New Developments in Model-Integrated Development of High-Confidence Software

Science of Integration for CPS Kickoff Meeting
11/29/2010

Joe Porter, Graham Hemingway, Nicholas Kottenstette,
Harmon Nine, Chris vanBuskirk,
Gabor Karsai, and Janos Sztipanovits

Institute for Software Integrated Systems
Vanderbilt University
Nashville, TN 37205

Overview: High-Confidence Embedded Software Design

I. Design working control system with Simulink-based model

II. Software design using ESMoL

III. Time-triggered schedule generation

IV. TrueTime platform simulation

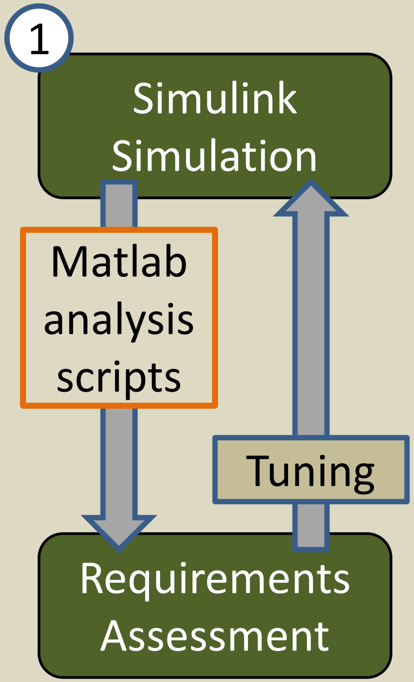
Workflow: Control Design

CONTROL DESIGN

SOFTWARE IMPLEMENTATION

SOFTWARE ANALYSIS

GENERATION & EXECUTION



Software Modeling

Platform Design

Scheduling

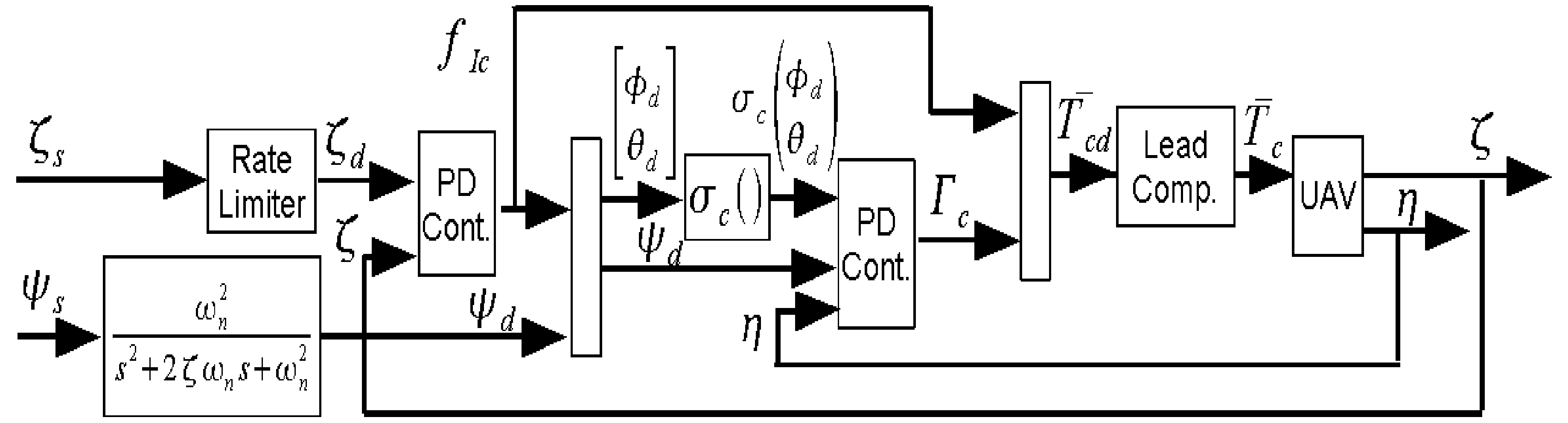
Deadlock

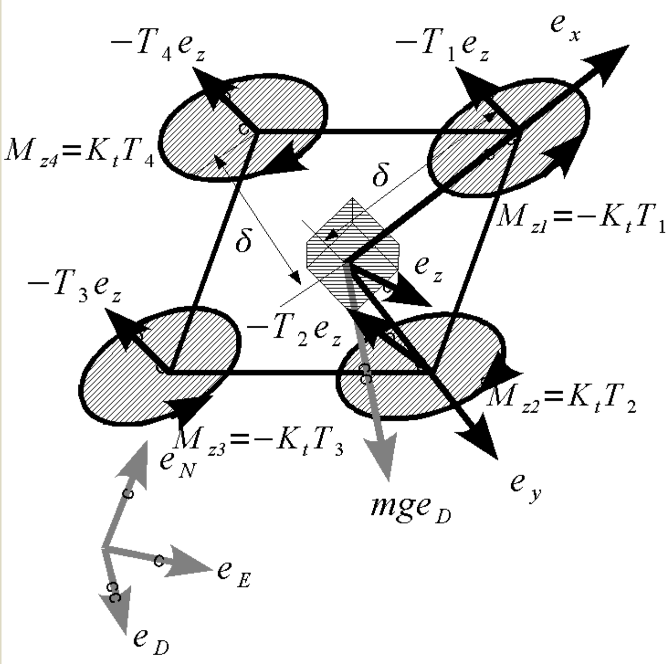
Platform/HIL Simulation

Testing

Control designers create Simulink and Stateflow models to capture and simulate the physical behavior as well as the engineering design. Design verification takes the form of scripts to assess controller performance (e.g. stability, settling time, overshoot) and adjust controller gains.

Quad-Rotor Cont. Subj. To Actuator Saturation





$$\dot{\zeta} = v_I$$

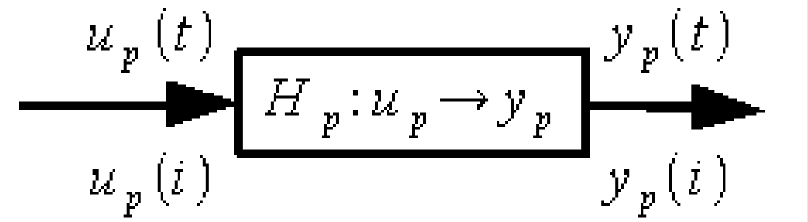
$$m\dot{v}_I = f_I = mge_D - TR^{\mathsf{T}}(\eta)e_Z$$

$$I\dot{\omega} = -\omega \times I\omega + \Gamma$$

$$\dot{\eta} = J(\eta)\omega$$

N. Kottenstette and J. Porter, "Digital passive attitude and altitude control schemes for quadrotor aircraft," ICCA09. http://www.isis.vanderbilt.edu/node/4051

Interior Conic Systems



Interior conic systems are inside the sector $[a, b]$

$$0 \le |a| < b \le \infty$$

$$\int_0^T y_p^T(t) y_p(t) dt - (a+b) \int_0^T y_p^T(t) u_p(t) dt + ab \int_0^T u_p^T(t) u_p(t) dt \le 0$$

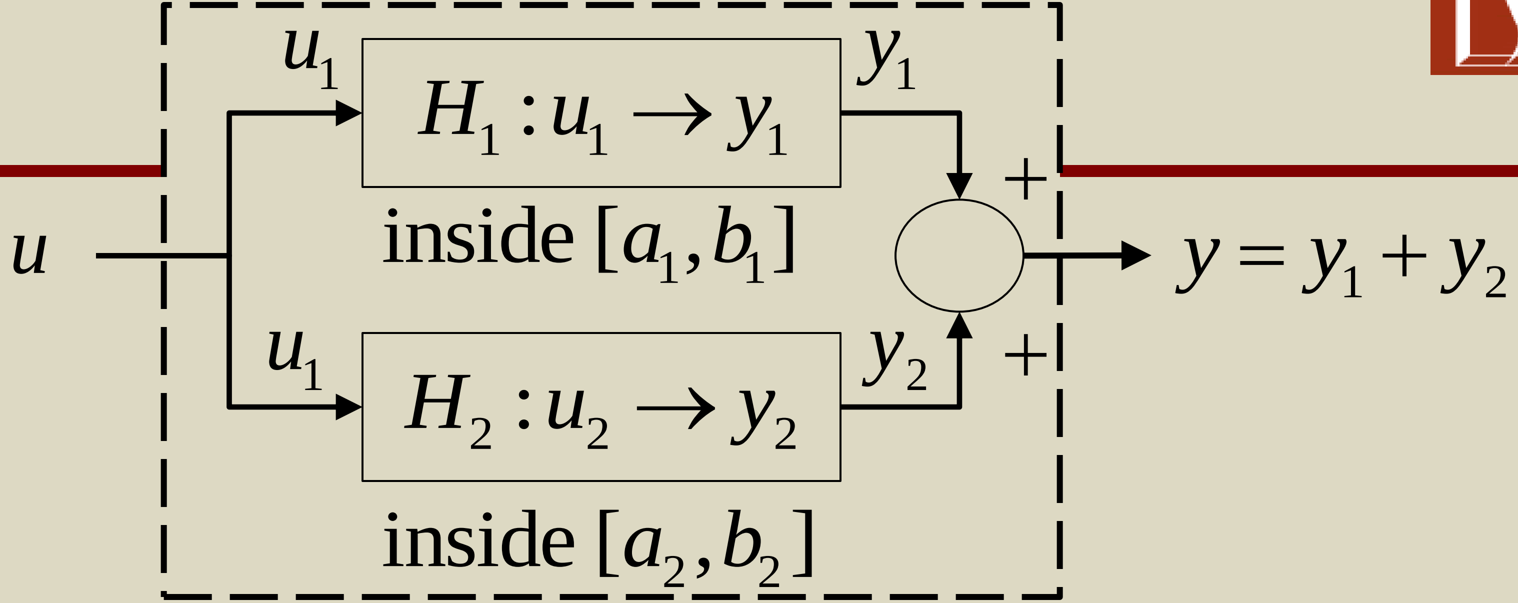
$$\| (y_p)_T \|_2^2 - (a_p + b_p) \left\langle y_p, u_p \right\rangle_T + a_p b_p \| (u_p)_T \|_2^2 \le 0$$

