



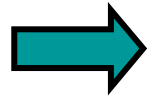
Multi-Fidelity Multi-Dimensional Analysis of Performance-Critical Systems

Peter H. Feiler

Apr 2007



Outline

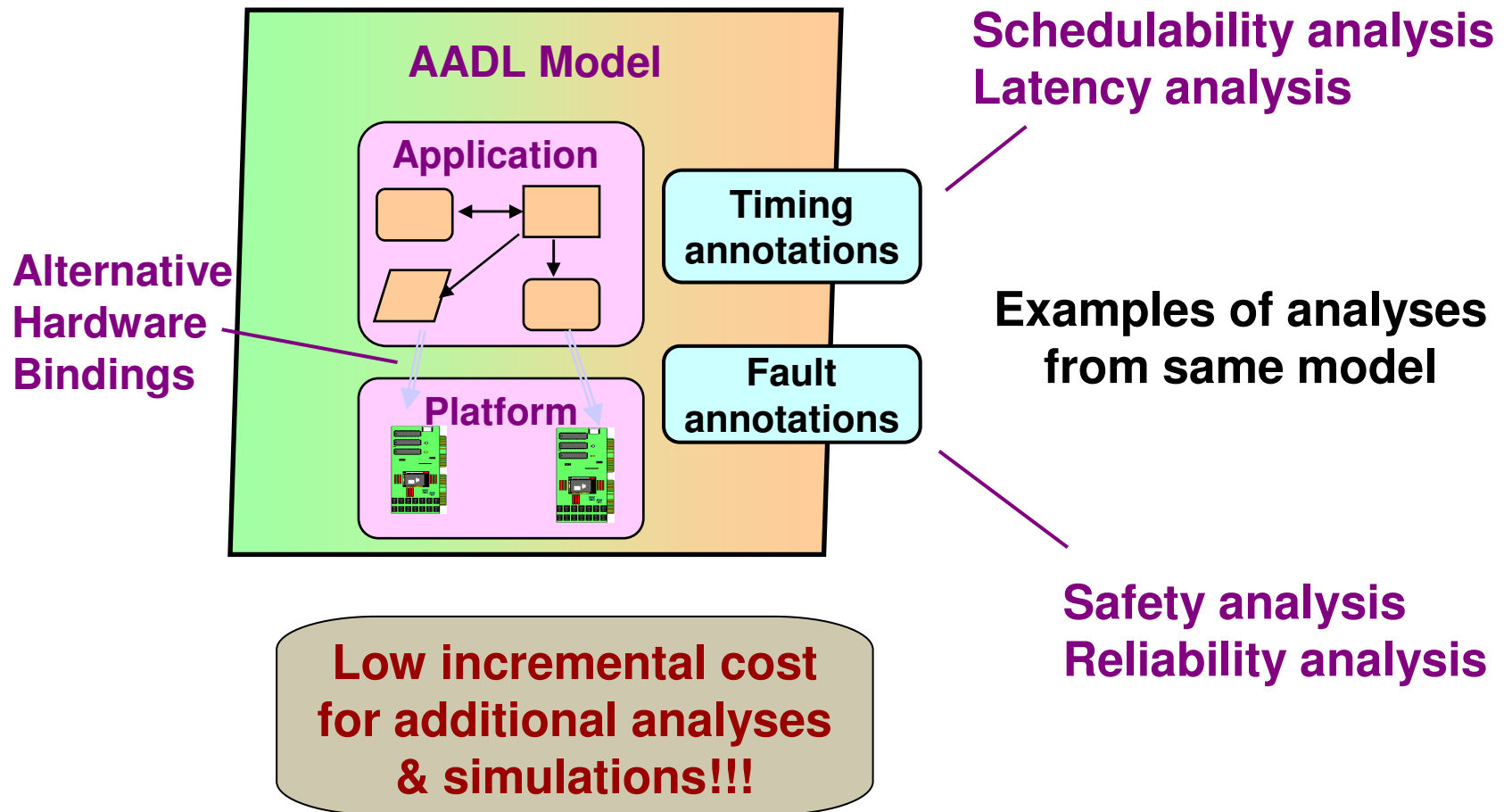


Model-based Embedded System Engineering

- Resource Consumption: Resource Budgeting
- Real-time Performance: Concurrency & Timing
- Real-time Performance: End-to-end Latency
- Security: Confidentiality Analysis
- Data Quality: Temporal Data Consistency

