Experimental Embedded System Platform for System/Security Co-Design

Matthew Eby, Janos Mathe, Jan Werner, Janos Sztipanovits, Gabor Karsai, Yuan Xue
Institute for Software Integrated Systems - Vanderbilt University

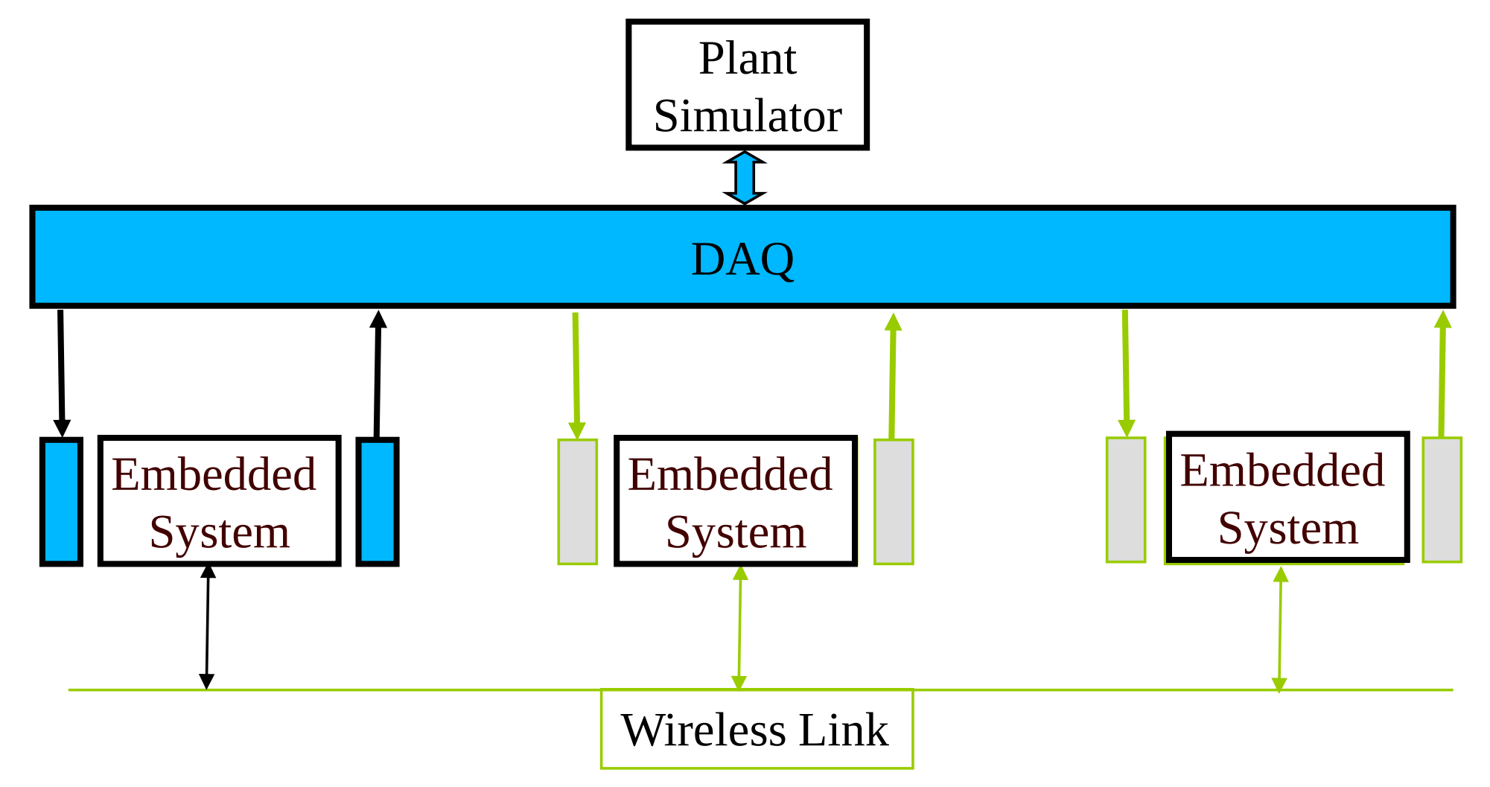
Testbed platform

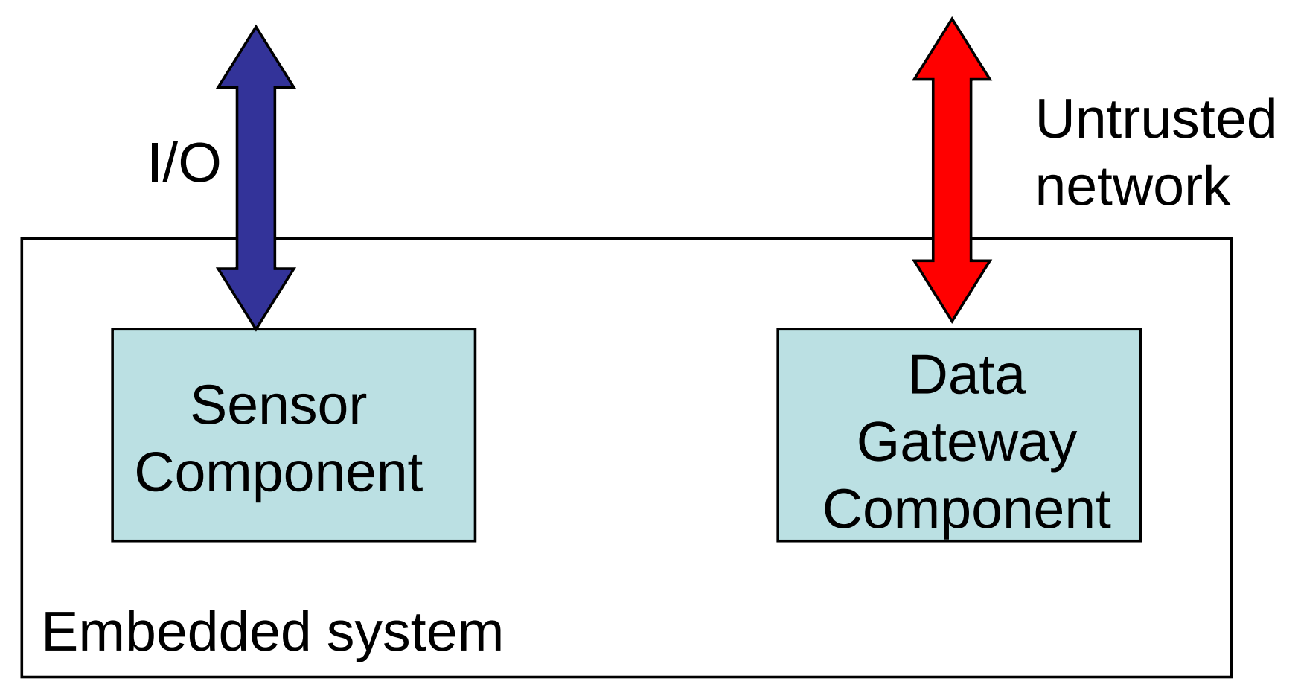
Single board computer SBC 4495 from MicroSys

Cyrix i486 compatible
64MB of RAM
14 bit A/D & D/A
24 I/O lines
Ethernet adapter
PCMCIA card slot
External storage on hard drive or compact flash card

Operating System

GNU/Linux
Gentoo 2005.1 with modified 2.4.32 kernel
GRSecurity kernel patch
No real-time extensions
System with the DCControl application fits on 8MB compact flash card





