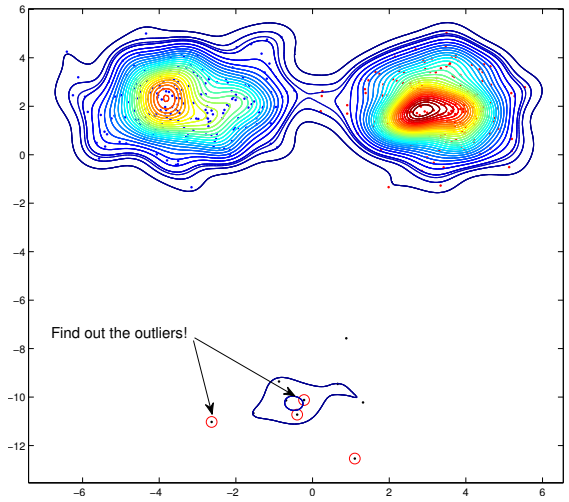
TUM INSEC OBJECTIVES

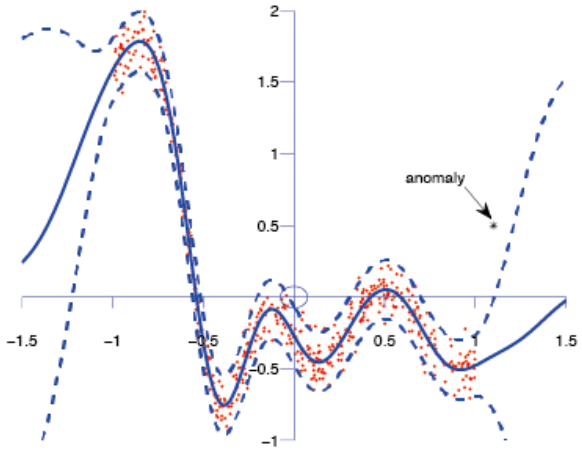
- SECURITY ARCHITECTURE
  - HW/SW security partitioning
  - Algorithms and protocols
  - Hypervisor functions
  - Threat analysis
- SOFTWARE
  - System architecture for MC-OS
  - Development of security monitor
  - Verification and test of system
- DEMOSTRATOR
  - High integration demonstration on BMW automotive platform.

Anomaly Detection

Machine learning based anomaly detection

- Classification based
  - Neural networks, Bayesian networks, SVMs[1]
- Nearest neighbor based
  - K[th] nearest neighbor, relative density
- Clustering based
  - EM[2] algorithm, Local outlier factor
- Statistical anomaly detection
  - Gaussian model based, regression model, kernel function based
- Information theoretic based
  - Geometric entropy minimization (GEM)
- Spectral based
  - Compact matrix decomposition, robust PCA