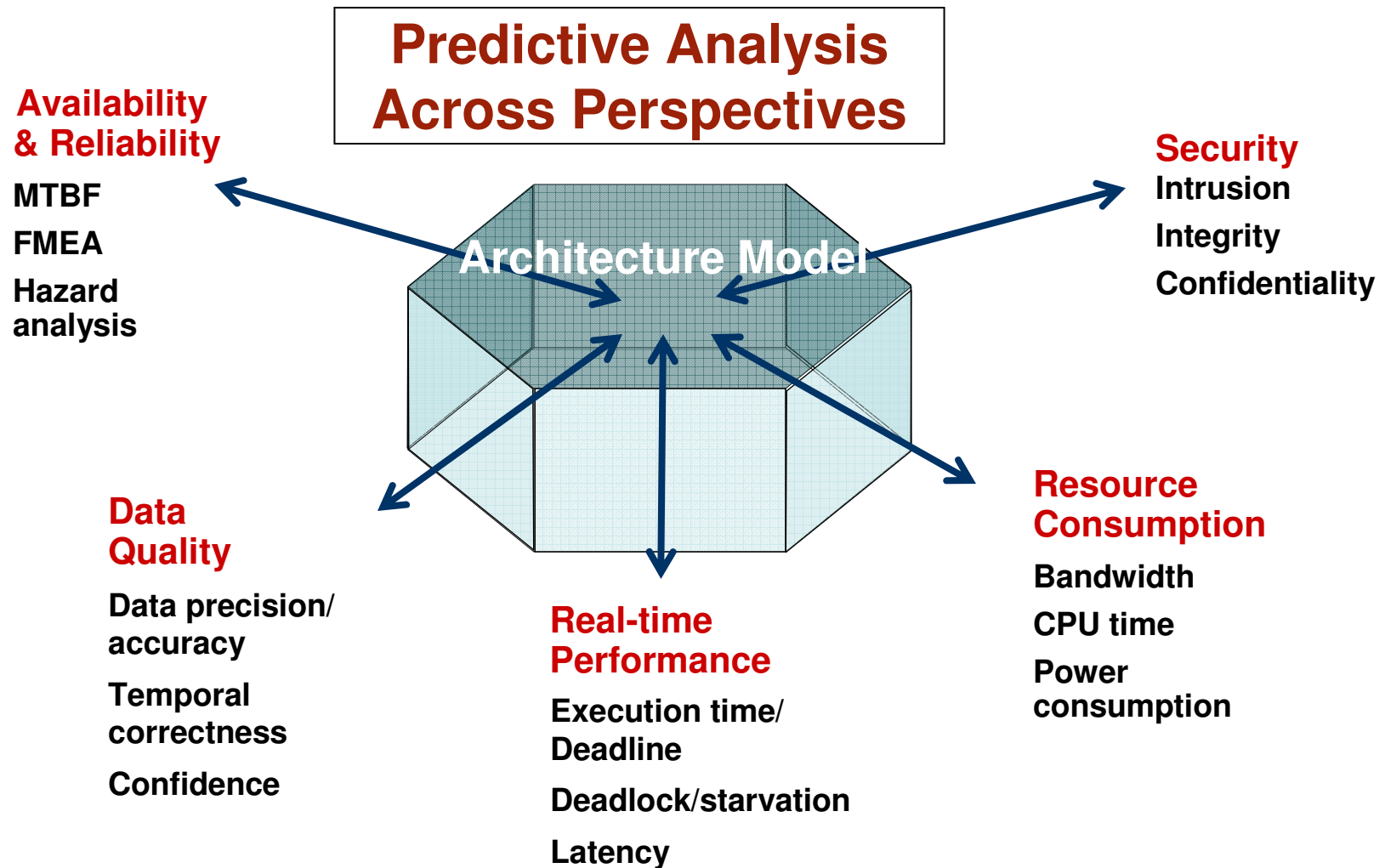


Single Source Architecture Model





Model-Based Assurance





Multi-Fidelity Analysis

- From requirements to detailed design
- From parts list to critical flows
- From subsystem models to schedulable task architecture