passive systems are inside the sector $[0, \infty]$,

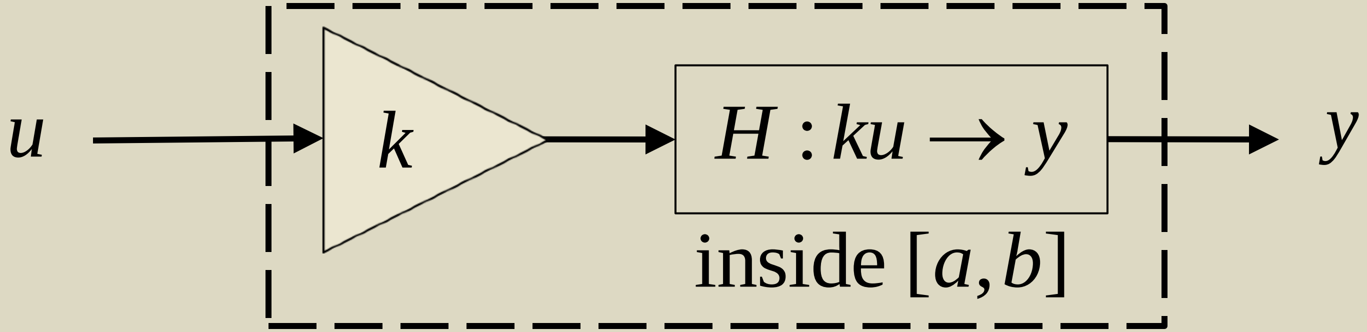
strictly input passive are inside the sector $[a, \infty] \quad a > 0$,

strictly output passive are inside the sector $[0, b] \quad b < \infty$.

Properties: Interior Conic Systems



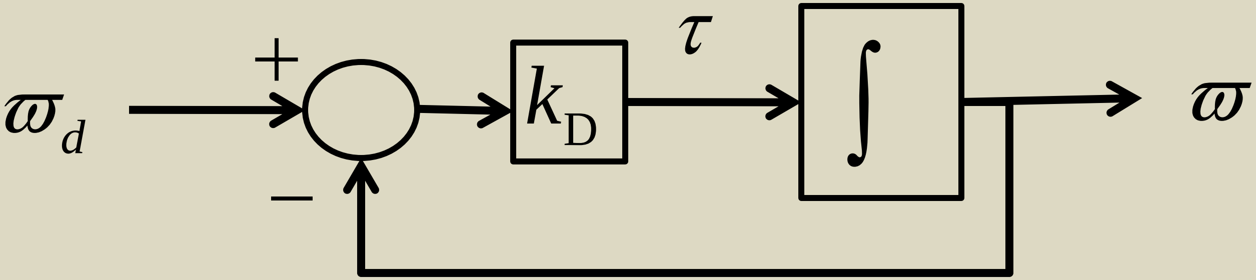
$H : u \rightarrow y$ inside the sector $\left[a_1 + a_2, b_1 + b_2\right]$



$H : u \rightarrow y$ inside the sector $\left[ka, kb\right]$, if $k > 0$

$H : u \rightarrow y$ inside the sector $\left[kb, ka\right]$, if $k < 0$

Non-linear control corollary with Nyquist Like Conditions



If $H : \tau \to \varpi$ is inside the sector $[a, b]$ $([0, \infty])$,

$|a| < b,\ 0 < b \leq \infty$ and the feedback law is

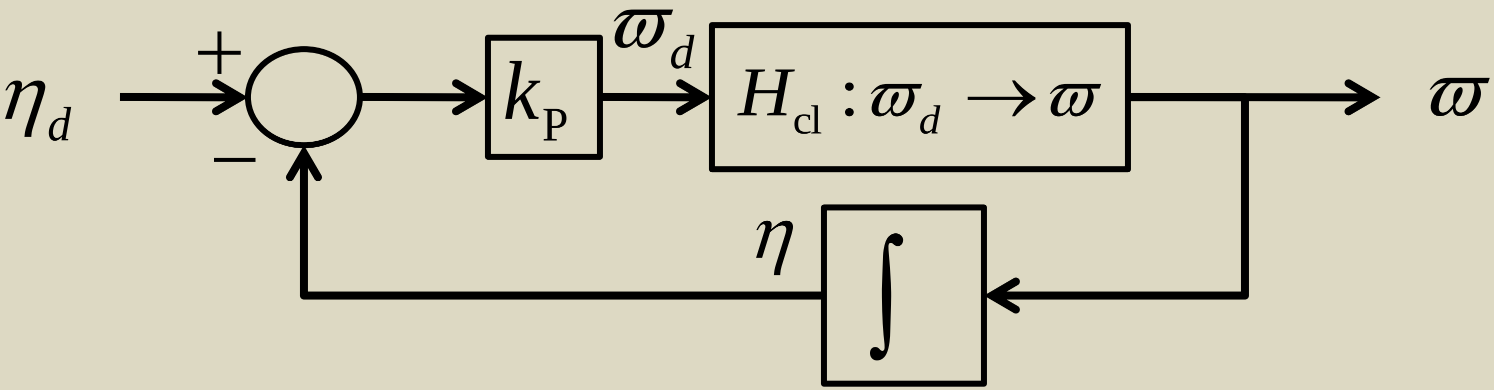
$\tau(t) = k_\mathrm{D}(\varpi_d(t) - \varpi(t))$ in which the gain satisfies:

$\frac{-1}{b} < k_\mathrm{D} < -\frac{1}{a}$ when $a < 0$;

$-\frac{1}{b} < k_\mathrm{D} < \infty$ when $a \geq 0$ then $H_\mathrm{cl} : \varpi_d \to \varpi$ is stable.

Classic Attitude/Robotic Control Structure

Next we observe that the following structure is also always stable.



If $H_{\mathrm{cl}} : \varpi_d \to \varpi$ is inside the sector $[0, b_{\mathrm{cl}}]$ $([0,1])$,

$0 < b_{\mathrm{cl}} < \infty$ and $H : \varpi \to \eta$ is inside the sector $[0, b]$ $([0,\infty])$,

$0 < b \leq \infty$ and the feedback law is $\varpi_d(t) = k_{\mathrm{P}}(\eta_d(t) - \eta(t))$

in which the gain k_{P} satisfies $0 < k_{\mathrm{P}} < \infty$,

then the system is stable.

Assumption: Dissipative-Conic Systems

Denote: $H : u \to y$ for a continuous-time finite-state system whose input-output mapping can be determined from the following ode:

$$\dot{x}(t) = f(x(t)) + g(x(t))u(t),\ x \in \Re^n,\ u \in \Re^m,\ f(0) = 0$$

$$y(t) = h(x(t)) + J(x(t))u(t),\ y \in \Re^m,\ h(0) = 0.$$

In addition the system is reachable and zero-state detectable.

Definition: continuous-time conic-dissipative systems inside the sector [a,b]

If there exists a conic dissipative supply function $s(u, y) \in \Re$ for the continuous-time system $H : u \to y$ of the following form:

$$s(u, y) = \begin{cases} -y^{\mathrm{T}} y + (a+b) y^{\mathrm{T}} u - ab u^{\mathrm{T}} u, \text{ if } |a|, |b| < \infty, a < b \\ y^{\mathrm{T}} u - a u^{\mathrm{T}} u, \text{ if } |a| < \infty, b = \infty. \end{cases}$$

such that

$\int_0^T s(u, y) dt \geq 0$ holds for all $T \geq 0$ then $H : u \to y$ is a conic-dissipative system inside the sector $\left[a, b\right]$.

