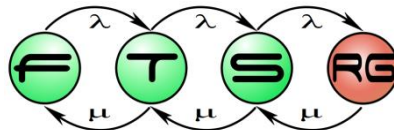


Architecture Modeling in embedded systems

Ákos Horváth

Model Driven Software Development
Lecture 11



Abstract

- “The software architecture of a program or computing system is the structure or structures of the system, which comprise software components, the externally visible properties of those components, and the relationships among them.”
- Software Architecture in Practice, Bass, Clements, and Kazman

General Concepts

Overview

- **First and foremost:** no universal agreement on what ADLs should represent
- Typically formal representation of architecture
- Human and machine readable
- Describes the system at a higher level
- Enables analysis on consistency, completeness, etc.

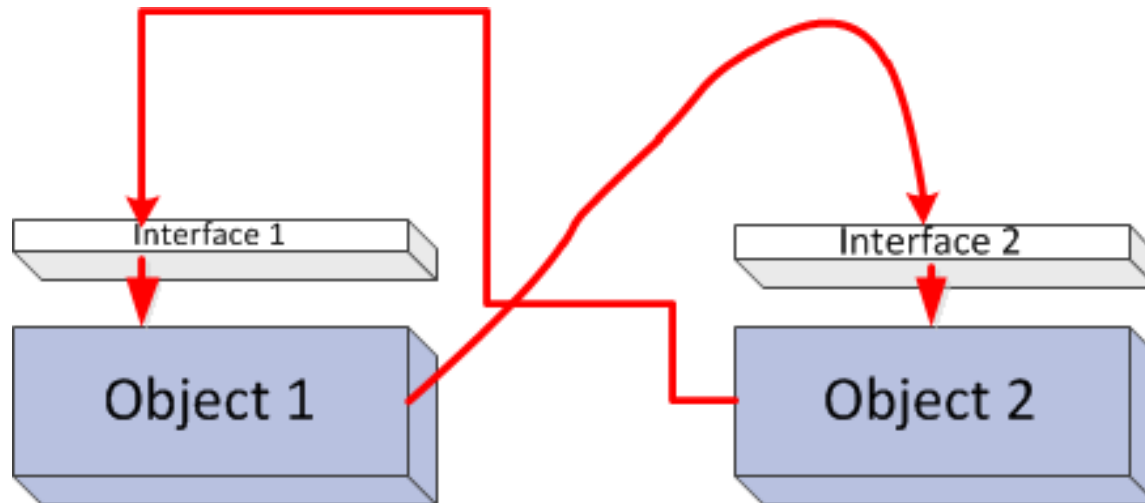
Design vs. Architecture

- Design
 - Functional requirements are addressed
- Architecture
 - Highest level of system description
 - Functional requirements are partitioned
 - Non-functional requirements are addressed
 - Typical Strategies
 - Layering
 - Diagnostics
 - Performance control and monitoring
 - COTS / reuse
 - GUI driven, API driven, etc.

Common Concept of Architecture (by Tw Cook)

■ Object Connection Architecture

- Configuration consists of
 - Interfaces: features that must be provided
 - Connections: object \rightarrow interface (+ call graph)

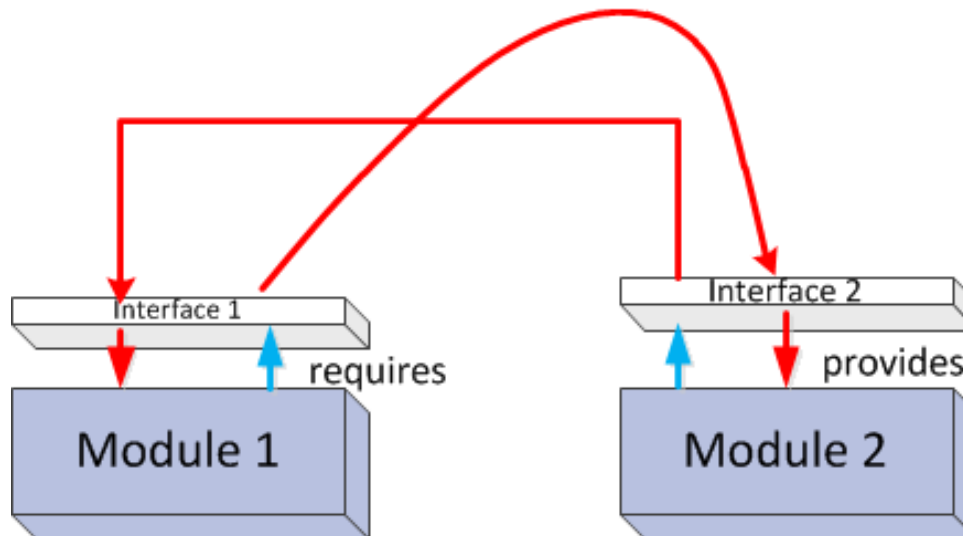


Common Concept of Architecture (by Tw Cook)

- Usually mature languages
 - C++, Java, Ada
- Module must be „built” before architecture is defined
- Conformance of a system to an architecture is low
- Architecture is sensitive to changes in the system

Common Concept of Architecture (by Tw Cook)

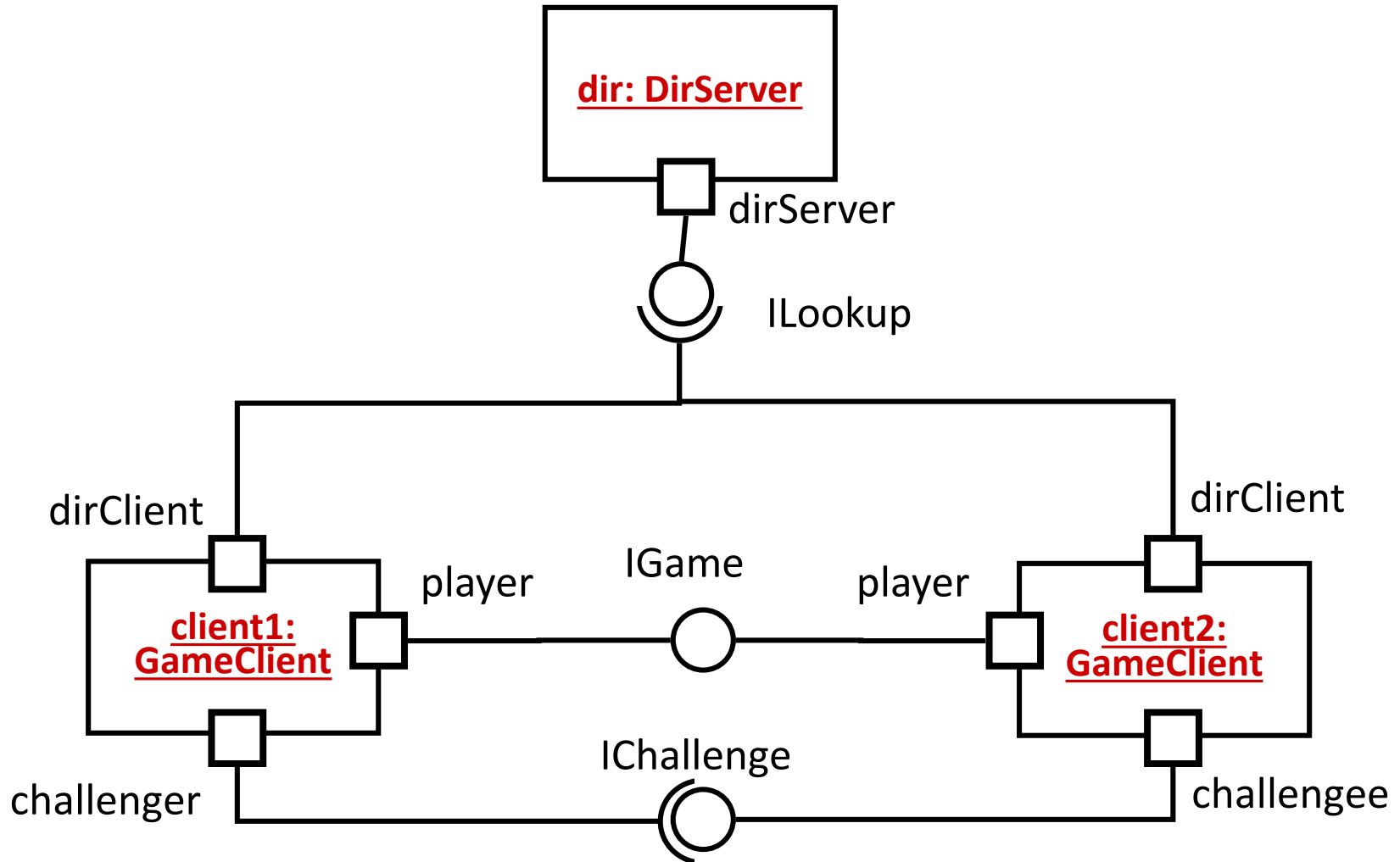
- Interface Connection Architecture
- Extends Interface and connection definition
 - Interface: both required and provided features
 - Connections: between required and provided interfaces
 - **Constraints** :
 - restricts behavior of connections and interfaces
 - Architecture constraints → system requirements