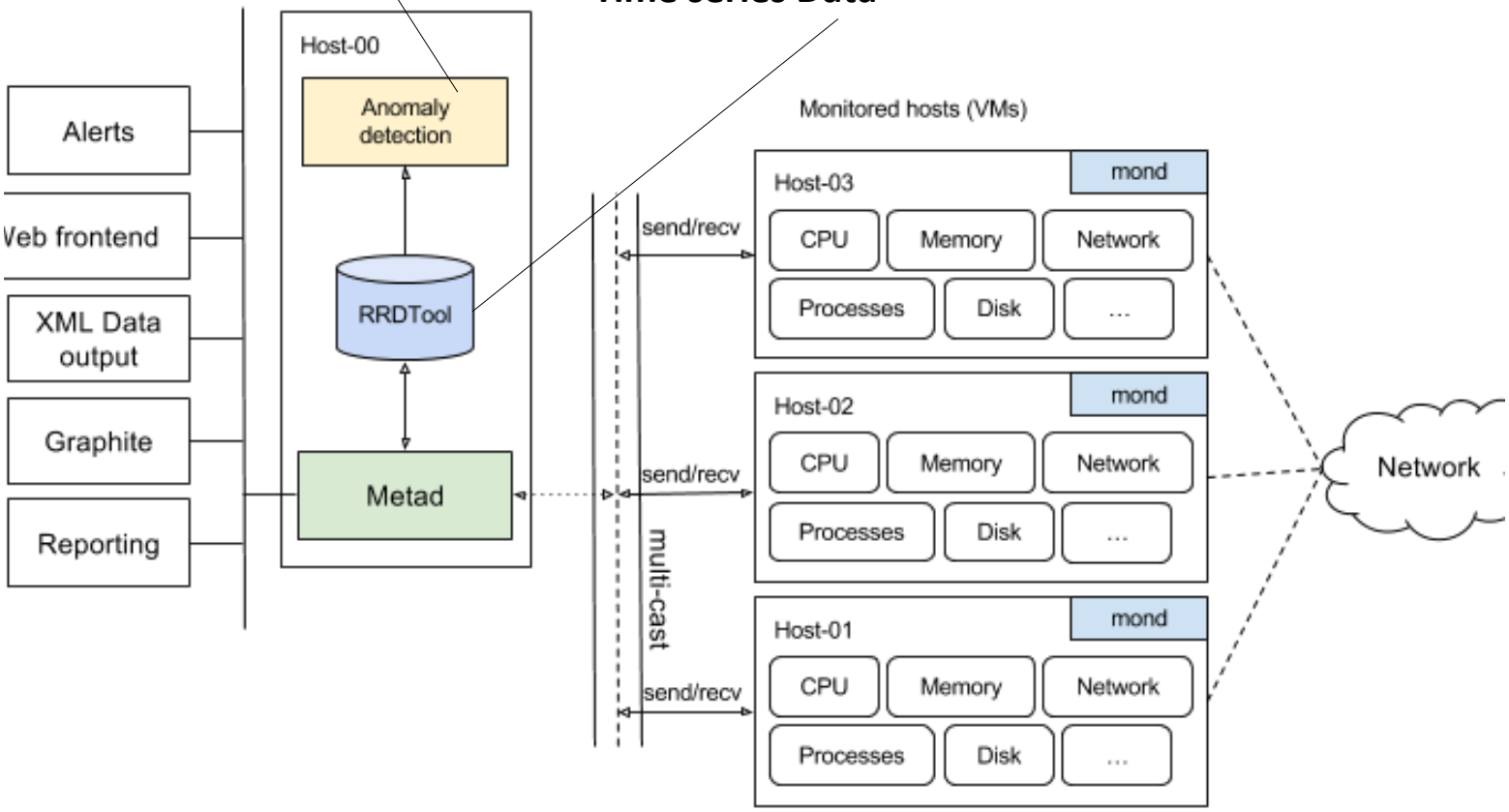


Smart Security Monitor (Architecture)

Embedded anomaly detection module

Catch the anomalies in real time!

NoDatabase: RoundRobinTools for Time series Data



Anomaly Detection (Cont.)

Selected publications

Xiao, Huang, and Claudia Eckert. **Indicative Support Vector Clustering with its Application on Anomaly Detection**. In IEEE 12th International Conference on Machine Learning and Applications (ICMLA'13), Miami, Florida, December 2013

Xiao, Han, Huang Xiao, and Claudia Eckert. **Learning from Multiple Observers with Unknown Expertise**. In Proceedings of 17th Pacific-Asia Conference on Knowledge Discovery and Data Mining, Gold Coast, Australia, April 2013. Springer.

Xiao, Huang, Han Xiao, and Claudia Eckert. **OPARS: Objective Photo Aesthetics Ranking System**. In 34th European Conference on Information Retrieval (ECIR'13), Moscow, Russia, March 2013

Xiao, Han, Huang Xiao, and Claudia Eckert. **Adversarial Label Flips Attack on Support Vector Machines**. In 20th European Conference on Artificial Intelligence (ECAI), Montepellier, France, August 2012.