Security mechanisms and vulnerabilities

Hardware mechanisms

Processor rings

•Memory protection

•Memory access bits

•Partitioning

•Separate bus for code and data – Harvard Architecture

Software mechanisms

Access control

•Partitioning

•Capabilities

•Software based memory access bits

Vulnerabilities

•Design flaws

•Race conditions

•Buffer overflows

•Input validation errors

•Format strings

•Code injection

Exploiting embedded systems

Embedded systems aren't harder to exploit than multipurpose OS's

Useful shellcode doesn't have to yield shell access

Security by obscurity doesn't work out

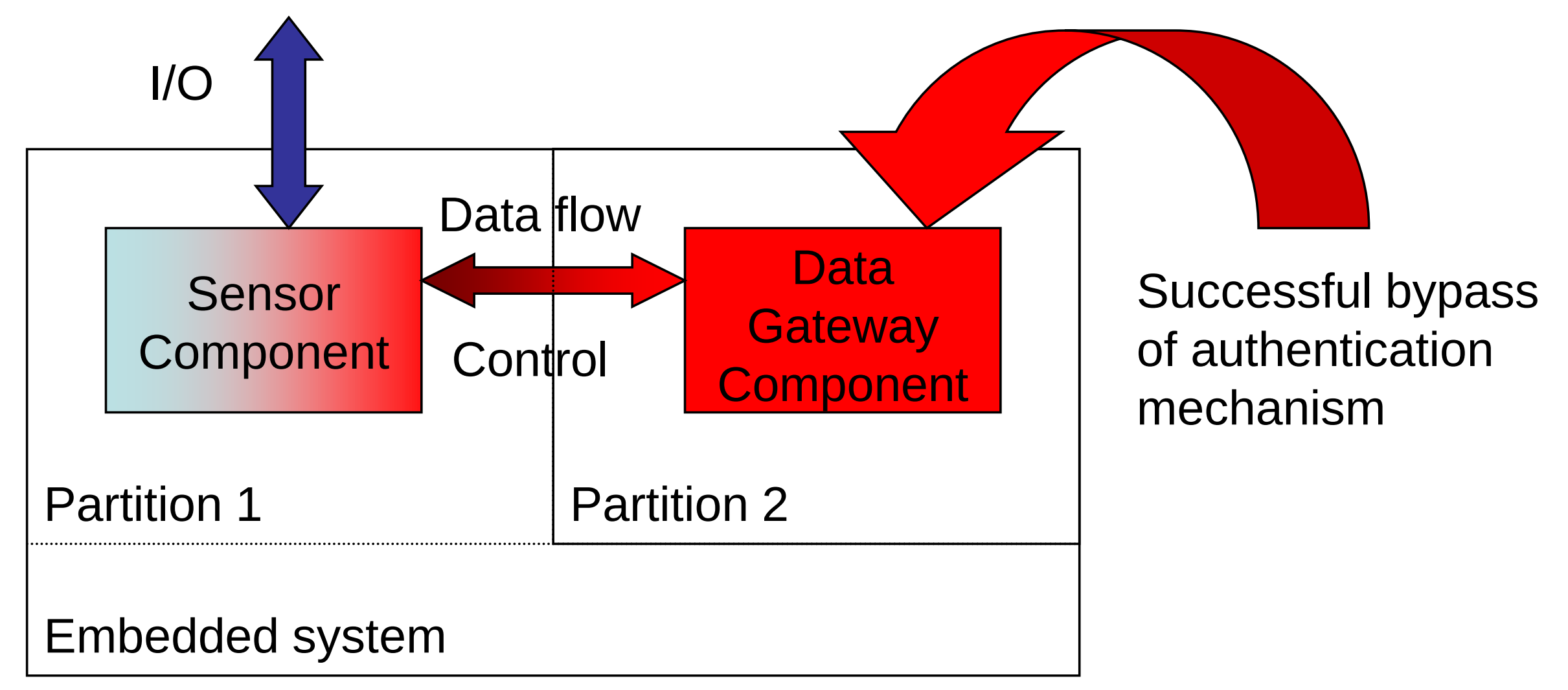
Possible Attack scenarios

Breaking data provider web application

Example web application written in PHP contains a bug which allows accessing restricted areas without authentication