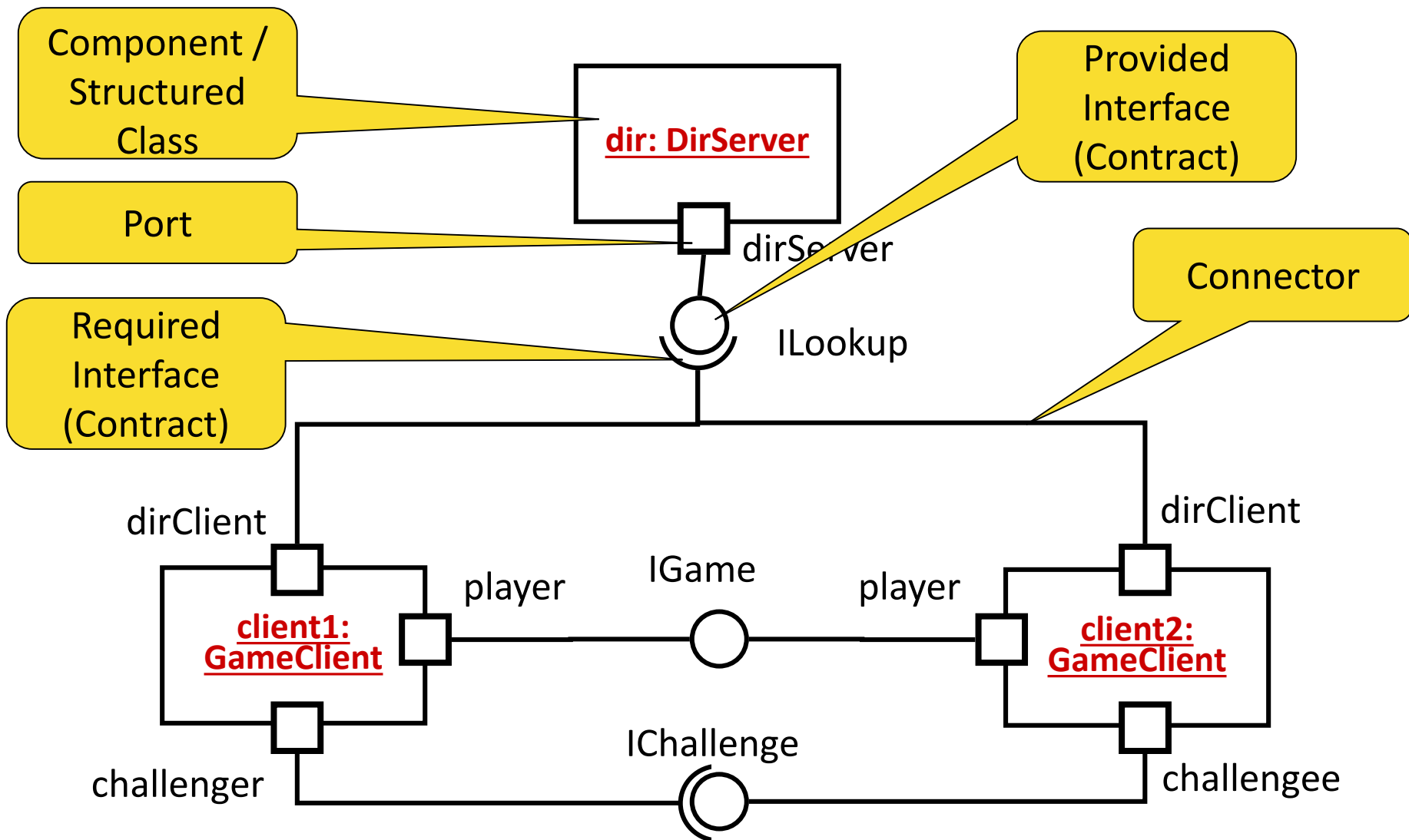
Common Concept of Architecture (by Tw Cook)

- Better conformance of a system to an architecture
- Architecture can be built before modules are „implemented”
- Most ADL approaches follows this concept
- Similar techniques widely used
 - Design-by-contract
 - Strong partitioning RTOS
 - Etc.

Example: Component Diagram in UML



Example: Component Diagram in UML



Architecture Analysis and Design Language (AADL)

AADL

- Architecture Analysis and Design Language (AADL) is a standard architecture modeling language
 - Avionics
 - Aerospace
 - Automotive
 - Robotics
- Component based notation
 - Task and communication architecture
- Designed for modeling and analysis in mind
- SAE standard (AS 5506A)

- First was called Avionics Architecture Description Language
 - Derived from MetaH created by Honeywell
- V1 version in 2004
- V2 version in 2009

AADL

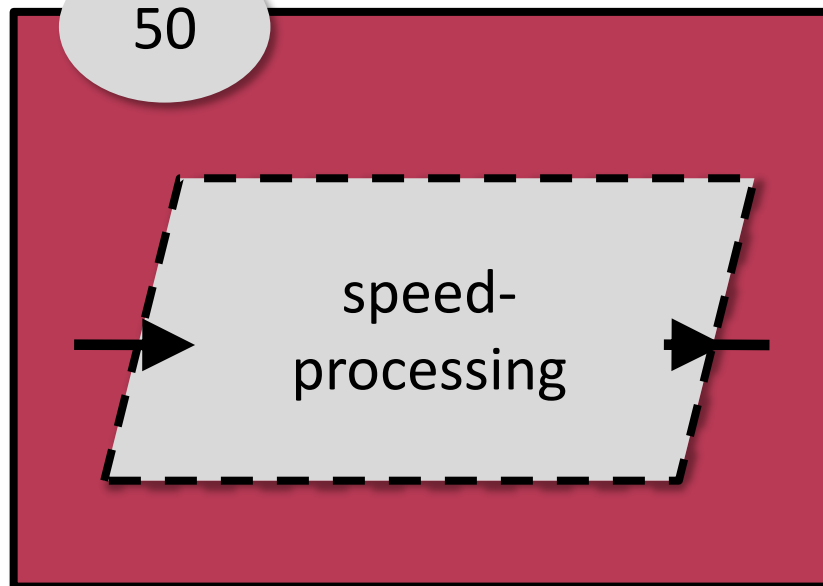
- Based on the component-connector paradigm
- Key Elements:
- Core AADL language standard (V2-Jan,2009, V1-Nov 2004)
 - Textual & graphical, precise semantics, extensible
- AADL Meta model & XMI/XML standard
 - Model interchange & tool interoperability
- Annexes Error Model Annex as standardized extension
 - Error Model Annex addresses fault/reliability modeling, hazard analysis
- UML 2.0 profile for AADL
 - Transition path for UML practitioner community via MARTE
- EMF representation also available (without EFeatureMap!)