Properties: Dissipative-Conic Systems

If $H : u \to y$ is a dissipative-conic system inside the sector $[a, b]$ then there exists a storage function

$V(x) > 0,\ x \in \Re^n$,V(0)=0, such that

$\dot{V}(x) \leq s(u, y)$

therefore if :

$b = \infty, |a| < \infty$, then $H : u \to y$ is stable.

$|a| < b < \infty$, then $H : u \to y$ is asymptotically stable.

Quad-Rotor Equations of Motion

$$m\dot{v}_I = f_I = mge_D - TR^{\mathrm{T}}(\eta)e_Z$$

$$I\dot{\omega} = -(\omega\times)I\omega + \Gamma$$

$$\dot{\eta} = J(\eta)\omega$$

$$\omega = [p,q,r]^T, \quad (\omega\times) = \begin{bmatrix} 0 & -r & q \\ r & 0 & -p \\ -q & p & 0 \end{bmatrix}, \quad J(\eta) = \begin{bmatrix} 1 & \sin(\phi)\tan(\theta) & \cos(\phi)\tan(\theta) \\ 0 & \cos(\phi) & -\sin(\phi) \\ 0 & \dfrac{\sin(\phi)}{\cos(\theta)} & \dfrac{\cos(\phi)}{\cos(\theta)} \end{bmatrix}$$

$$\eta = [\phi,\theta,\psi]^T, \quad R(\eta) = \begin{bmatrix} c_\theta c_\psi & c_\theta s_\psi & -s_\theta \\ s_\phi s_\theta c_\psi - c_\phi s_\psi & s_\phi s_\theta s_\psi + c_\phi c_\psi & c_\theta s_\phi \\ c_\phi s_\theta c_\psi + s_\phi s_\psi & c_\phi s_\theta s_\psi - s_\phi c_\psi & c_\theta c_\phi \end{bmatrix}$$

$$R^T(\eta)R(\eta) = I, \quad \dot{R}(\eta) = -(\omega\times)R(\eta), \quad \omega_I = R^T(\eta)\omega$$

Rigid Body Rotational Dynamics Are Passive

$$\text{Recall: } \mathrm{I}\dot{\omega} = (\omega\times)I\omega + \Gamma$$

$$\text{Denote } y = kI\omega \text{ in which k=(}\frac{1}{\max\left\{I_{(1,1)}, I_{(2,2)}, I_{(3,3)}\right\}}\text{) s.t. } \omega = \frac{1}{k}I^{-1}y$$

$$\text{Choose the Storage Function: } V(y) = \frac{1}{2k}y^{\mathrm{T}}y > 0, y \neq 0$$

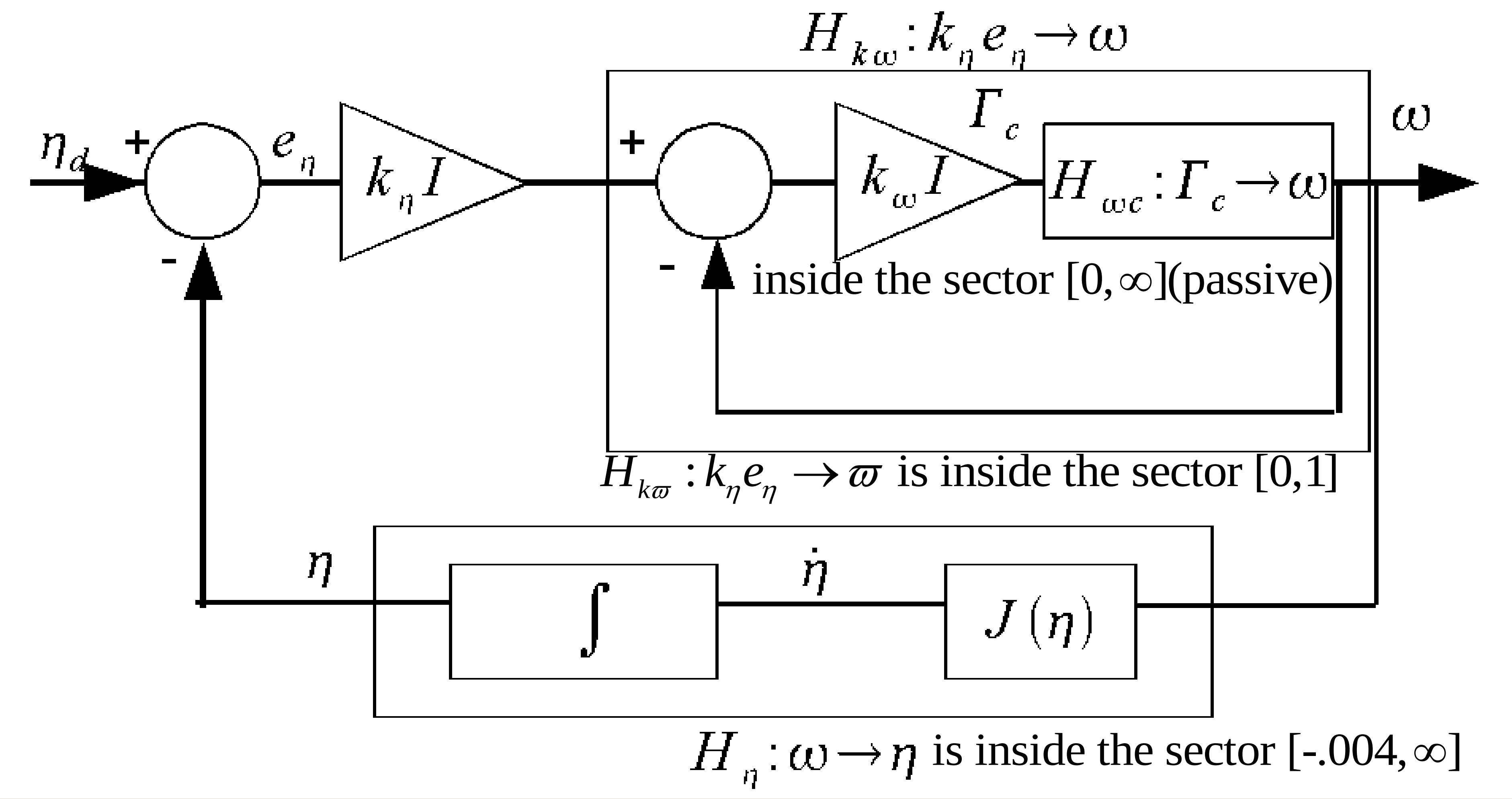
$$\dot{V}(y) = y^{\mathrm{T}}\dot{y} = y^{\mathrm{T}}(\frac{1}{k}I^{-1}y\times)y + y^{\mathrm{T}}\Gamma$$

$$\text{Recall that: } (\frac{1}{k}I^{-1}y\times) = -(\frac{1}{k}I^{-1}y\times)^{\mathrm{T}}$$

$$\text{therefore } \dot{V}(y) = y^{\mathrm{T}}\Gamma$$

Which is a lossless passive system (inside the sector $[0,\infty]$).

Attitude PD Control Subsystem



$H_{k\omega} : k_\eta e_\eta \to \omega$

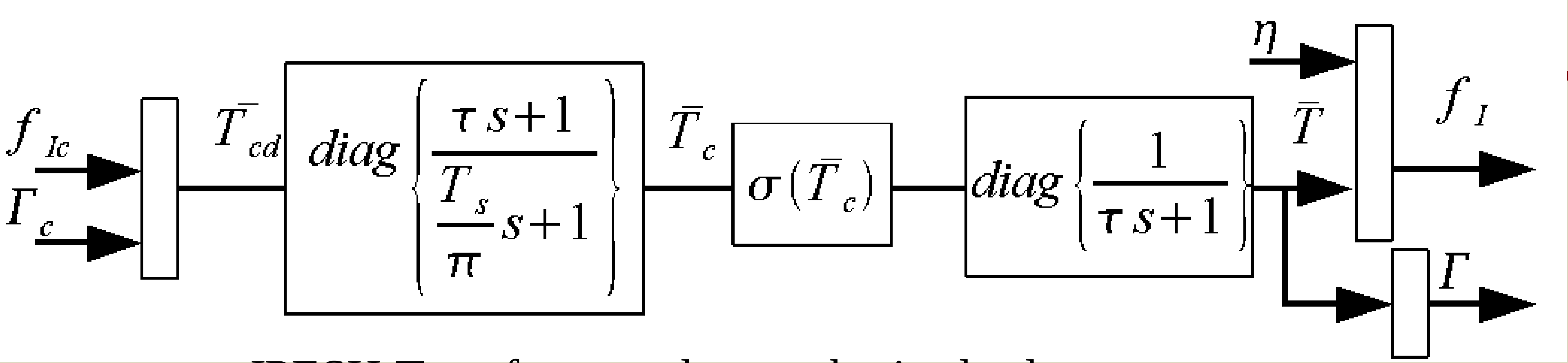
inside the sector $[0, \infty]$(passive)