Breaking data provider application

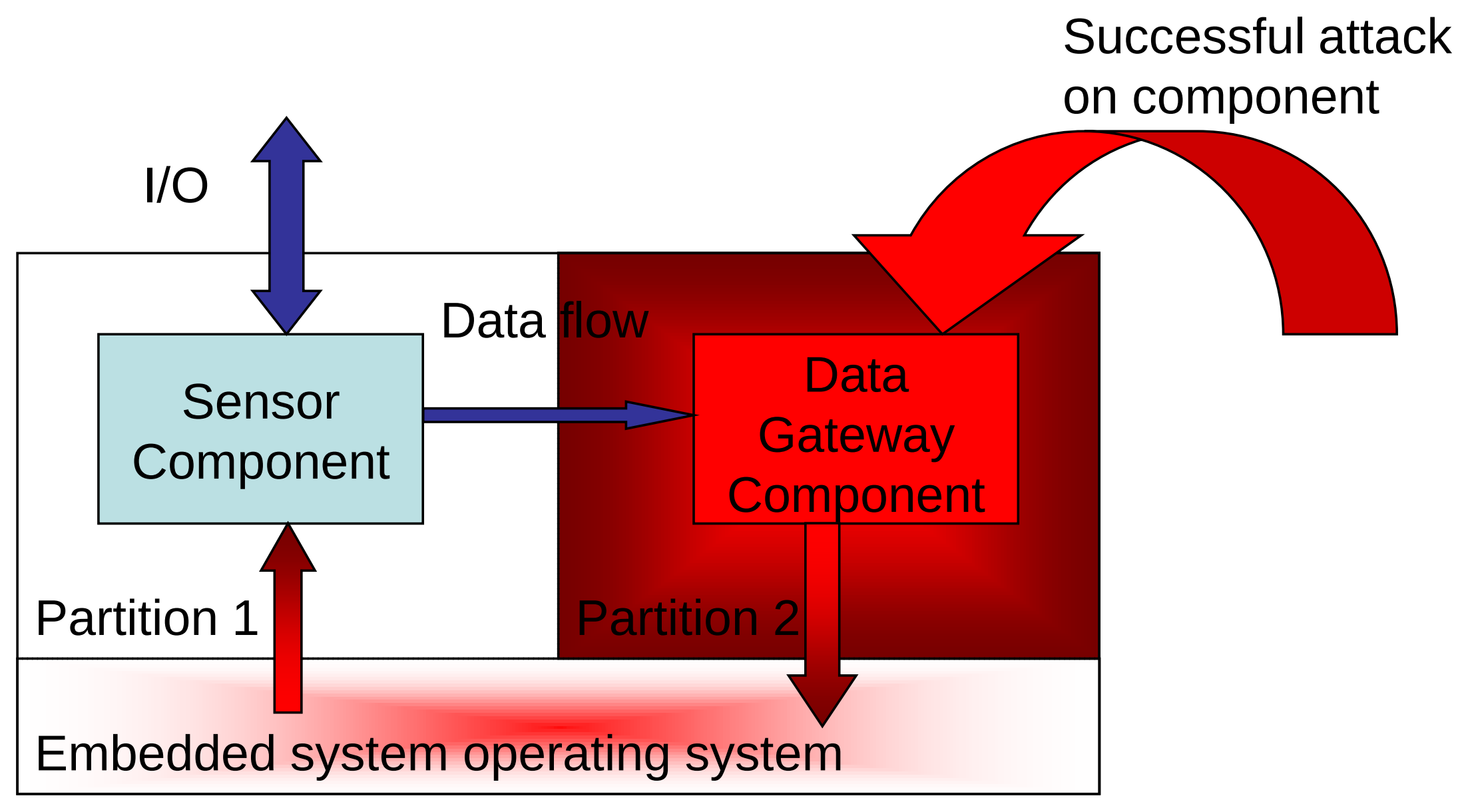
Example TCP/IP application contains a buffer overflow bug which exploited yields access to system



Compromised gateway component is used to change parameters of sensor component

Changing behavior of the sensor component through control link
Gateway component allows authenticated users to change parameters of the sensor component.

Changing behavior of the sensor component through operating system layer
Running sensor component may be affected with modification of configuration files or through some operating systems mechanisms (signals, tracing)



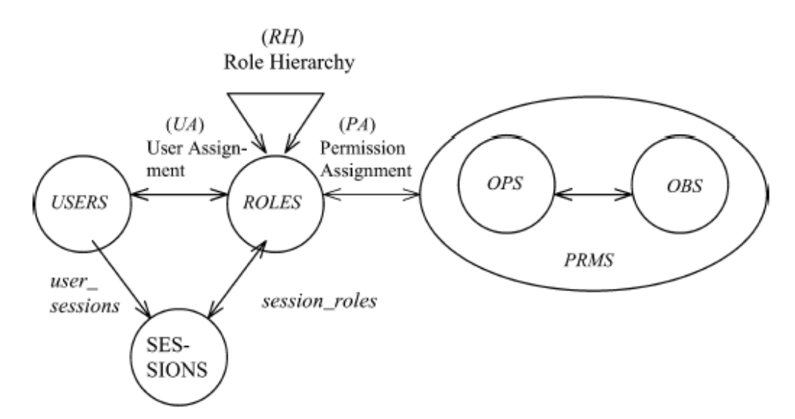
Compromised gateway component is used to change parameters of sensor component using operating system facilities