AADL

- Precise execution semantics for components
 - Thread, process, data, subprogram, system, processor, memory, bus, device, virtual processor, virtual bus
- Continuous control & event response processing
 - Data and event flow, synchronous call/return, shared access
 - End-to-End flow specifications
- Operational modes & fault tolerant configurations
 - Modes & mode transition
- Modeling of large-scale systems
 - Component variants, layered system modeling, packaging, abstract, prototype, parameterized templates, arrays of components and connection patterns
- Accommodation of diverse analysis needs
 - Extension mechanism, standardized extensions

AADL Representation Forms

```
thread speed_processing
features
  raw_speed_in: in
data port;
  speed_out: out data
port;
properties
  Period => 50 ms;
end data_processing;
```



```
<ownedThreadType name=„speed_processing“>
  <ownedDataPort name=“raw_speed_in“/>
  <ownedDataPort name=“speed_out“ direction=“out“/>
  <ownedPropertyAssociation property=“Period“
    <ownedValue xsi:type=“aadl2:IntegerLiteral“
      value=“50“ unit=“ms“
    </ownedValue>
  </ownedPropertyAssociation>
</ownedThreadType>
```


AADL Language Elements

- Core modeling
 - Components
 - Interactions
 - Properties
- Engineering support
 - Abstractions
 - Organization
 - Extensions
- Infrastructure

- Strong modeling capabilities for embedded SW and Computer systems

AADL Components

- Top element **system**

Example:

```
package F22Package
  public
    system F22System
  end F22System;
  system WeaponSystem
  end WeaponSystem;
  system implementation F22System.impl
    subcomponents
      weapon: system WeaponSystem;
    end F22System.impl;
  end F22Package;
```

AADL SW Components


- **System** – hierarchical organization of components
- **Process** – protected address space
- **Thread group** – logical organization of threads
- **Thread** – a schedulable unit of concurrent execution
- **Data** – potentially sharable data
- **Subprogram** – callable unit of sequential code



System



Process



Thread group



Thread



Data



Subprogram

AADL SW Components

■ Process

- Protected virtual address space
- Contains executable program and data
- Must contain 1 thread

■ Thread

- Concurrent tasks
- Periodic, aperiodic, sporadic ,background, etc.
- Interaction through port connection, subprogram calls or shared data access
- errors: recoverable, unrecoverable

AADL SW Components

■ Ports and Connections

- Data (non queued data), Event (queued signals) or Event data (queued messages)
- Complex Connection hierarchies through components
- Timing
- Feature groups

■ Data

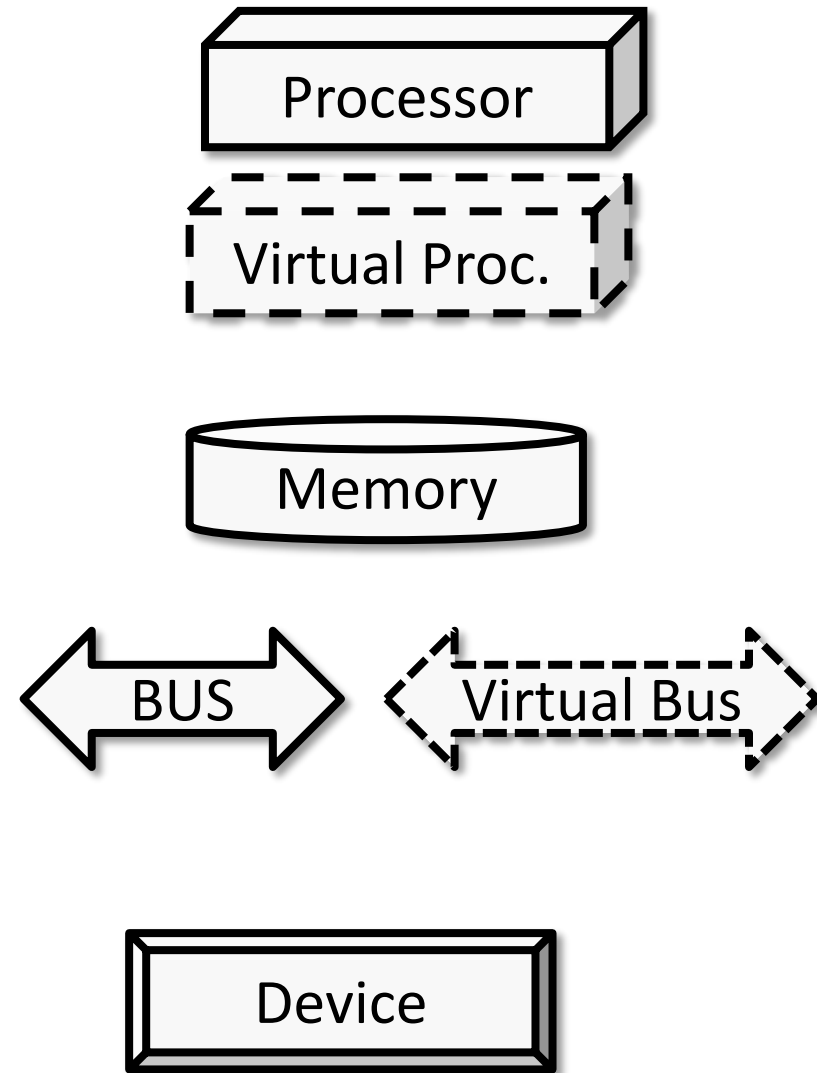
- Optional but makes the analysis more precise

■ Flows

- Logical flow of data and control

AADL Computer Components

- **Processor / Virtual Processor** – Provides thread scheduling and
- **Memory** – provides storage for data and source code
- **Bus / Virtual Bus** – provides physical/logical connectivity between
- **Device** – interface to external environment



AADL Computer Components

- “Real” HW components
 - Bus transmission time, latency,
 - Processor timing, jitter
 - Memory capacity
 - Etc.
- Logical resources
 - Thread scheduling of a processor
 - Communication protocol over network connection (modeled as bus)
 - Transactional memory (modeled as memory)

AADL Computer Components

■ Processor

- As HW
 - MIPS rating, size, weight, clock, memory manager
- As Logical resource
 - Schedule threads → scheduling policies and interruption
 - Execute SW

■ Bus

- As HW
 - Physical connection inside/between HW components
- As logical resource
 - Protocol, which are used for the communication

■ Memory

- Processes must be in memory
- Processors need access to memory

■ Device Components

- Represents element that are not decomposed further
- Sensors/Actuators
- Device Driver

AADL Binding

■ Binding

- Bringing SW models and the execution platform together
- Virtual processors → can be subcomponents of other virtual processors → ARINC653 partitioning
- Hierarchical Scheduling
- virtual buses to physical ones
 - One-to-one
 - Many-to-one

Summary

- After 15 years of mainly DoD research it is getting mature enough
- Many pilot project uses AADL
 - FAA
 - DoD
 - Lockheed Martin
 - Rockwell Collins (Steven P. Miller)
- Many research paper on formal analysis, simulation and code generation
- Ongoing harmonization with SysML and MARTE

AUTOSAR & EAST-ADL

History

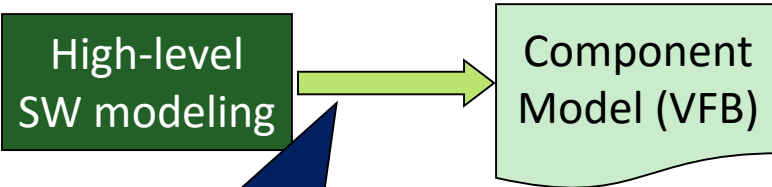
- AUTomotive Open System ARchitecture
- Started in 2002
- BMW, Bosch, Daimler, Conti, VW, + Siemens
- Industrial standardization group
 - Current standard version: 4.0 (end 2009)
 - Currently we use 3.1 (end 2008)
- Members: OEMs, Tool vendors, Semiconductor manufacturers ☐ Europe-dominated
- Scope
 - Modeling and implementation of automotive systems
 - Distributed
 - Real-time operating system
 - String interaction with HW and environment
- Out of scope
 - GUI, Java, internet connectivity, File systems, Entertainment systems, USB connectivity etc.