$H_{k\varpi} : k_\eta e_\eta \to \varpi$ is inside the sector $[0,1]$

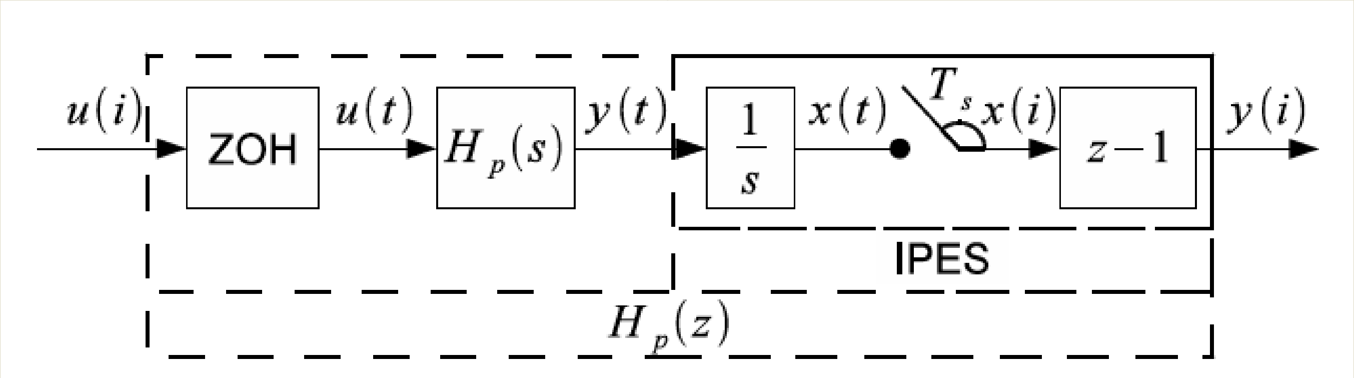
$H_\eta : \omega \to \eta$ is inside the sector $[-.004, \infty]$

NB: $J(\eta) > 0, \phi, \theta \in [-\frac{29}{90}\pi, \frac{29}{90}\pi], \psi \in [-\pi, \pi]$

Lead-Compensator, Thrust Mapping



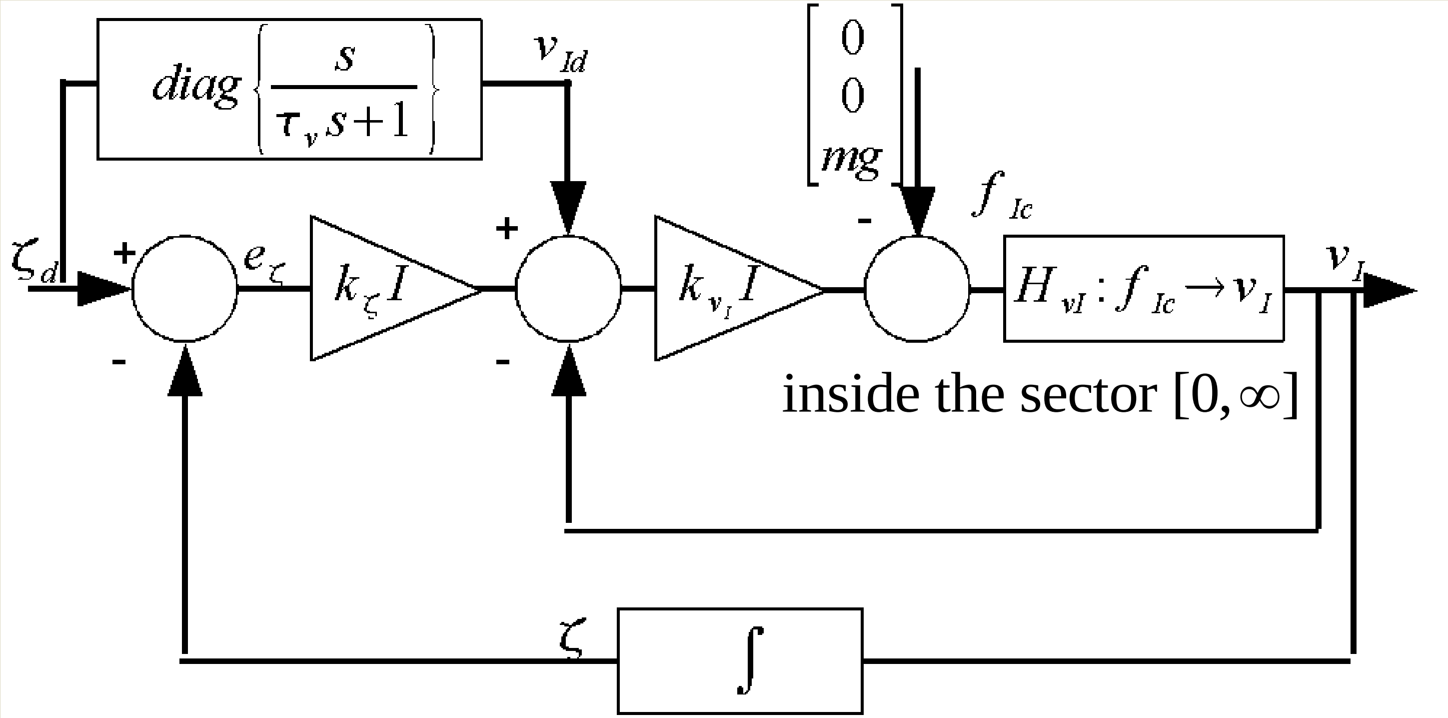
IPESH-Transform used to synthesize lead-compensators.



$$T = -f_{Icz}, \quad \begin{bmatrix} \phi_{\text{set}} \\ \theta_{\text{set}} \end{bmatrix} = \begin{bmatrix} s_\psi & -c_\psi \\ c_\psi & s_\psi \end{bmatrix} \begin{bmatrix} \frac{f_{Icx}}{f_{Icz}} \\ \frac{f_{Icy}}{f_{Icz}} \end{bmatrix}, \quad \begin{bmatrix} T_1 \\ T_2 \\ T_3 \\ T_4 \end{bmatrix} = \begin{bmatrix} 0 & -\delta & 0 & \delta \\ \delta & 0 & -\delta & 0 \\ -K_t & K_t & -K_t & K_t \\ 1 & 1 & 1 & 1 \end{bmatrix}^{-1} \begin{bmatrix} \gamma_x \\ \gamma_y \\ \gamma_z \\ T \end{bmatrix}$$