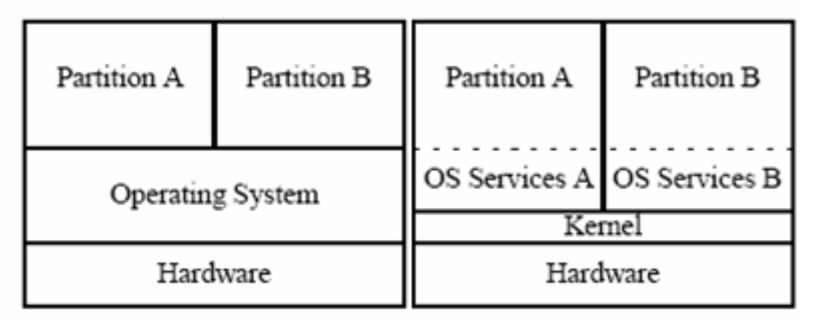
Possible solutions

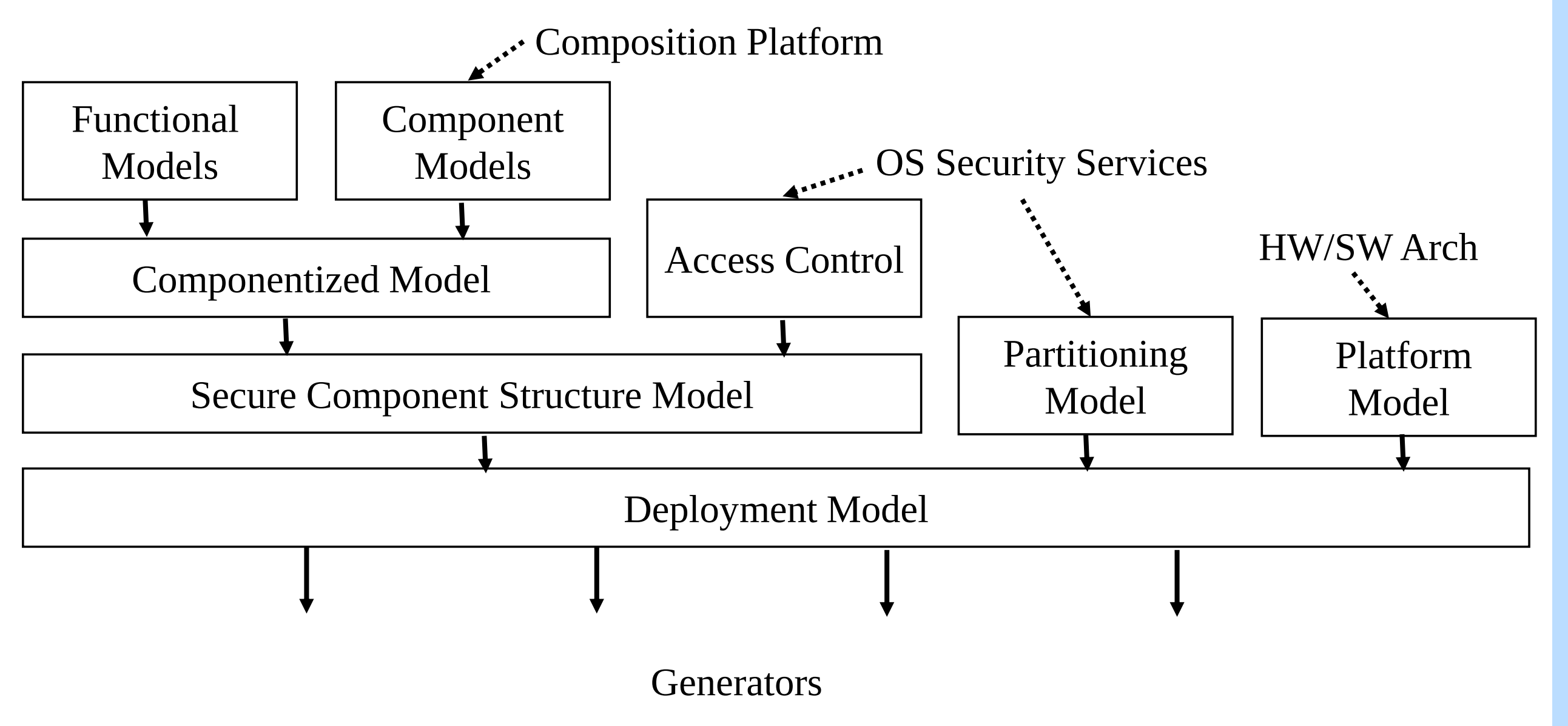
Introducing security on the design level