Key Concepts of AutoSAR

- A standard runtime architecture
 - **component-oriented**
 - layered
 - extensible
 - New functionalities
 - New components (component implementations)
 - all major interfaces standardized
 - Standardized Run Time Environment (RTE)
- A standard modeling and model interchange approach
 - follows the principles of model-driven design
 - supports the interchange of designs
 - supports the collaborative development
 - Between different developers,
 - Teams,
 - And even companies
- Conformance test framework
 - assuring the conformance to the standard

High-level design flow

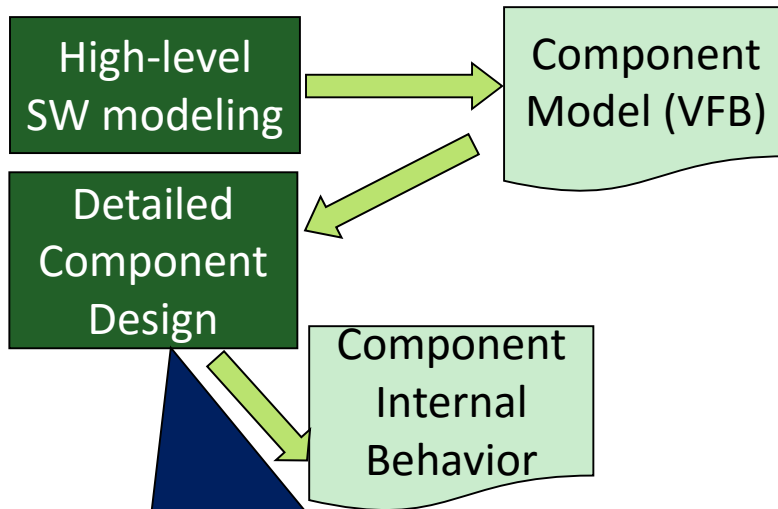
High-level design process



High-level software modeling

- Definition of
 - components
 - component ports
 - port interfaces
 - data types – logical
- Result
 - Virtual Functional Bus (VFB)-level software model

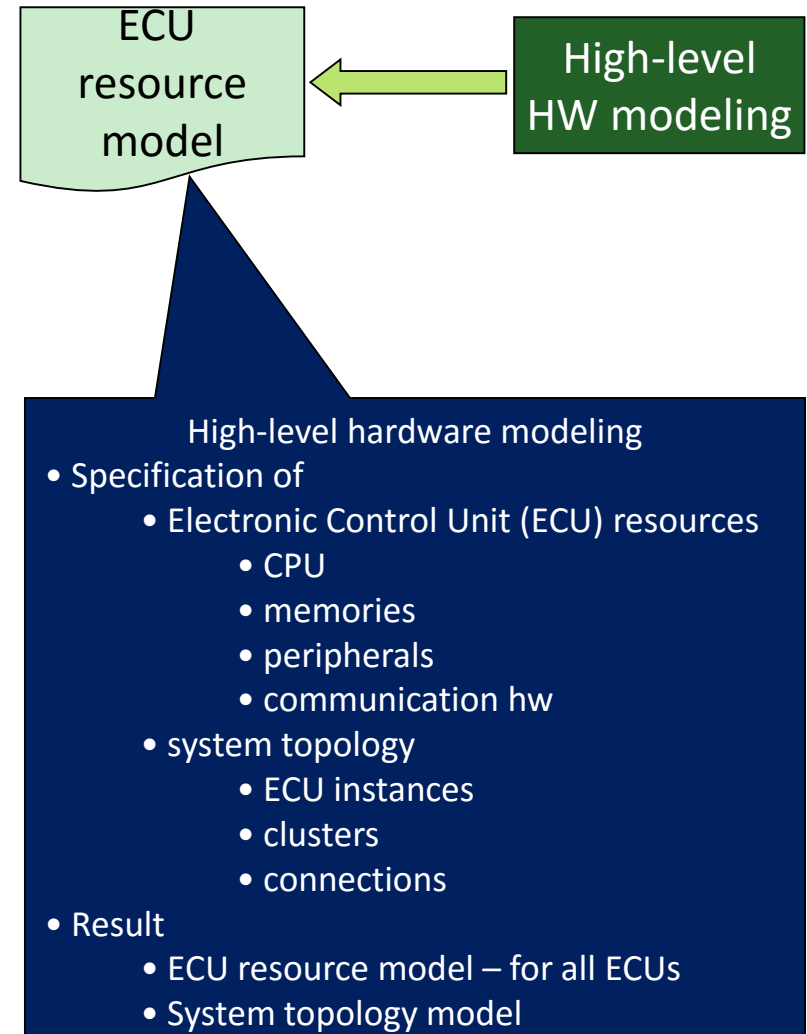
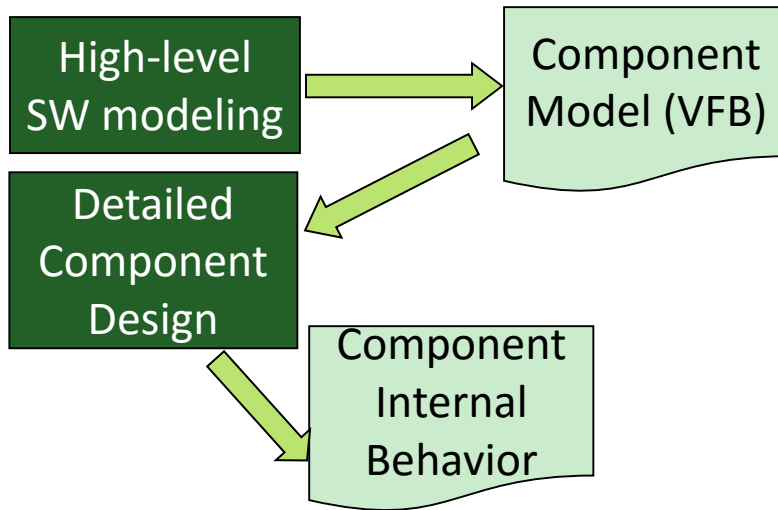
High-level design process



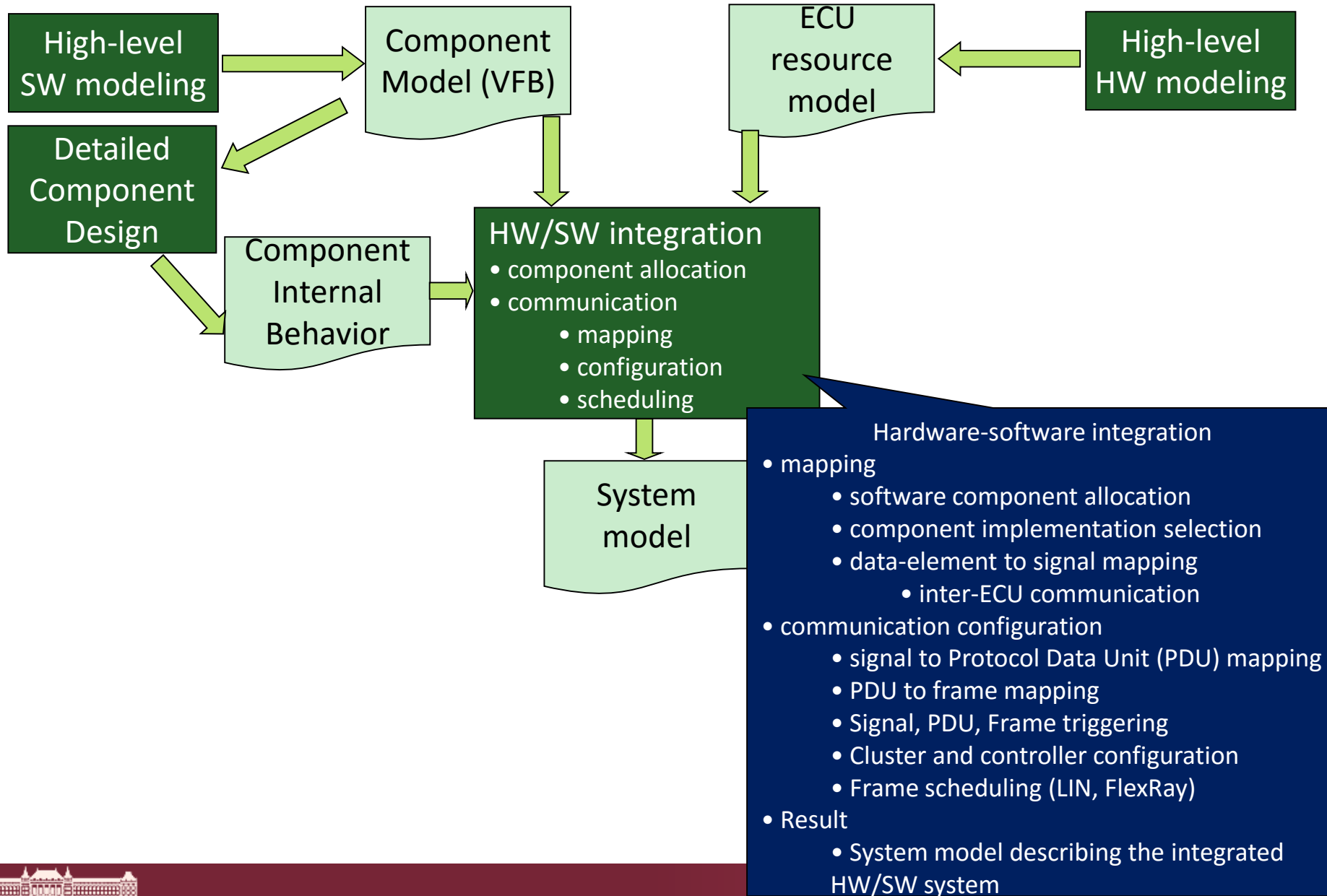
Detailed component design

- Specification of
 - component internal behavior
 - functional breakdown
 - implementation/use of ports
- Non-AutoSAR
 - specification of detailed behavior
 - any tool can be used
 - UML
 - Simulink
 - etc.
- Result
 - AutoSAR component internal behavior model
 - Non-AR: behavioral models/design