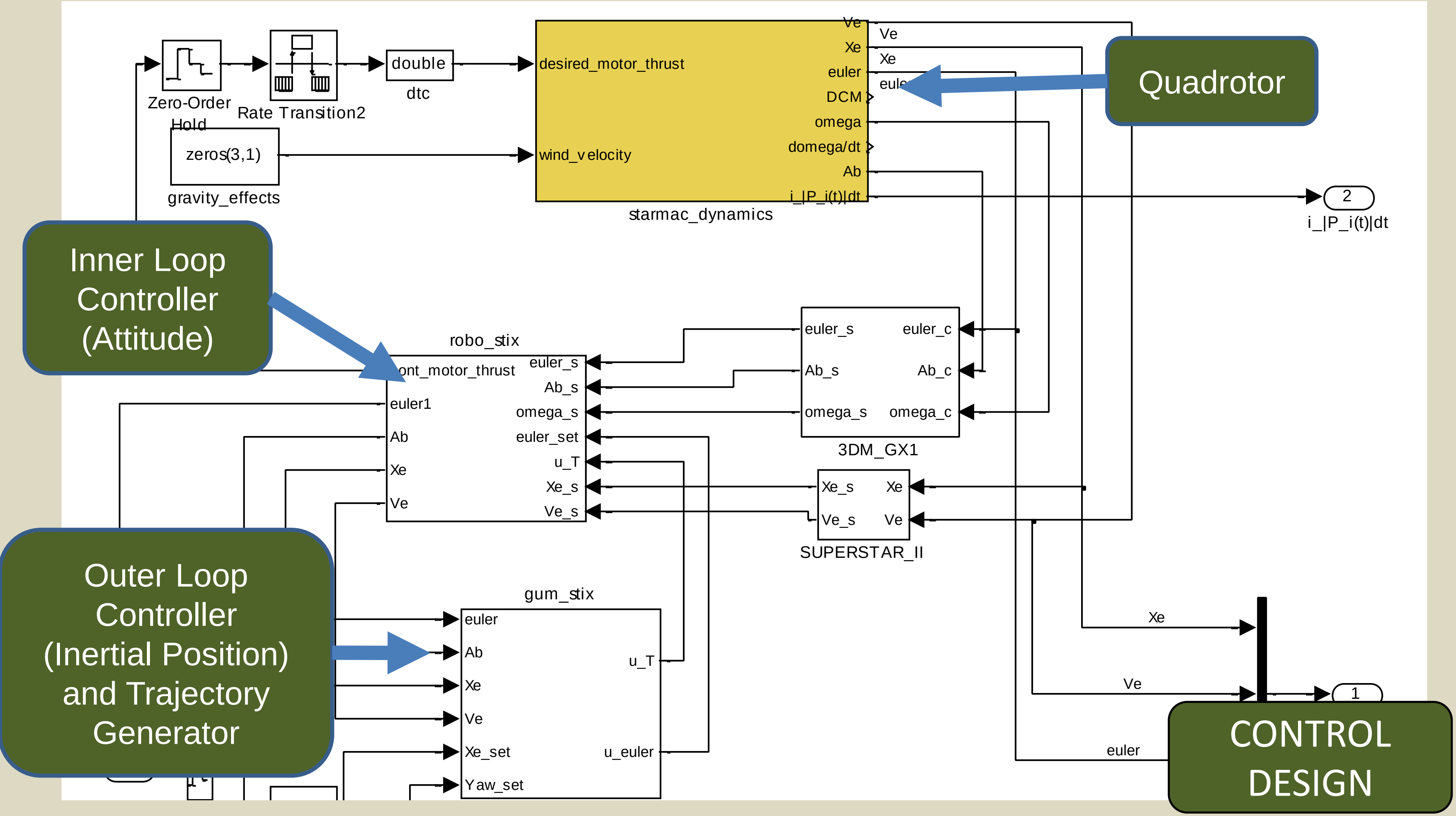
Inertial PD Control Subsystem

IPESH-Transform used



inside the sector $[0, \infty]$

Quadrotor: Simulink



Quadrotor

Inner Loop Controller (Attitude)

Outer Loop Controller (Inertial Position) and Trajectory Generator

CONTROL DESIGN

Workflow: Import Control Design to ESMoL

CONTROL DESIGN

SOFTWARE IMPLEMENTATION

SOFTWARE ANALYSIS

GENERATION & EXECUTION

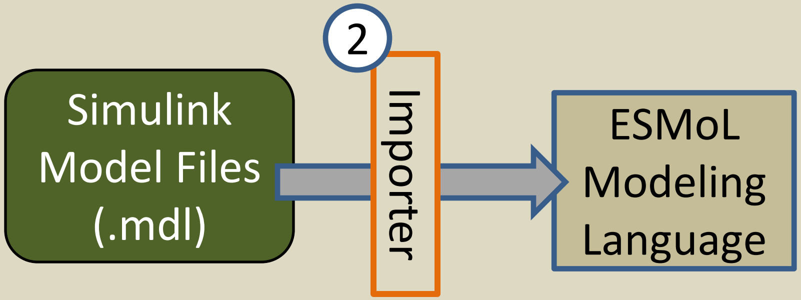
Software Modeling (Arch/Deployment)

Scheduling

Platform/HIL Simulation

Deadlock

Testing

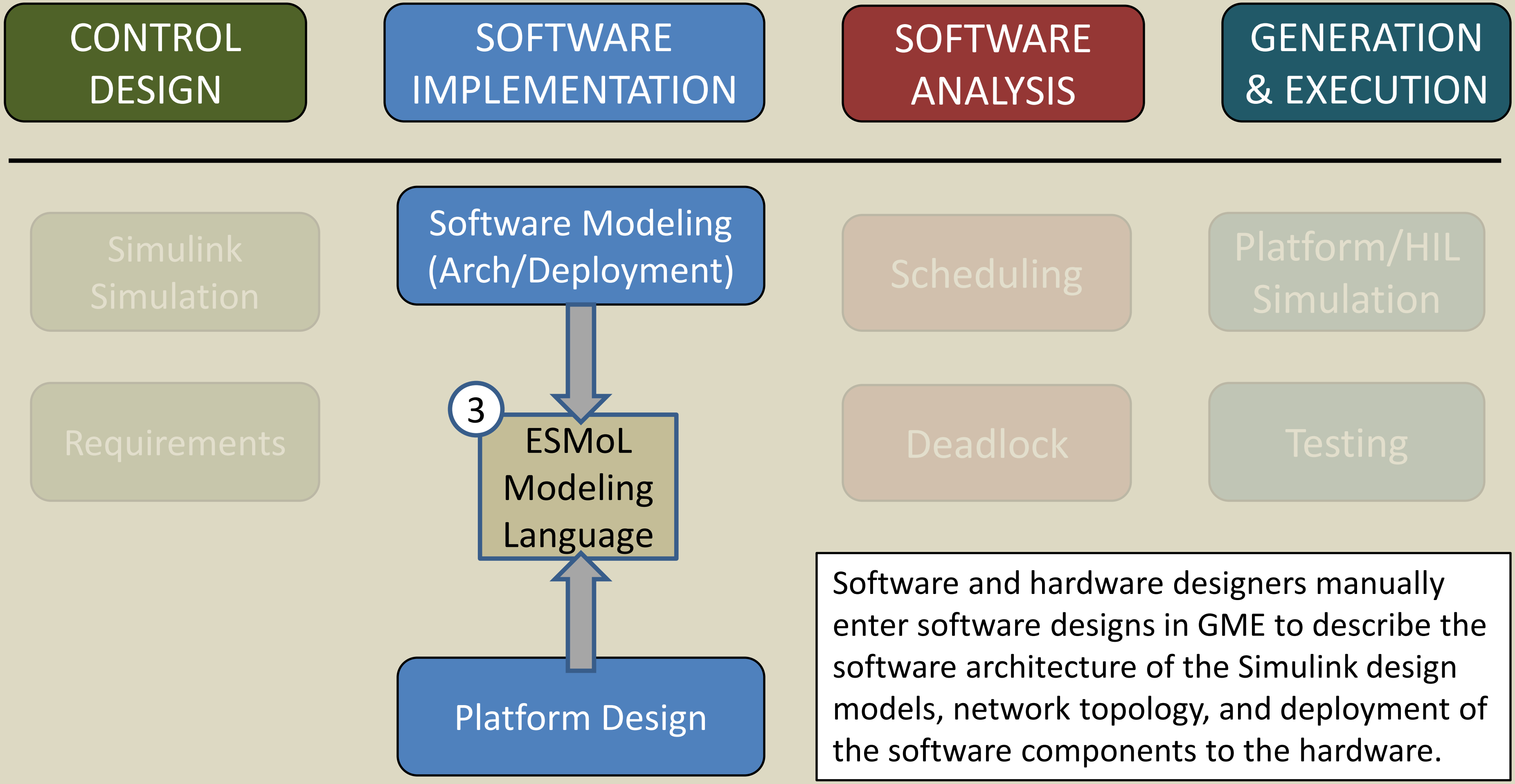


Requirements

Platform Design

The ESMoL domain-specific modeling language (DSML) includes a sublanguage which fully represents Simulink and Stateflow model structures. The tools include a fully automated model importer.

Workflow: Software and Hardware Design



CONTROL DESIGN

SOFTWARE IMPLEMENTATION

SOFTWARE ANALYSIS

GENERATION & EXECUTION

Simulink Simulation

Requirements

Software Modeling (Arch/Deployment)

