



eSecurity

Attackers / Threats / Risk Analysis
(A2 A3)

Overview

- State of the art
- Current status



State of the art

- ISO27001 / BS7799 / ISO17799
- NIST 800-12 / NIST 800-30



Risk assessment process

- System characterization
- Threat identification
- Vulnerability identification
- Control analysis
- Likelihood determination
- Impact analysis
- Risk determination
- Control recommendation



System characterization

- System architecture and boundaries
- System functions
- System and data criticality
- System and data sensitivity (CIA)
 - Confidentiality
 - Integrity, including
 - authenticity
 - non-repudiation
 - Availability



Threat identification

- Vulnerability:
 - accidentally triggered
 - intentionally exploited
- Threat source:
 - circumstance or event with the potential to cause harm to a system
- Threat likelihood, depends on:
 - thread sources (motivation, resources, capabilities)
 - vulnerabilities
 - existing controls



Threat source categories

- Natural
- Environmental
- Human



Human threat sources (who)

- Hacker
- Computer criminal
- Terrorist
- Industrial espionage
- Insider



Threat source motivation (why)

- Insider:
 - Revenge (terminated employee)
 - Errors or omissions (poorly trained employee)
- Hacker:
 - Challenge
 - Ego
- Computer criminal
 - Monetary gain

Threat source action (what)

- System intrusion
- Unauthorized system access
- Fraud and theft
- System bugs
- System sabotage
- ... and many more



Vulnerability identification

- A vulnerability is a flaw or weakness in aspects of a system that could result in:
 - a security breach
 - a violation of a security policy
- System aspect examples:
 - design
 - implementation
 - procedure
- Vulnerabilities depend on:
 - Phase of life cycle (designed, implemented, operational)
 - Nature of the system
- Finding vulnerabilities:
 - Information sources
 - Checklists
 - Security testing