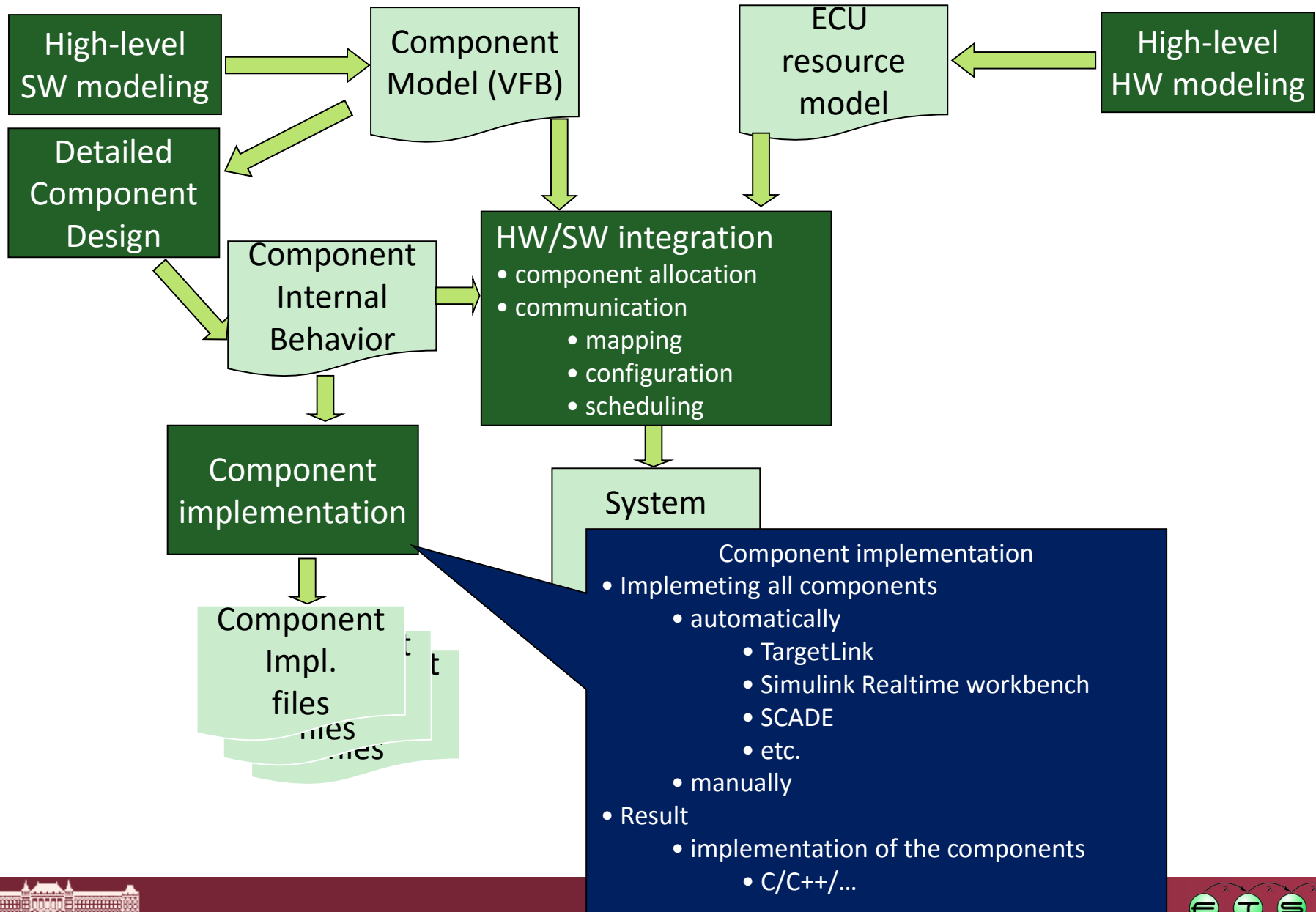
High-level design process



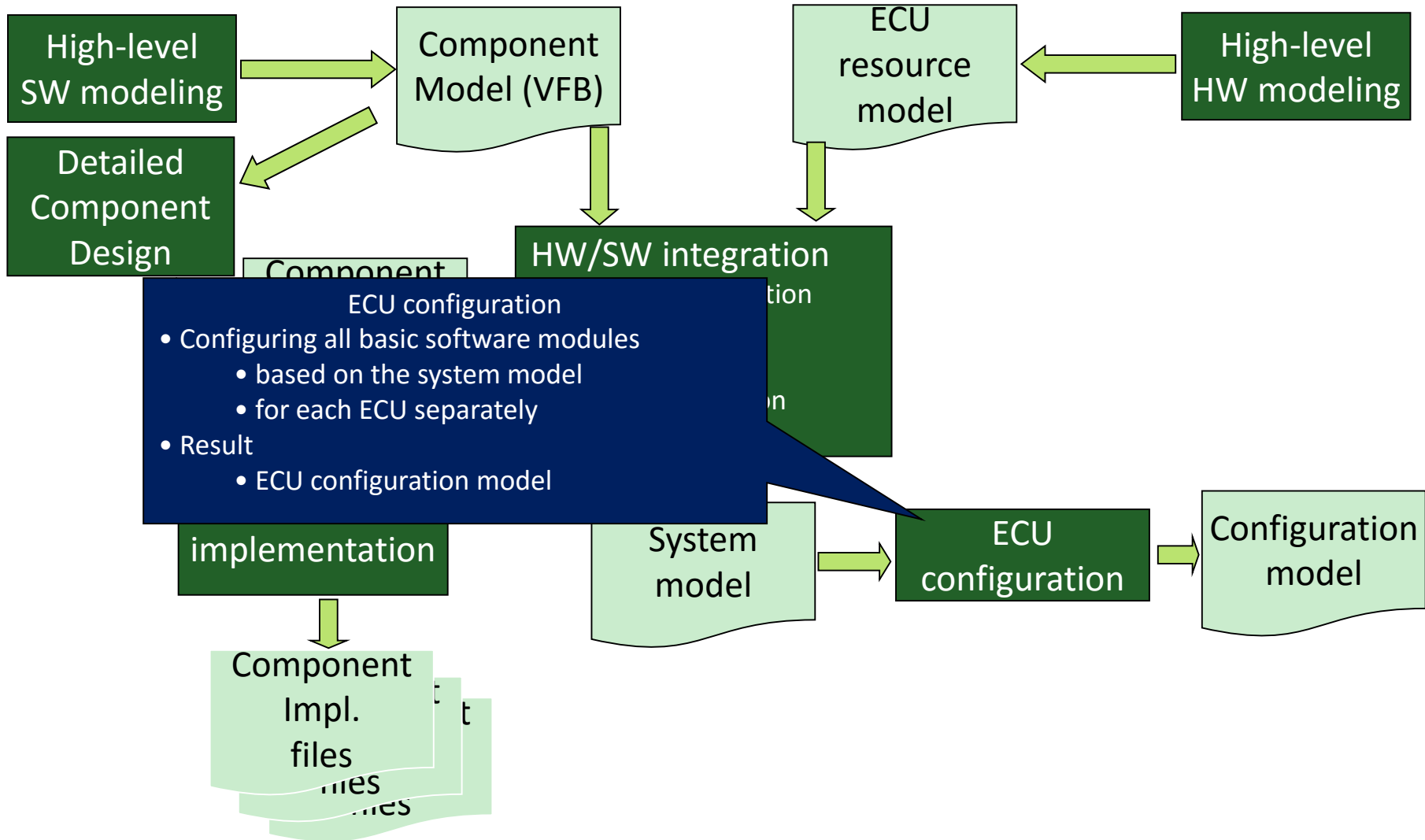
High-level design process



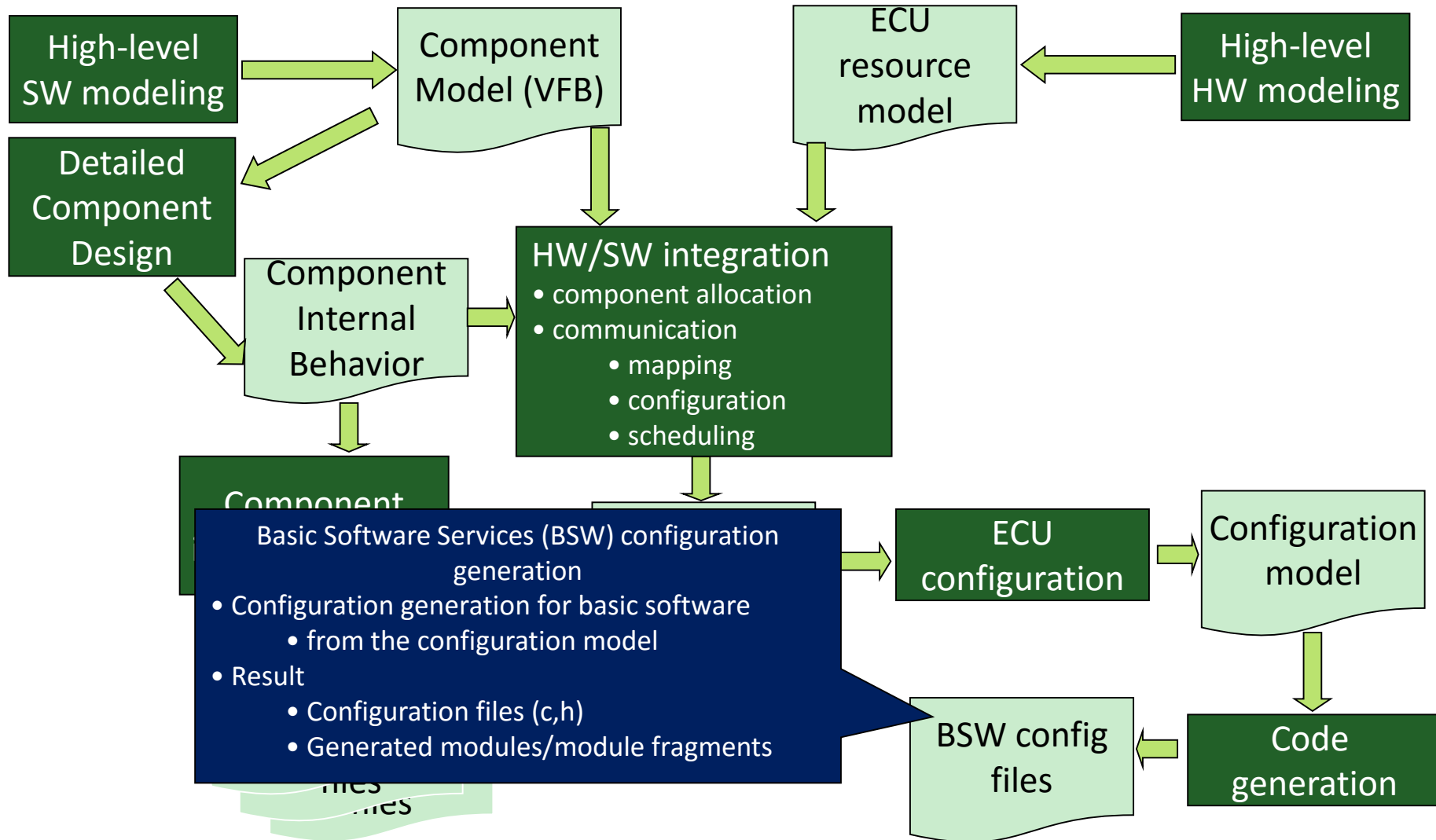
High-level design process



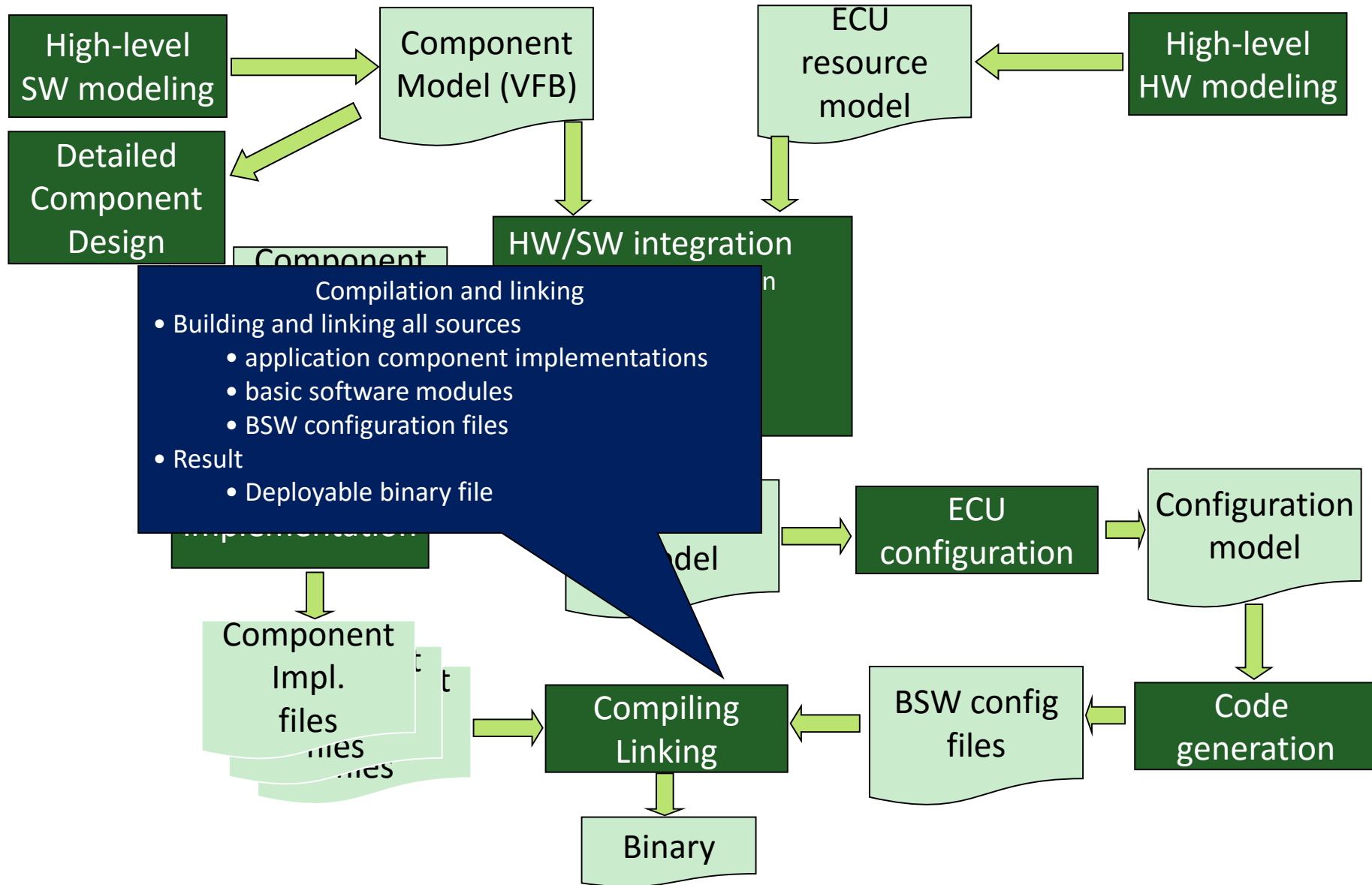
High-level design process



High-level design process



High-level design process



Models in the design flow

- Software Component Template
 - Components, ports, interfaces
 - Internal behavior
 - Implementation (files, resource consumption, run time, etc.)
- ECU Resource Template
 - Hardware components, interconnections
- System Template
 - System topology, HW/SW mapping
 - Comm. matrix

Models in the design flow 2

- Basic Software Module Template
 - BSW modules
 - Services
 - Schedulable entities
 - Resource consumption
- ECU Configuration Parameter Definition Template
 - Configurable parameters of BSW modules
- ECU Configuration Description Template
 - Actual configurations of BSW modules
 - Based on the ECU Parameter Definition