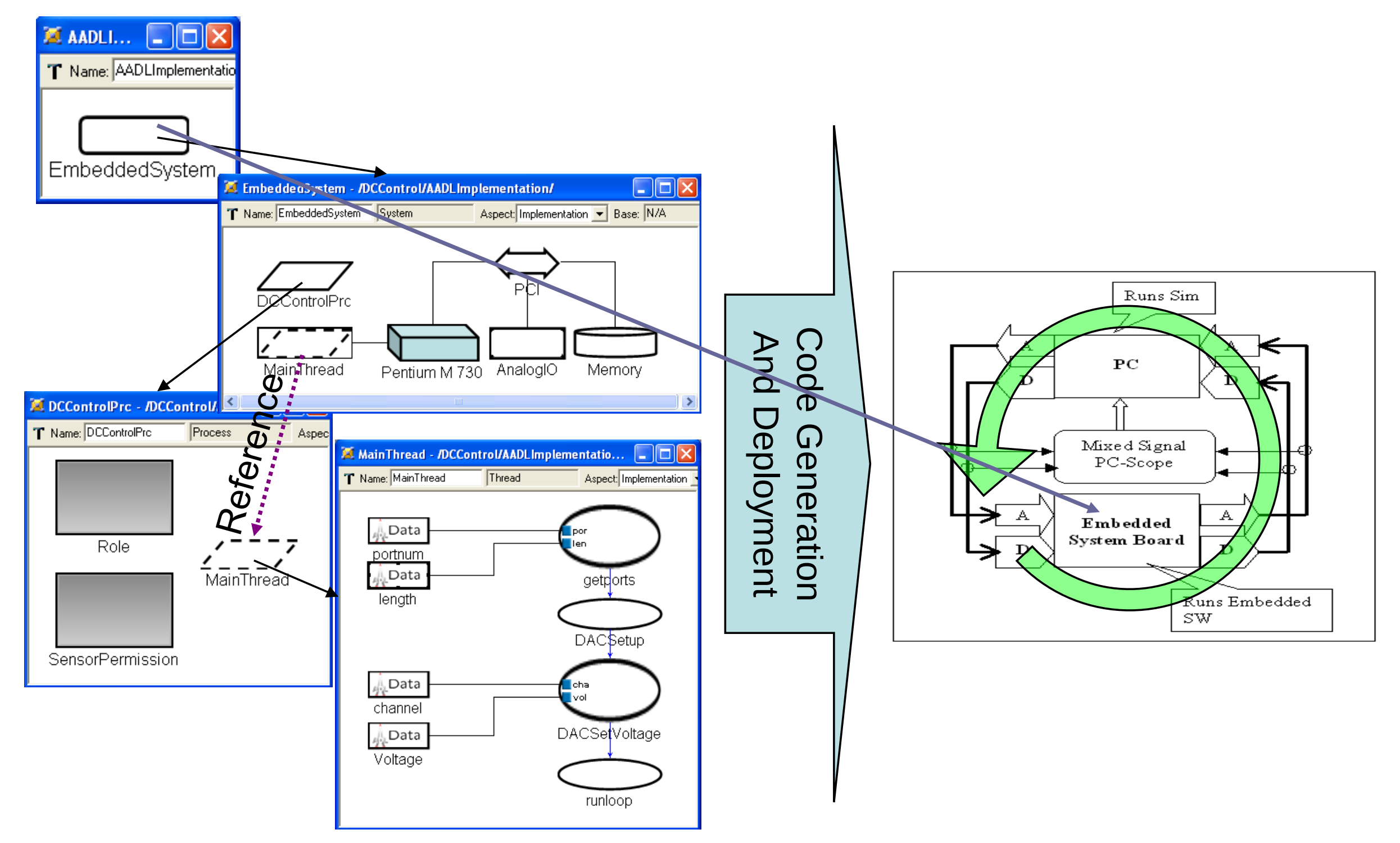
Avoiding design flaws and known bad programming habits using automated code generation

Enforcing security mechanisms on the operating system level and access control between applications


Role Hierarchy
User Assignment
Permission Assignment
USERS
ROLES
OPS
OBS
PRMS
SESSIONS


Partition A
Partition B
Operating System
Hardware
Partition A
Partition B
OS Services A
OS Services B
Kernel
Hardware


Composition Platform
Functional Models
Component Models
OS Security Services
Componentized Model
Access Control
HW/SW Arch
Secure Component Structure Model
Partitioning Model
Platform Model
Deployment Model
Generators


EmbeddedSystem
References
Code Generation And Deployment
PC
Embedded System Board