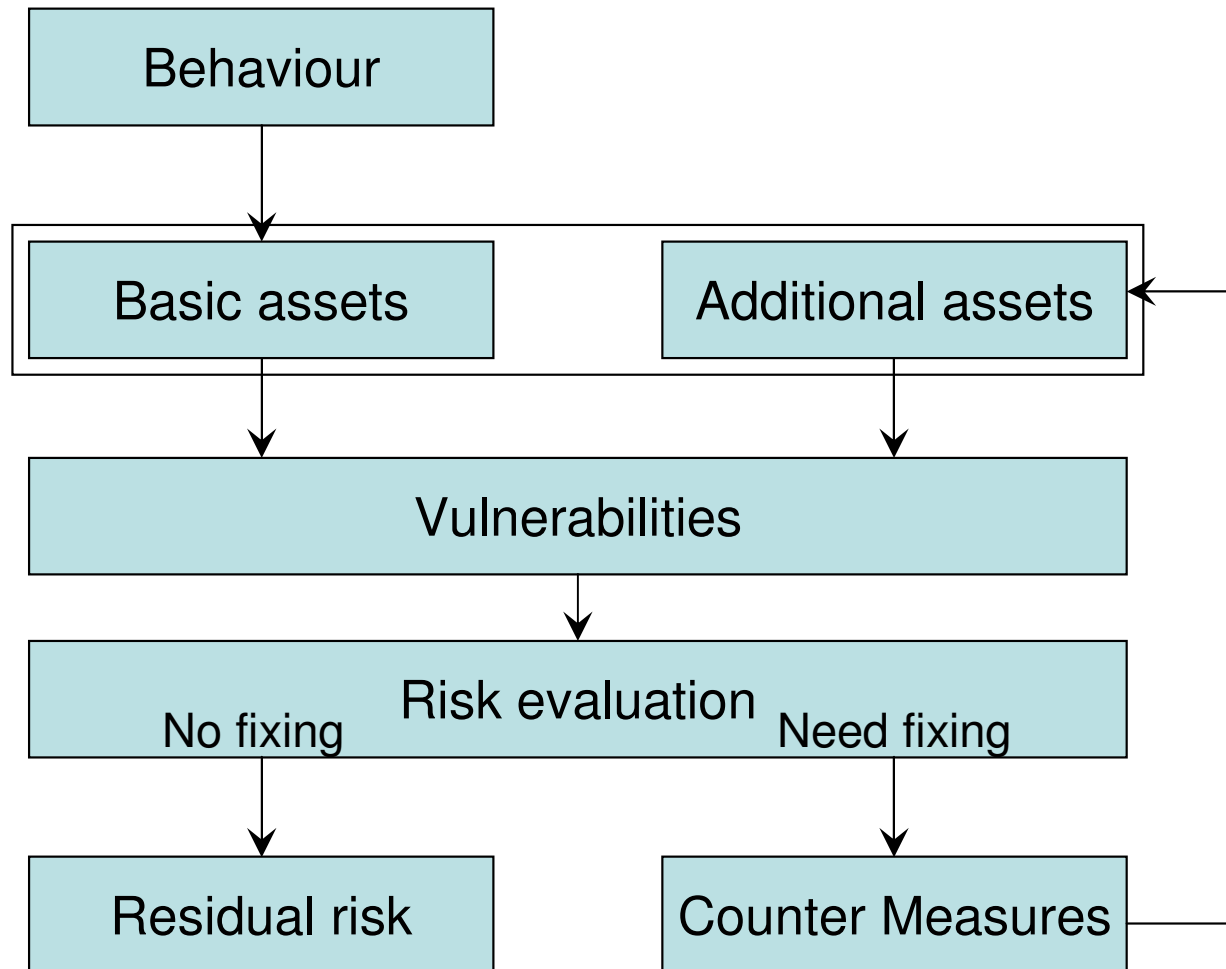


and further steps ...

- Control analysis
 - effectiveness current measures
- Likelihood determination
 - threat sources + vulnerabilities + controls
- Impact analysis
 - damage
- Risk determination
 - likelihood + damage => risk
- Control recommendations
 - cost-effective set of measures



Simplified process



In the context of vehicle related systems ...

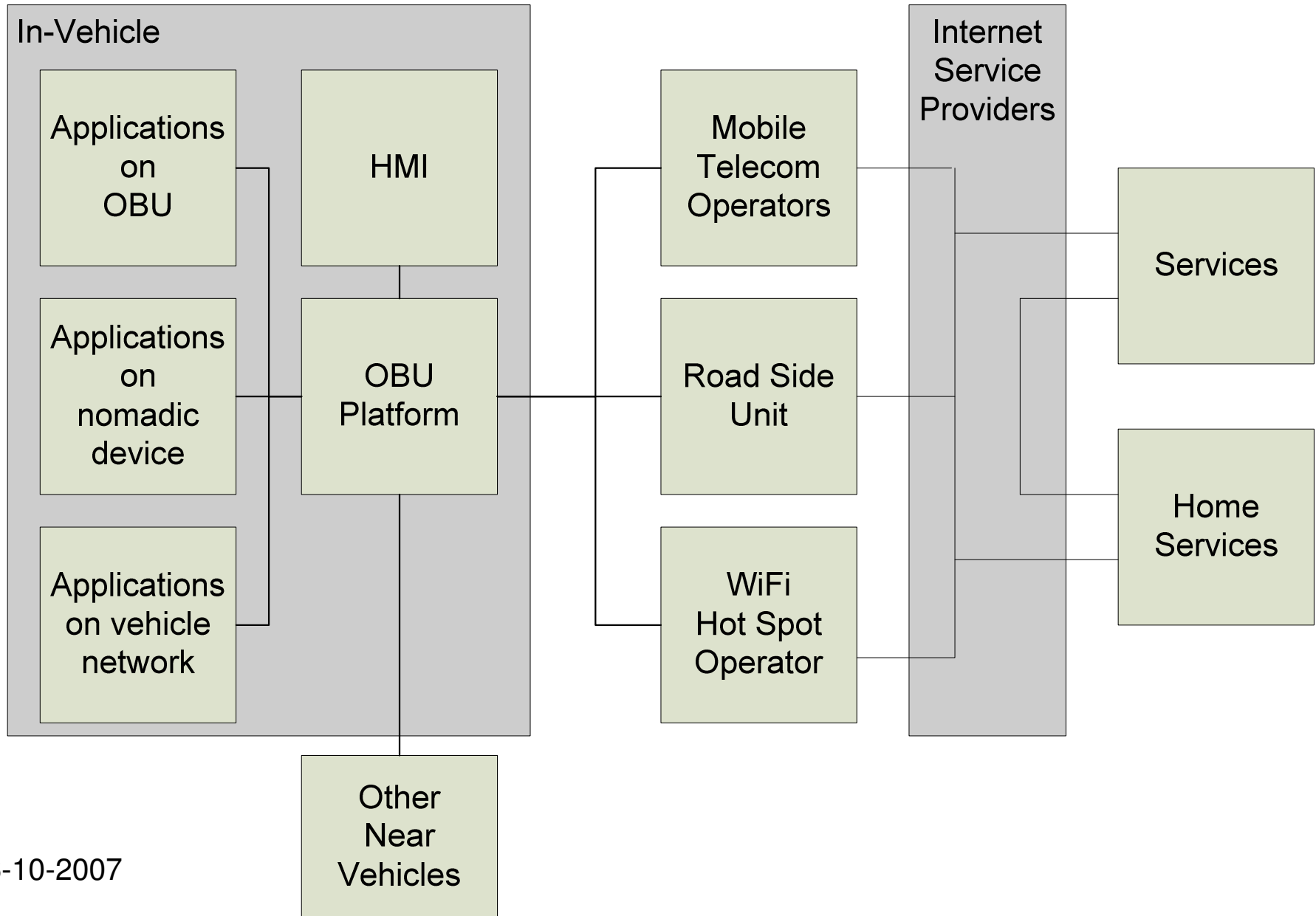


Current effort (A2-A3)