Outline

- Model-based Embedded System Engineering
- ➔ Resource Consumption: Resource Budgeting
- Real-time Performance: Concurrency & Timing
- Real-time Performance: End-to-end Latency
- Security: Confidentiality Analysis
- Data Quality: Temporal Data Consistency

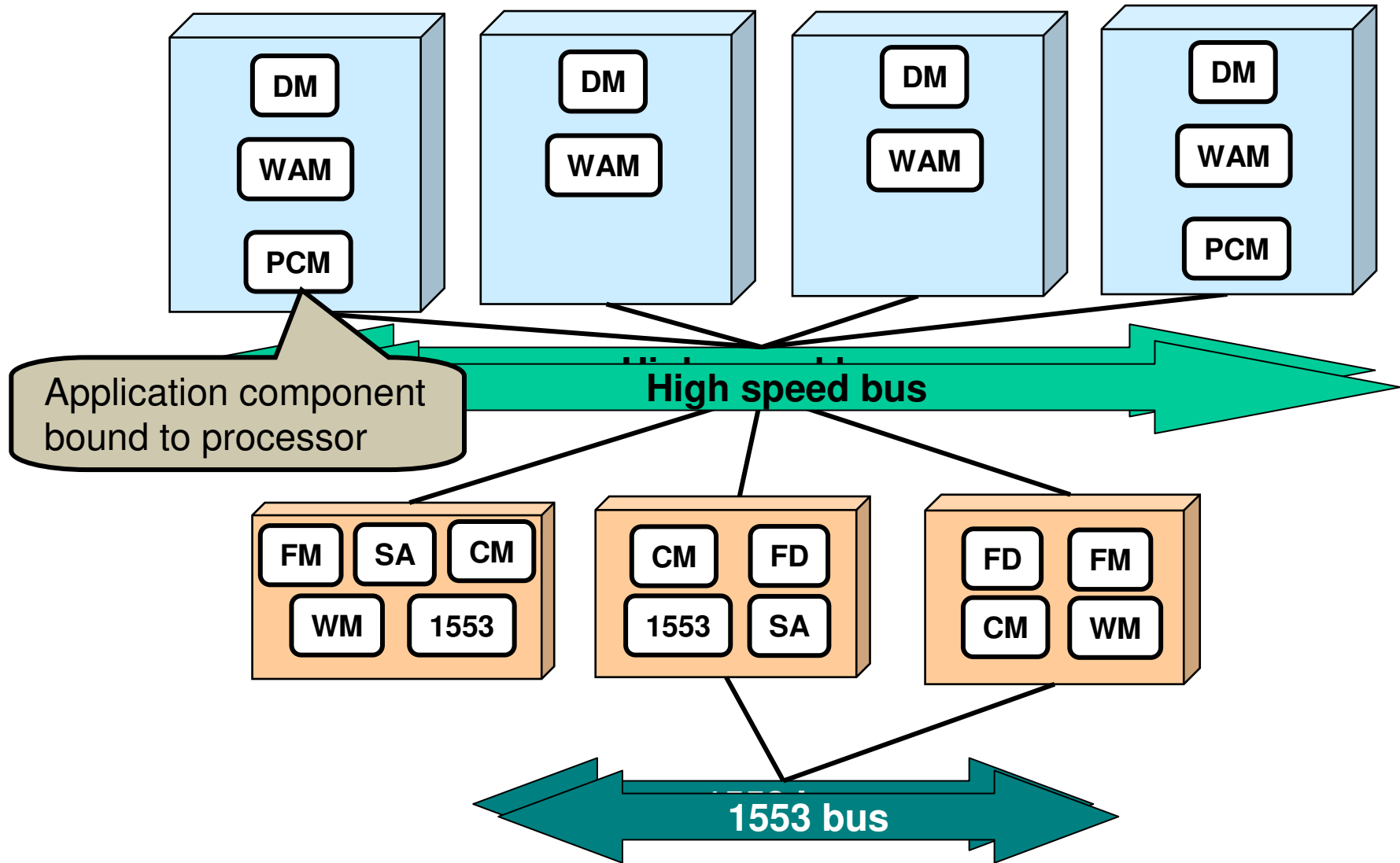


Resource Budgeting

- Resource management throughout life cycle
- Resource budgets for processors, memory, bus/networks
 - Compute resources: MIPS, MB, bandwidth
 - Physical resources: power consumption
- Budgets for major subsystems
 - System wide & resource specific budget totals
- System decomposition & budget refinement
- Task & communication model
 - Budgets against execution & communication rates
 - Scheduling analysis