AutoSAR vs. UML/SysML/... modeling

- AutoSAR defines models with
 - Domain Specific Constructs
 - *Precise syntax*
 - Synthesizable constructs
 - Direct model -> transformations
 - Direct model -> detailed model mappings
 - Different abstraction levels
 - From Virtual Function Bus to configuration
- Result
 - Models *are* primary design *and* implementation artifacts
 - More precise, consistent modeling should be done

AUTOSAR Components

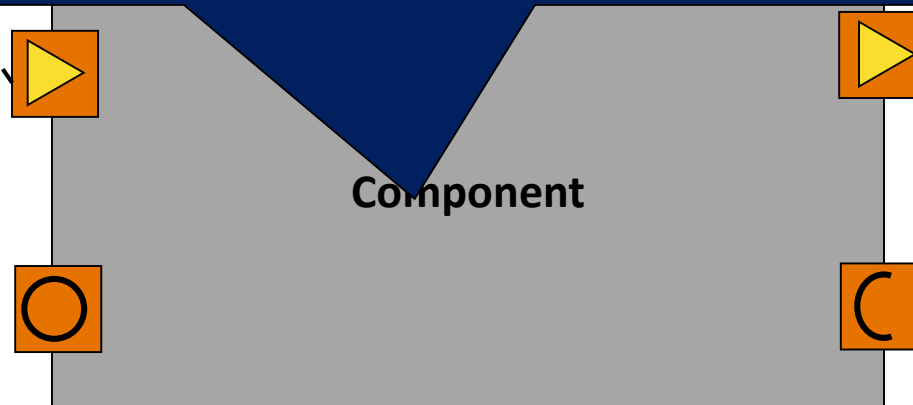
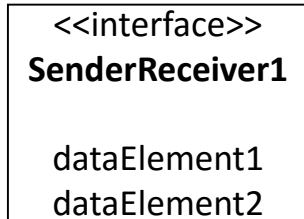
Component-oriented design

- What is a component?
 - “A component is a self contained, reusable entity that encapsulates a specific functionality (and/or data), and communicates with other components via explicitly defined interfaces.”
- AutoSAR uses the term *component* for application-level components
 - Elements related to the high-level functionality of the system under design
- Basic software (middleware) components are called *modules*.
 - Standard elements of the AutoSAR architecture

Component-based approach

Component

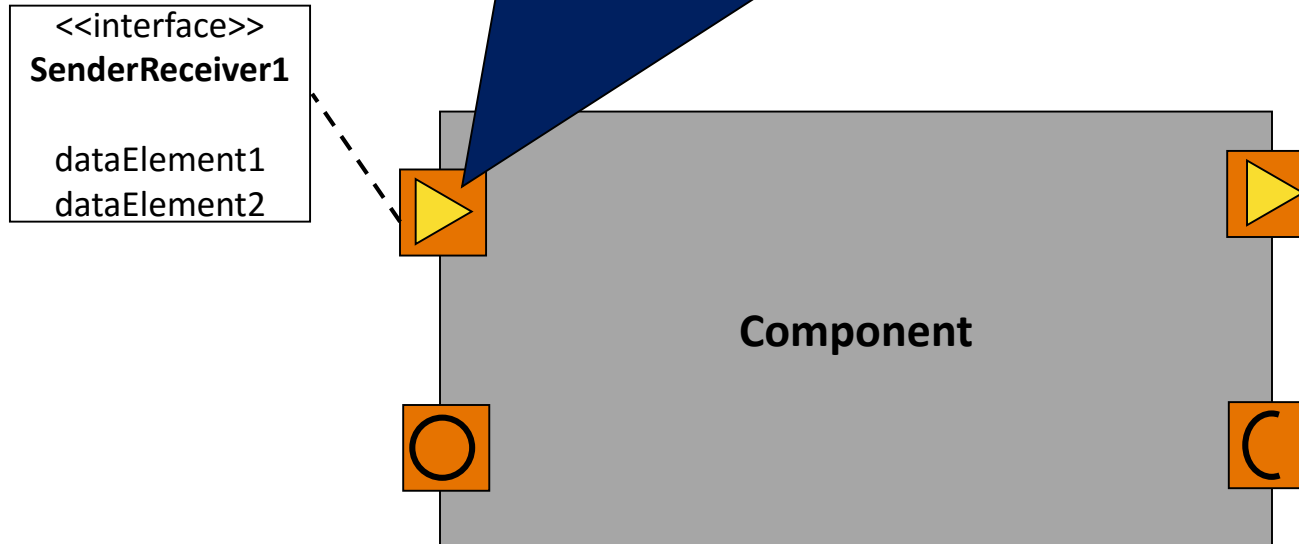
- Encapsulates a specific functionality
- Different kinds
 - Composite component – hierarchical refinement
 - Application SW component – generic, high level functionality
 - Sensor/actuator SW-C – handling sensor or actuator data
 - ECU HW abstraction – higher level device driver and abstraction
 - ComplexDeviceDriver – time-critical, low-level driver
 - Calibration parameter SWC – collects system calibration parameters
 - Service SWC – represents a basic software module from the service layer