3

ESMoL Modeling Language

Platform Design

Scheduling

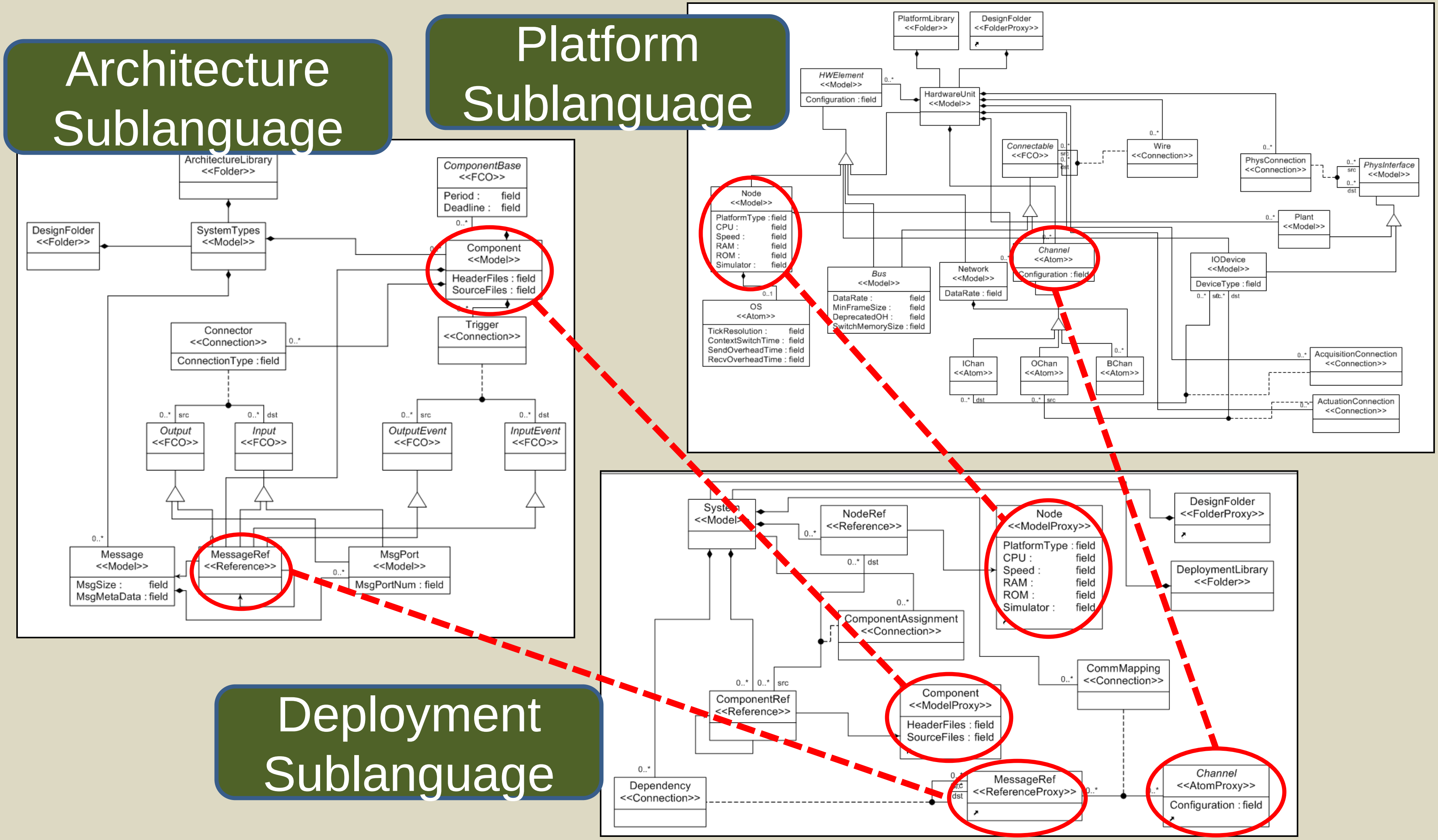
Deadlock

Platform/HIL Simulation

Testing

Software and hardware designers manually enter software designs in GME to describe the software architecture of the Simulink design models, network topology, and deployment of the software components to the hardware.

ESMoL Language: Model-Integrated Computing (MIC)

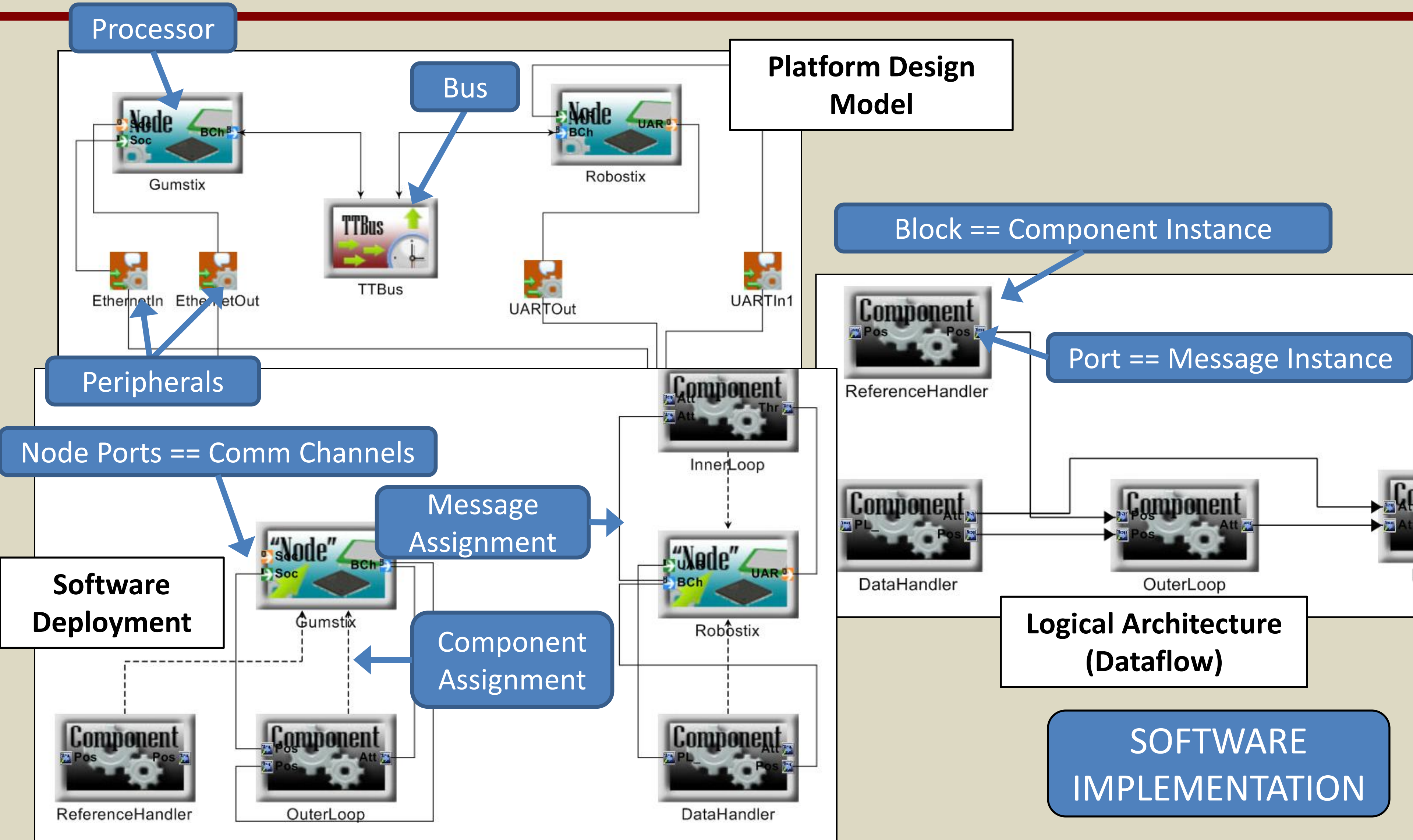


Architecture Sublanguage

Platform Sublanguage

Deployment Sublanguage

Quadrotor Software Design: GME & ESMoL



Processor

Bus

Platform Design Model

Block == Component Instance

Port == Message Instance

Peripherals

Node Ports == Comm Channels

Message Assignment

Component Assignment

Software Deployment

Logical Architecture (Dataflow)

SOFTWARE IMPLEMENTATION

Workflow: Software Analysis

CONTROL DESIGN

SOFTWARE IMPLEMENTATION

SOFTWARE ANALYSIS

GENERATION & EXECUTION

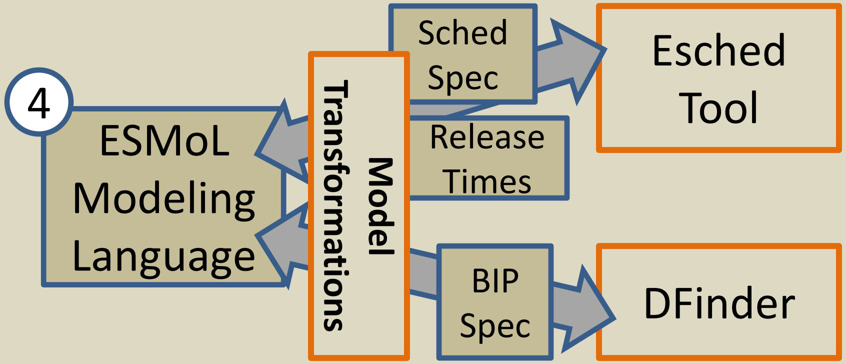
Simulink Simulation

Software Modeling (Arch/Deployment)

Scheduling

Platform/HIL Simulation

Requirements



Testing

Round-trip analysis is integrated into the tool environment.

Platform Design

Deadlock

Model interpreters generate scheduling specifications and import results. BIP analysis is under development.