Basic System Architecture



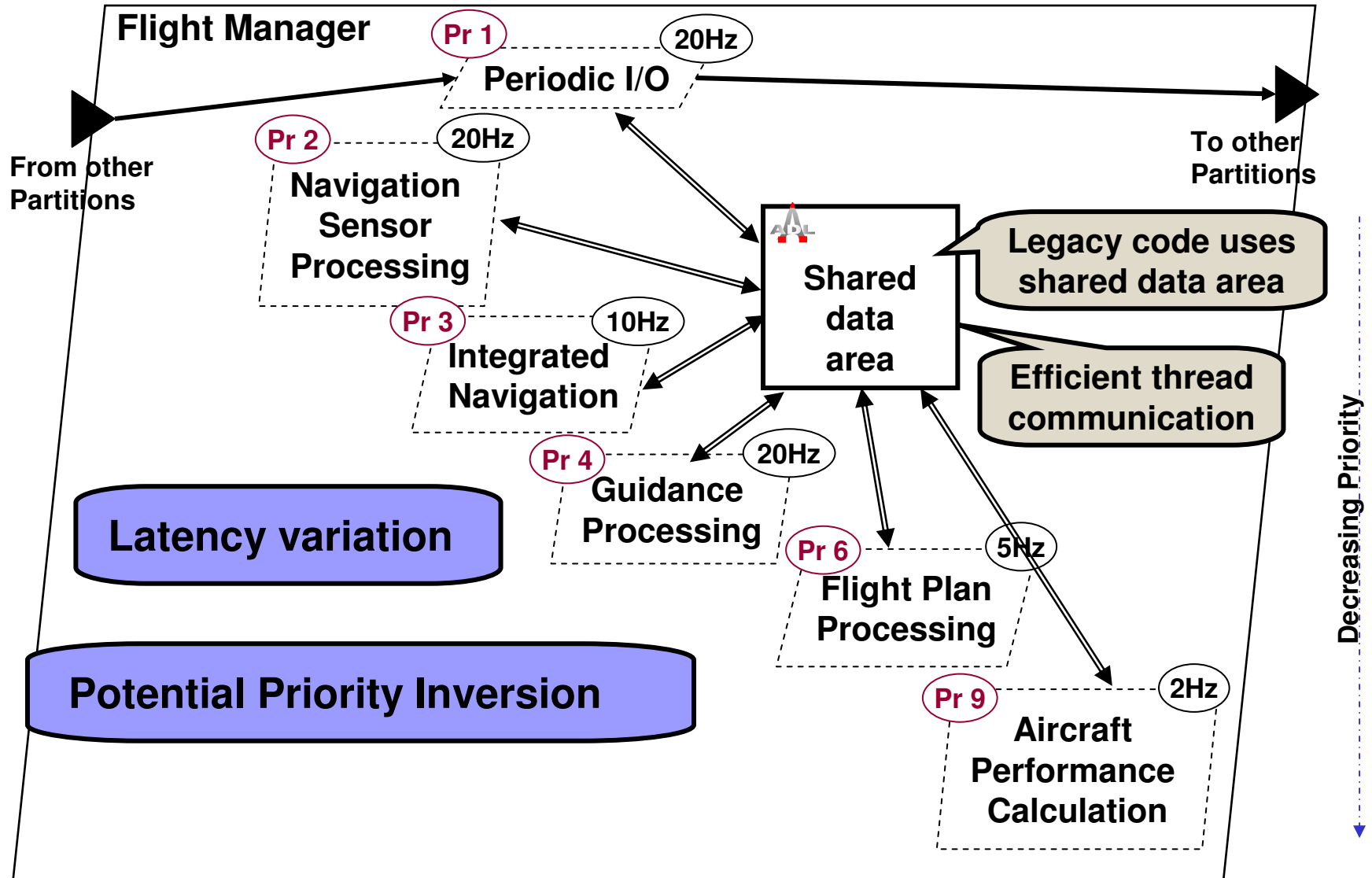


Outline

- Model-based Embedded System Engineering
- Resource Consumption: Resource Budgeting
- ➔ Real-time Performance: Concurrency & Timing
- Real-time Performance: End-to-end Latency
- Security: Confidentiality Analysis
- Data Quality: Temporal Data Consistency