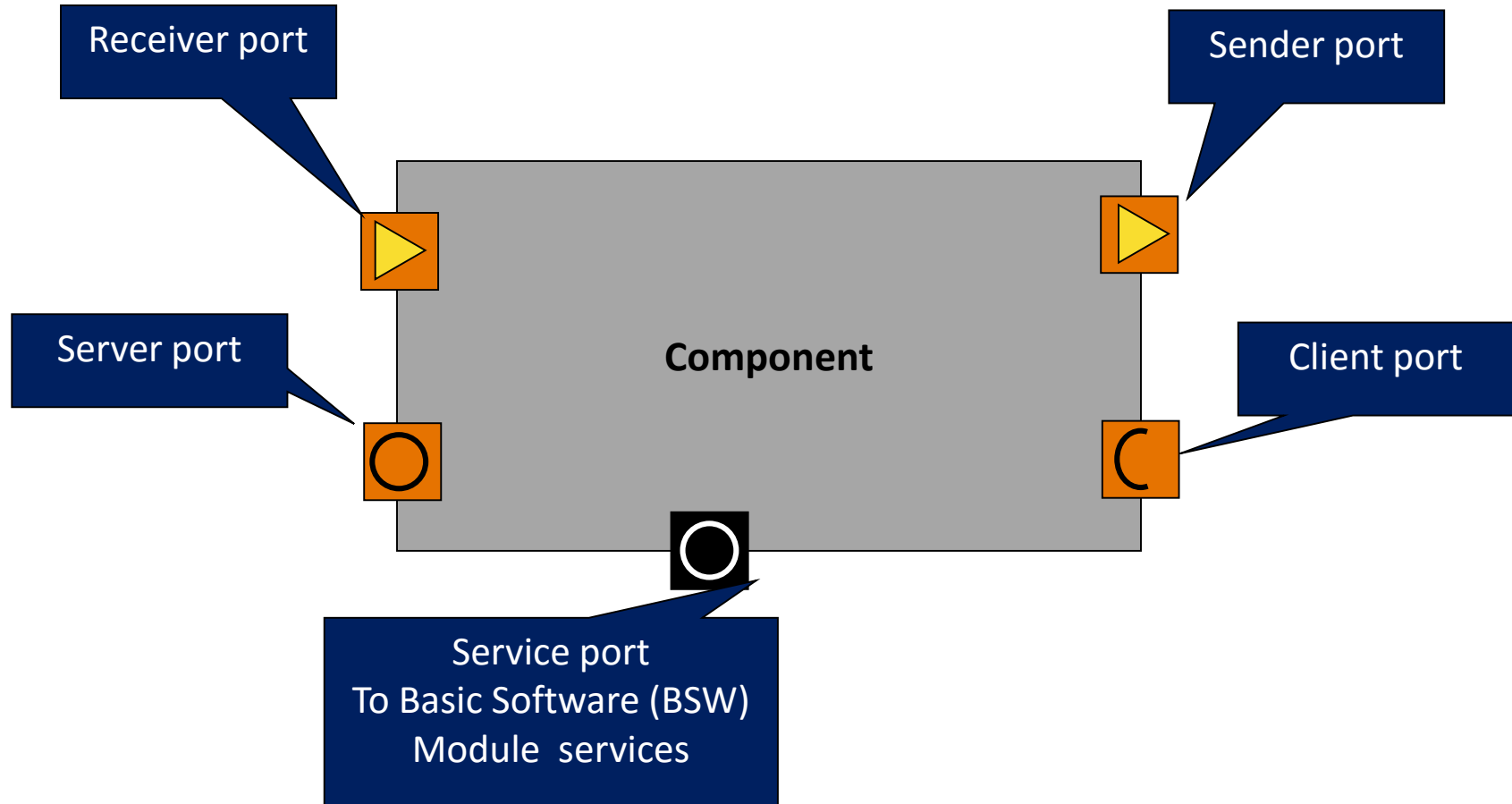
Component-based approach

Ports

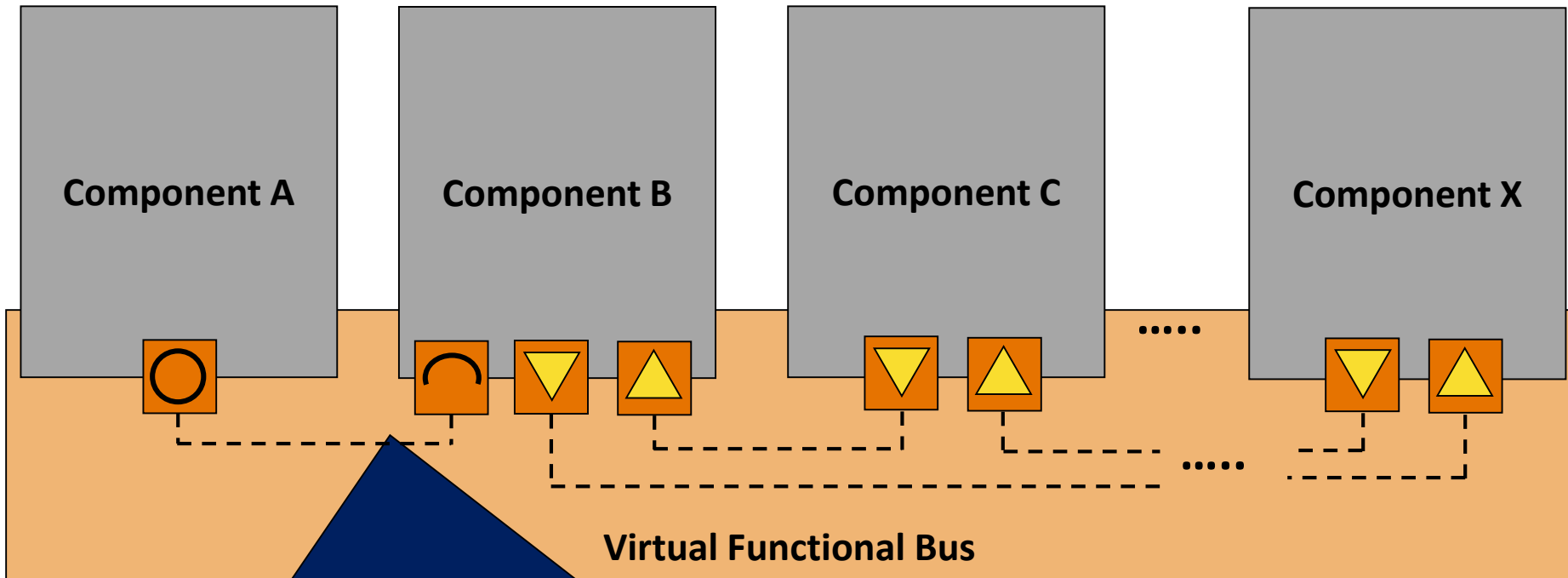
- The only interaction points between the component and its environment
- Are implementing *port interfaces*
 - sender receiver (message-based unidirectional communication)
 - client-server (remote procedure call)



Component-based approach – port notation



Component interconnection – the Virtual Functional Bus



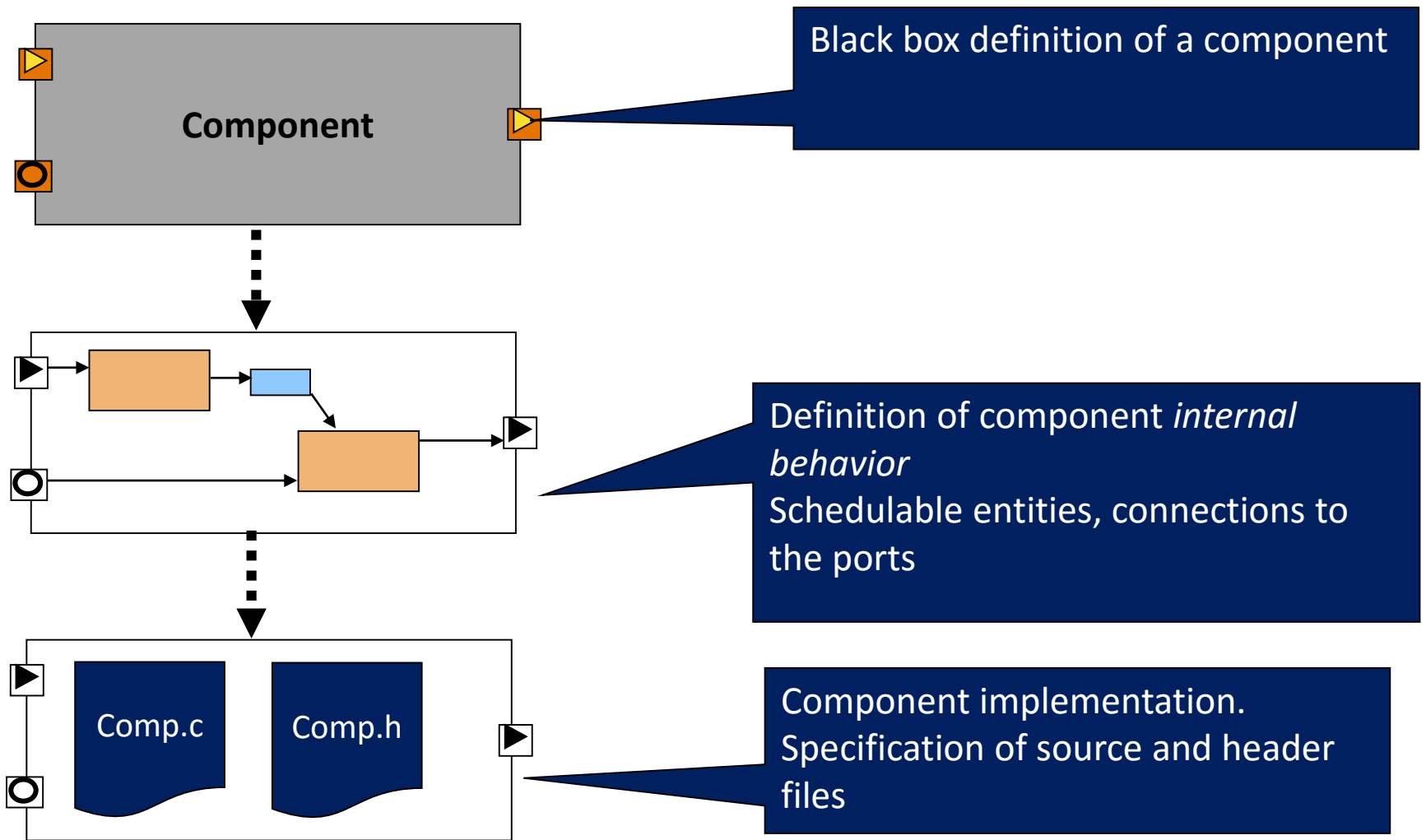
Virtual Functional Bus (VFB)

- Abstract interconnection layer
 - Implementation of data/control transport between components
 - No hardware/network dependency
 - Hides the details of the implementation
- Allows high-level integration *and simulation* of components
 - Before hardware architecture is chosen

Software Components

- On high-level, *atomic* components are black boxes
- Detailed design “looks into” these black boxes
- Main goals
 - Detail the behavior to get schedulable entities
 - Specify the semantics of port handling
 - Specify any service needs
 - Specify any RAM, nvRam needs

Refinement of a component



Component internal behavior

- Specification of the internals of an atomic SWC
- Schedulable elements
 - Called: runnable entities
- Connection of ports
 - Port semantics
 - Port API options
- Inter-runnable communication
- Runnable activation and events

Summary

- AutoSAR defines
 - A component-oriented system design approach
 - Domain specific modeling language
 - A high level design process
 - Standard middleware (basic software) stack
 - Standard interfaces
 - Standard configuration descriptors
- AutoSAR compliant ECU software
 - Includes several BSW and application components
 - RTE provides the integration (glue) between these
 - Configuration and glue code is mostly auto-generated