Quadrotor: Schedule Verification and Generation

Schedule Specification

```
Resolution 5us

Proc RS 4MHz 0s 0s
Comp InnerLoop =50Hz 1ms
Comp DataHandling =50Hz 1ms
Comp ADC =50Hz 1us
Comp SerialIn =50Hz 1ms
Comp SerialOut =50Hz 1ms
Msg DataHandling.sensor_data 8B RS/ADC RS/DataHandling
Msg DataHandling.pos_ref 8B RS/SerialIn RS/DataHandling
Msg InnerLoop.thrust_commands 8B RS/InnerLoop RS/SerialOut
Msg LocalOrder 1B RS/DataHandling RS/InnerLoop


Proc GS 100MHz 0s 0s
Comp OuterLoop =50Hz 1ms

Bus TT_I2C 100kb 1ms
Msg OuterLoop.ang_ref 8B GS/OuterLoop RS/InnerLoop
Msg DataHandling.pos_msg 8B RS/DataHandling GS/OuterLoop
```

Calculated Schedule

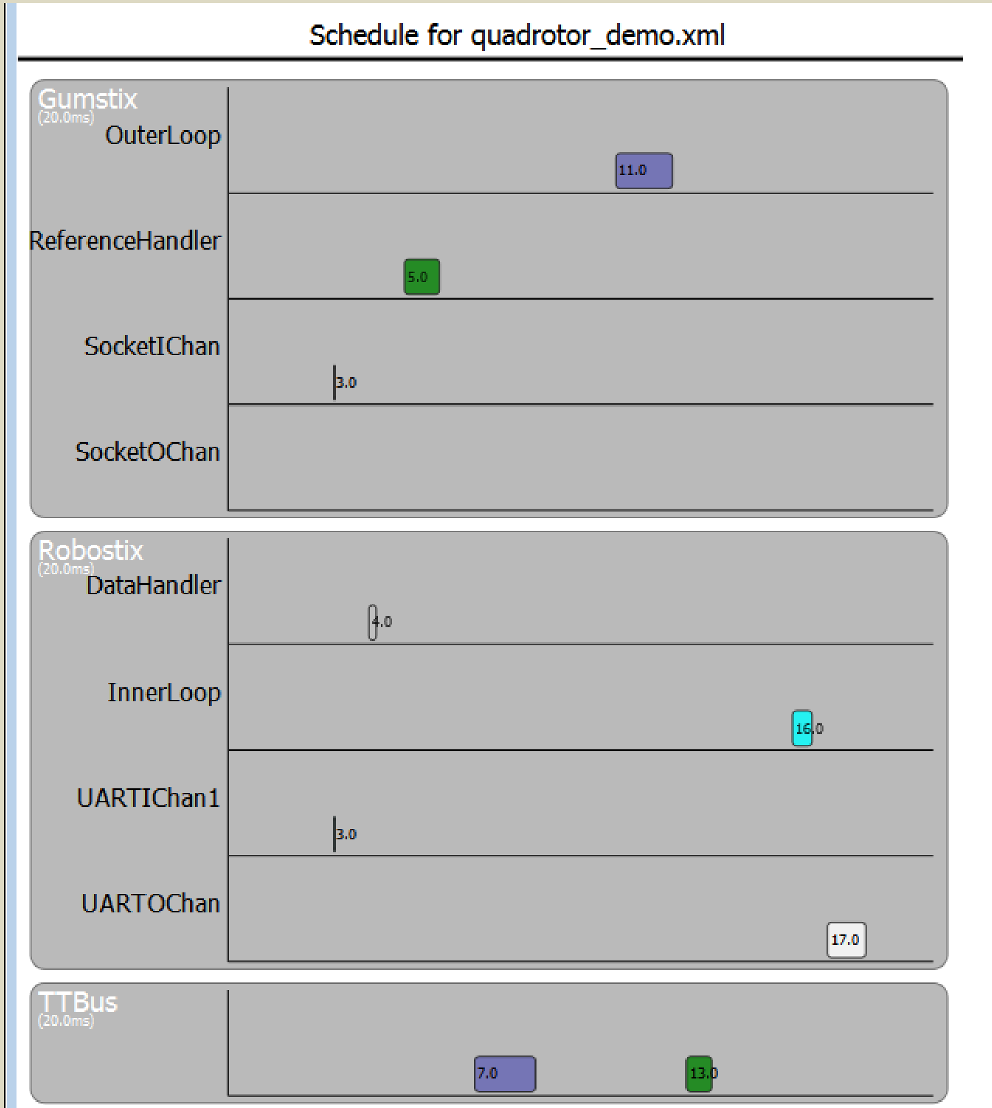
```
Hyperperiod 20 ms

TTBusSync 0
Gumstix/EthernetIn_0 3
Gumstix/ReferenceHandler_0 5
Gumstix/OuterLoop_0 11

TTBusSync 0
Robostix/UARTIn1_0 3
Robostix/DataHandler_0 4
Robostix/InnerLoop_0 16
Robostix/UARTOut_0 17

TTBusSync 0
TTBus/DataHandler.Pos_Data_msg_0 7
TTBus/OuterLoop.Att_Ref_msg_0 1
```

Schedule Visualization



Calculated Schedule

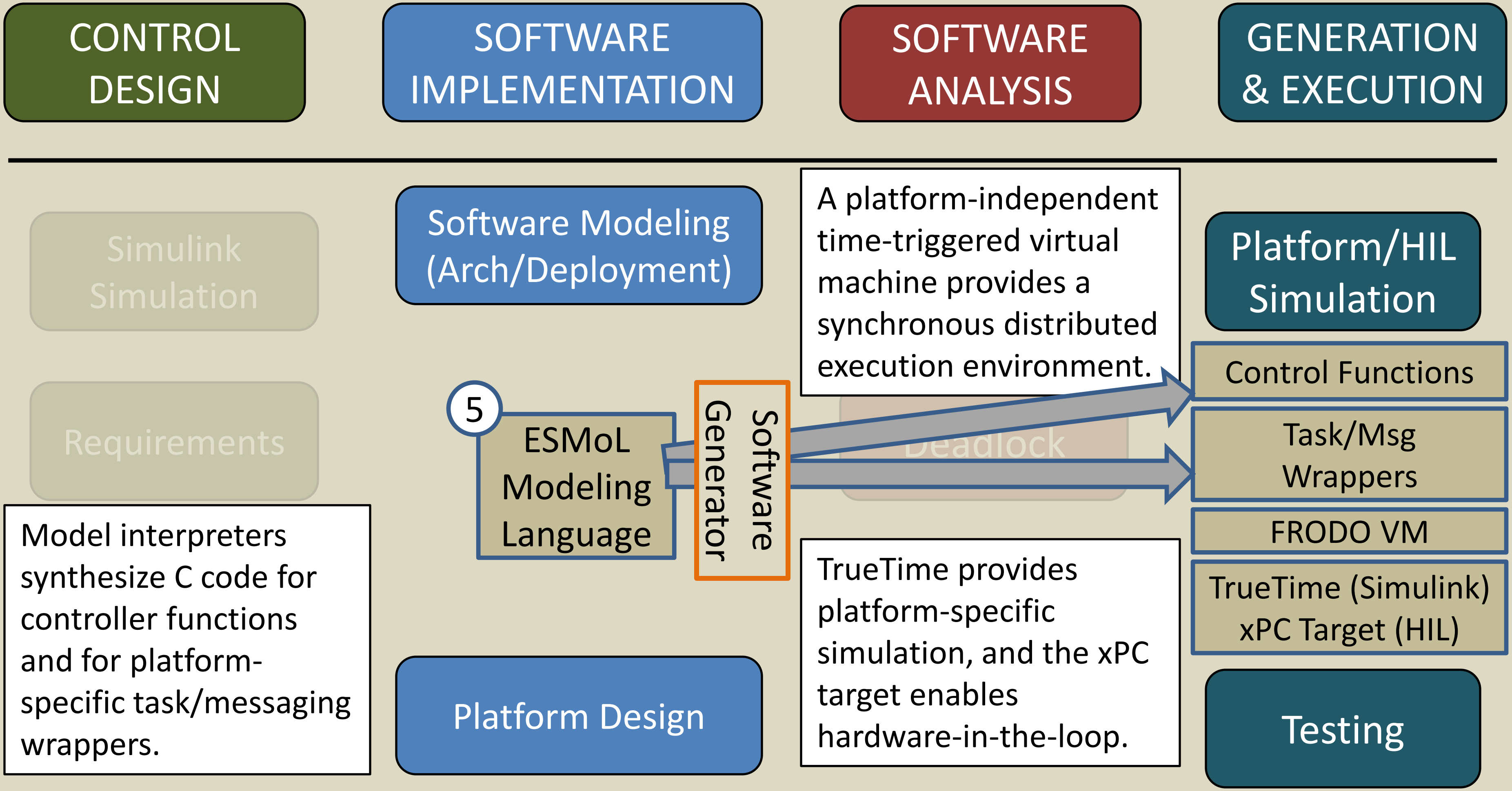
Hyperperiod 20 ms

TTBusSync 0
Gumstix/EthernetIn_0 3
Gumstix/ReferenceHandler_0 5
Gumstix/OuterLoop_0 11

TTBusSync 0
Robostix/UARTIn1_0 3
Robostix/DataHandler_0 4
Robostix/InnerLoop_0 16
Robostix/UARTOut_0 17