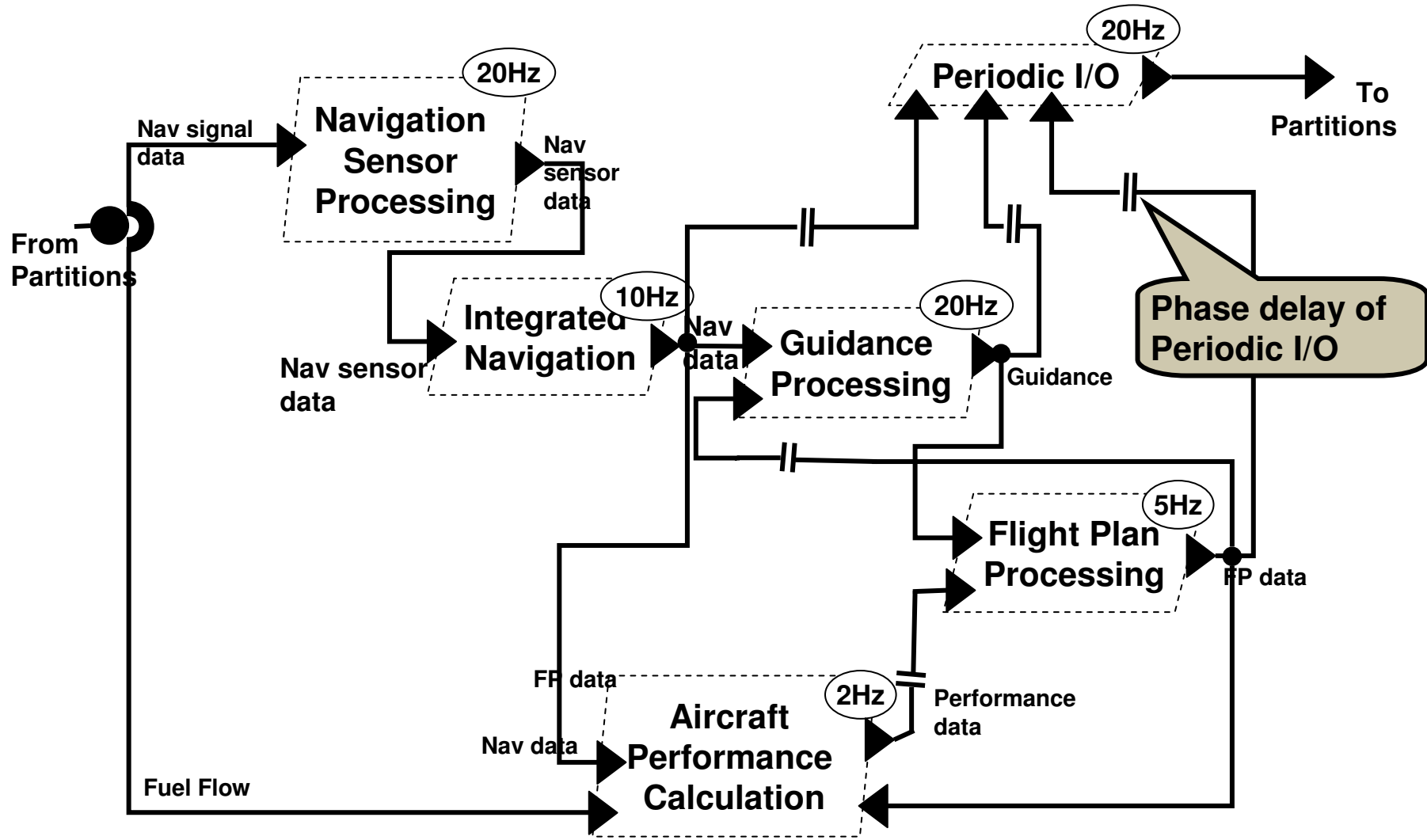


Migration of Legacy Implementation





Flow-based Flight Manager Model





Scheduling Analysis Demo

- If a single processor system is not schedulable
- Explore these options using AADL and analysis tools
 - Leverage operational modes
 - Processor speed dependent execution time
 - Rebind to different execution platform
 - Reduce worst-case execution time
 - Identify schedulable rate from sensitivity analysis results
- Might consider
 - Repartition system
 - Use faster processor
 - Add second processor
 - Rewrite code to make it faster
 - Consider lower signal processing rate for controller