- Generalized system architecture
 - COMeSafety?
 - Current attempt: CVIS / C2C manifesto
- Treats and vulnerabilities
 - ... challenge



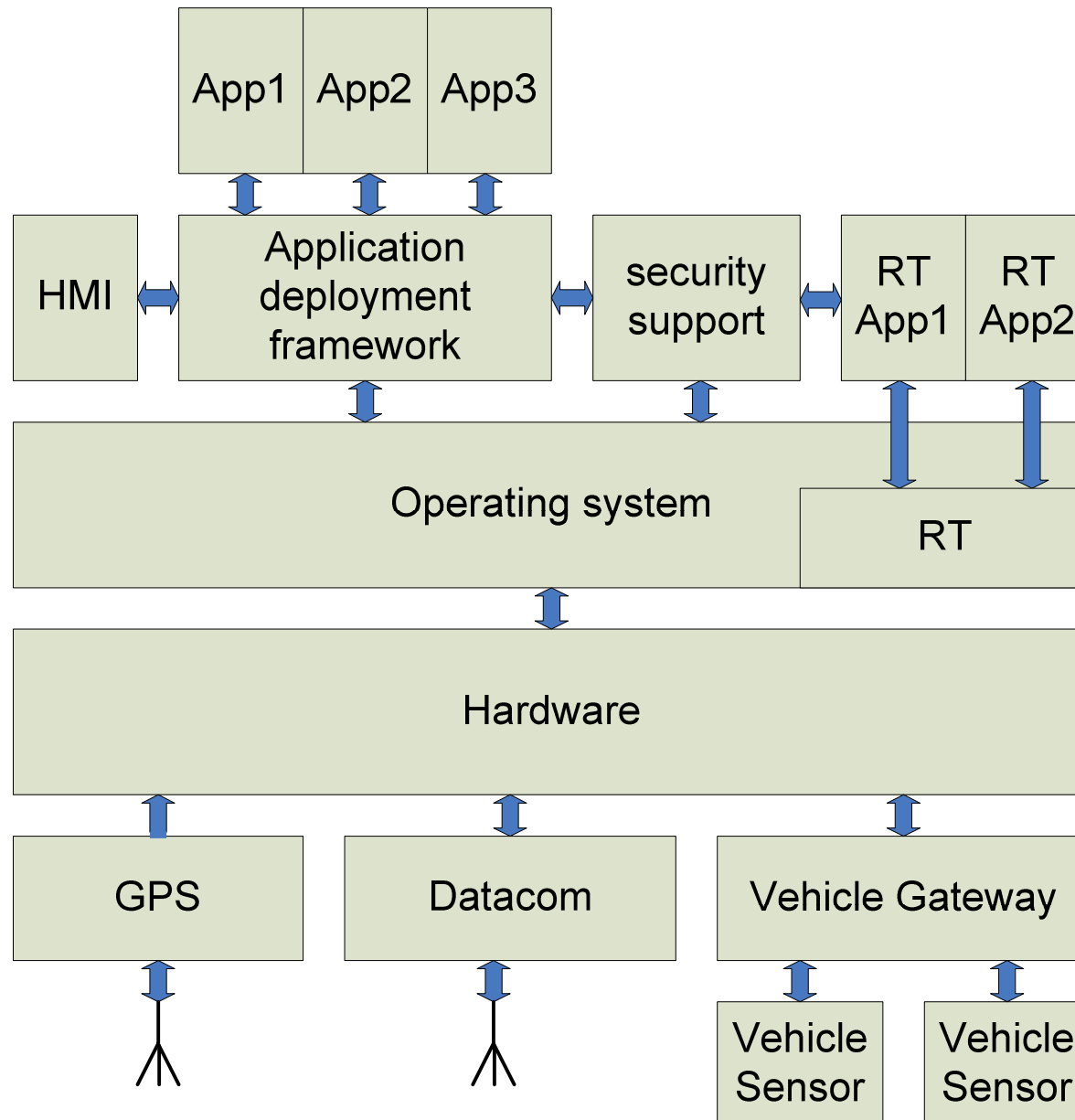
Architecture (system)



16-10-2007



Architecture (OBU HW/SW)



Treats and vulnerabilities

- The generalized architecture is the basis, so it should be validated carefully
- It is not easy to execute a conventional analysis for a generalized architecture
- SECA approach for an functional-level risk analysis (SeveCOM)

Treats and vulnerabilities SECA

The SECA approach:

- Get characteristics of many applications
- Reduce application set
- Application use case with more details
- Attack use cases
- Countermeasure using a security mechanism

Discussion

- System model?
- Approach?
- Goals?

