The increasing complexity of electronic-based, security-related, interconnected embedded systems requires a comprehensive approach for security validation. The project VALSES (Virtual Prototyping zur Validierung der Sicherheit verteilter eingebetteter Systemarchitekturen) takes up this challenge by providing an analysis framework, based on system simulations to assess and analyze security measures throughout the design process of embedded systems.

Virtual prototyping
- Executable simulation model of the system (hardware/software)
- SystemC/C++ based simulation models
- Integration of actual software implementations (host code or binary execution)
- Supporting different abstraction levels throughout the design process
- Consideration of timing
- Simulation library concept to foster the reuse of simulation entities

Envisioned analysis flow
- Comprehensive specification of the system architecture and security measures
- Specification basis to generate virtual prototypes for security analyses
- Support system architecture analysis of structure-related weaknesses
- Support software based analysis based on the hardware/software simulation model
- Support hybrid simulation models

System architecture analysis
- System architecture analysis for structure-related weaknesses
- Data propagation analysis using a taint propagation approach
- Analysis based on control flow, data flow graphs and simulation runs
- Differentiation between security-related and nonsecurity-related information
- Ability to dynamically track sensitive information between sources and sinks
- Information propagation with regard to both hardware and software dependency

Security analysis
- Penetration testing in early stage of the development without physical prototypes
- Revealing implementation weaknesses by means of successful attacks on the executable system model
- Inclusion of real software implementations to detect security flaws based on implementation errors

Modelling approach
- Graphical specification of simulation entities, system structure and security-related information such as potential attack surfaces and protection goals
- UML-based specification with custom profiles
- Specification of documentation-related information such as encryption and handshaking protocols

FZI Forschungszentrum Informatik | Research Division ISPE
Dr. Alexander Viehl | viehl@fzi.de | +49 721 9654-414
For more information www.fzi.de/