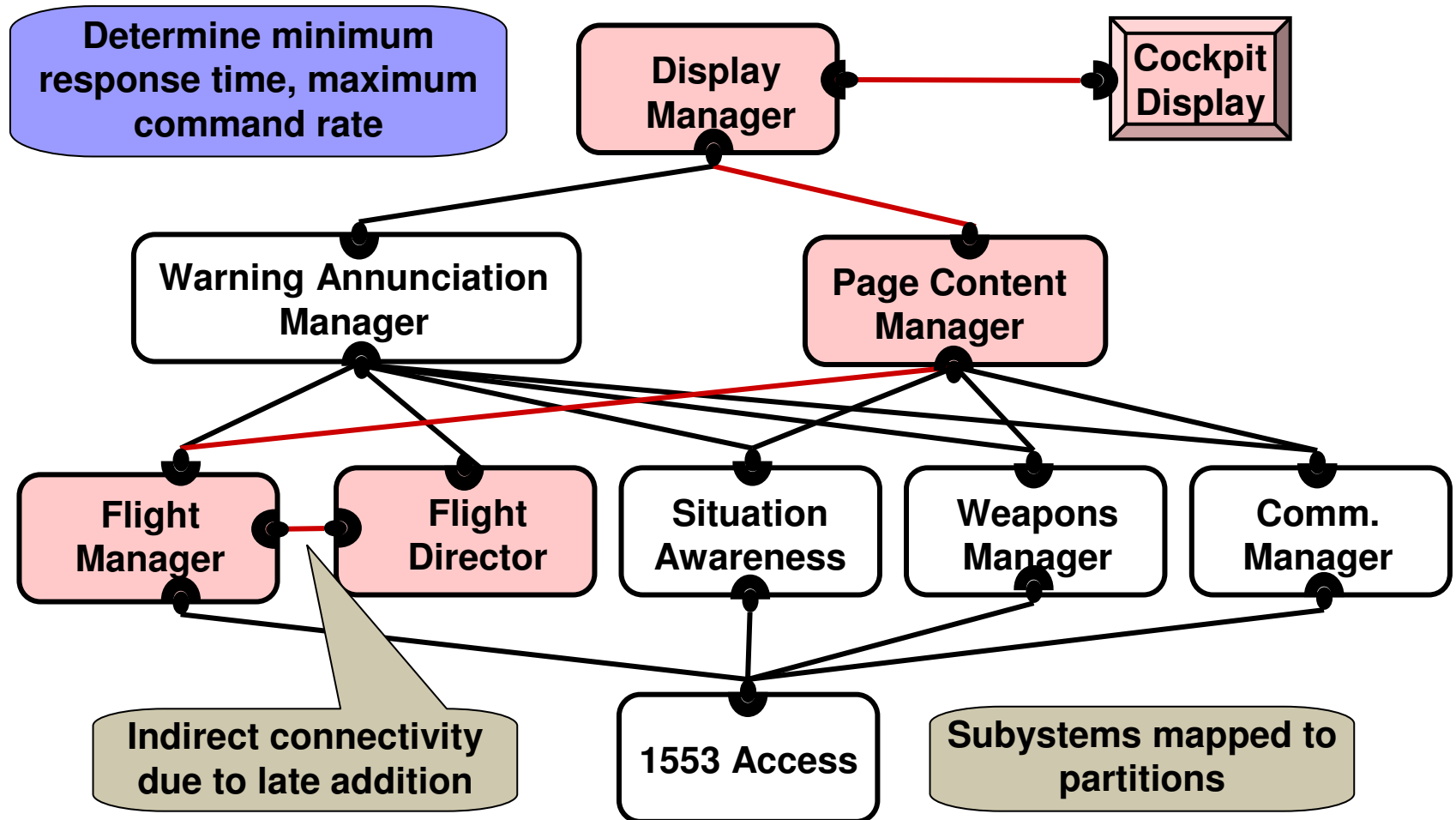


Outline

- Model-based Embedded System Engineering
- Resource Consumption: Resource Budgeting
- Real-time Performance: Concurrency & Timing
- ➔ Real-time Performance: End-to-end Latency
- Security: Confidentiality Analysis
- Data Quality: Temporal Data Consistency



High-level Flow Analysis





Response Time Analysis Demo

- High-level end-to-end analysis
 - Account for latency impact of partition hops
 - Account for device latency
 - Account for subsystem processing
- Detailed end-to-end latency analysis
 - AADL model from design data base
 - Task model with 165 end-to-end flows



Outline

- Model-based Embedded System Engineering
- Resource Consumption: Resource Budgeting
- Real-time Performance: Concurrency & Timing
- Real-time Performance: End-to-end Latency
- ➔ Security: Confidentiality Analysis
- Data Quality: Temporal Data Consistency




Security Analysis

- Security levels & information flow
 - Components with security levels
 - Security levels & containment hierarchy
 - Security levels and connections
 - Security levels & execution platform components
- Full scale security models
 - Bell LaPadula
 - Chinese Wall
- Safety criticality & control of components
 - Component have safety criticality levels
 - Impact on high criticality components



Outline

- Model-based Embedded System Engineering
 - Resource Consumption: Resource Budgeting
 - Real-time Performance: Concurrency & Timing
 - Real-time Performance: End-to-end Latency
 - Security: Confidentiality Analysis
-  Data Quality: Temporal Data Consistency



Performance Improvement Gone Bad

A real customer experience

- Ground station to accommodate sensor load growth
 - Reduce load in network
 - Two subsystems communicate state change instead of state
- The impact
 - Other subsystems increase network load sporadically
 - Receiving subsystem goes down
- The cause
 - Transmission protocol without guaranteed delivery
 - Overload result in dropping of transmitted state deltas
 - Missing deltas result in inconsistent receiver state



Avoiding Future Mistakes

- Relevant characteristics as properties
 - State vs. state-change communication through ports
 - Bus protocols with or without guaranteed delivery
- Annotating the model
 - Application engineer characterizes data stream
 - Embedded system engineer characterizes hardware & protocols
- The analysis tool
 - Check that connections carrying state changes are bound to buses with guaranteed delivery



Capturing Domain Characteristics

- Domain types & base types
- Data value range and units of measurement
- Bounds on value deltas
- Data stream characteristics
 - Computational error
 - Miss rates
 - Freshness