TTBusSync 0
TTBus/DataHandler.Pos_Data_msg_0 7
TTBus/OuterLoop.Att_Ref_msg_0 1

Workflow: Generation & Execution

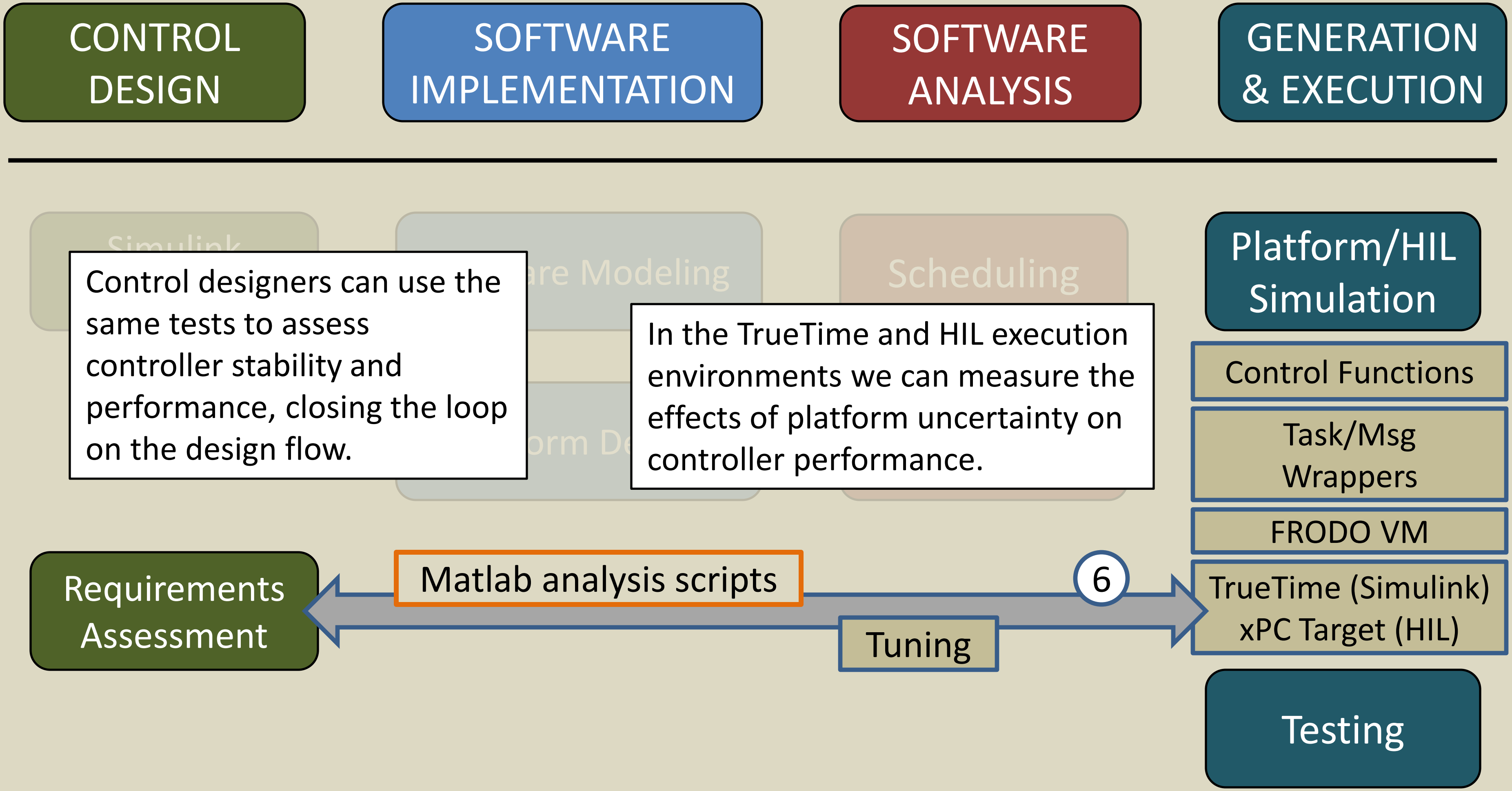


A platform-independent time-triggered virtual machine provides a synchronous distributed execution environment.

Model interpreters synthesize C code for controller functions and for platform-specific task/messaging wrappers.

TrueTime provides platform-specific simulation, and the xPC target enables hardware-in-the-loop.

Workflow: Assessment & Refinement (in progress)



CONTROL DESIGN

SOFTWARE IMPLEMENTATION

SOFTWARE ANALYSIS

GENERATION & EXECUTION

Simulink

are Modeling

Scheduling

orm De

Control designers can use the same tests to assess controller stability and performance, closing the loop on the design flow.

In the TrueTime and HIL execution environments we can measure the effects of platform uncertainty on controller performance.

Platform/HIL Simulation

Control Functions

Task/Msg Wrappers

FRODO VM

TrueTime (Simulink)
xPC Target (HIL)

Testing

Requirements Assessment

Matlab analysis scripts

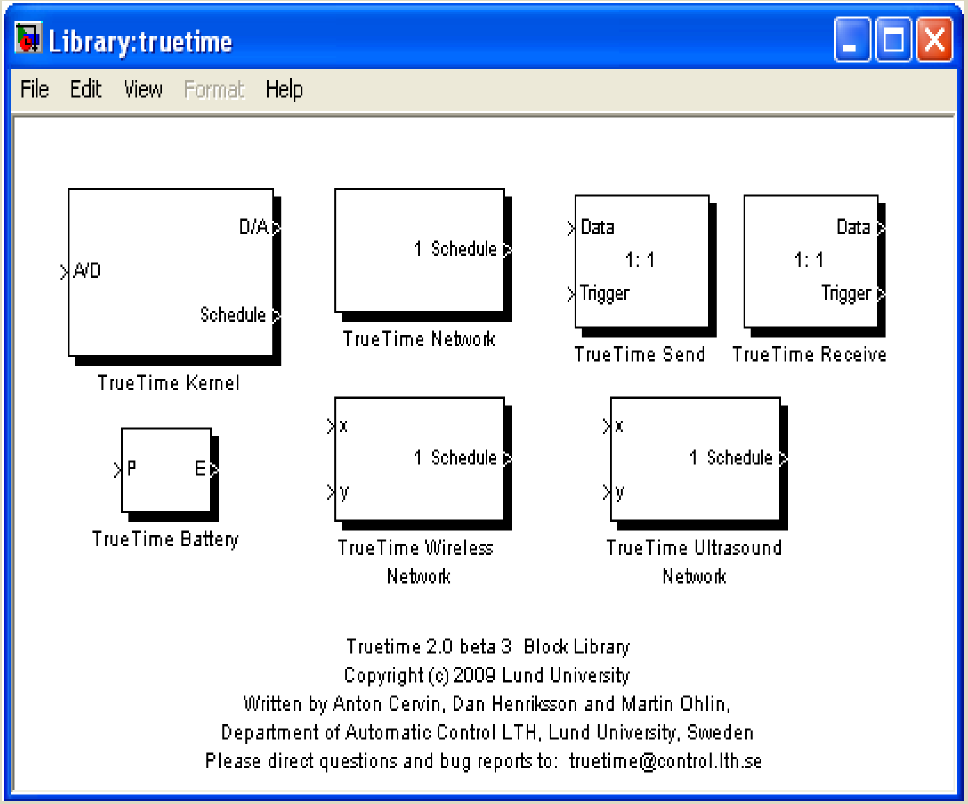
6

Tuning

TrueTime toolkit for Simulink

Set of Simulink blocks for simulating task scheduling and execution and network communication.

- Task-level execution
- Diverse & detailed network models
- C++/M-code/SL-block integration
- Highly flexible on-line scheduler + API
- Standard Simulink visualization of schedule execution



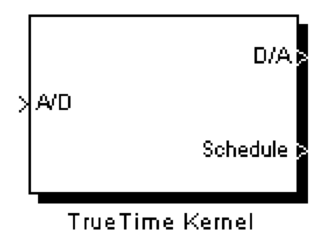
Truetime 2.0 beta 3 Block Library
Copyright (c) 2009 Lund University
Written by Anton Cervin, Dan Henriksson and Martin Ohlin,
Department of Automatic Control LTH, Lund University, Sweden
Please direct questions and bug reports to: truetime@control.lth.se

Mapping ESMoL to TrueTime

There is a mapping from ESMoL model software & hardware elements to TrueTime blocks and code:

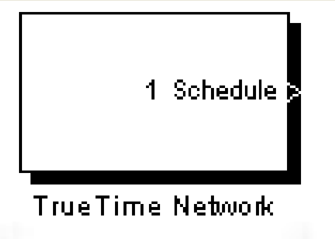
ESMoL Node

TT Kernel



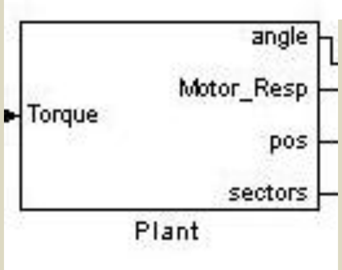
ESMoL Bus

TT Network



ESMoL Plant

Simulink Block

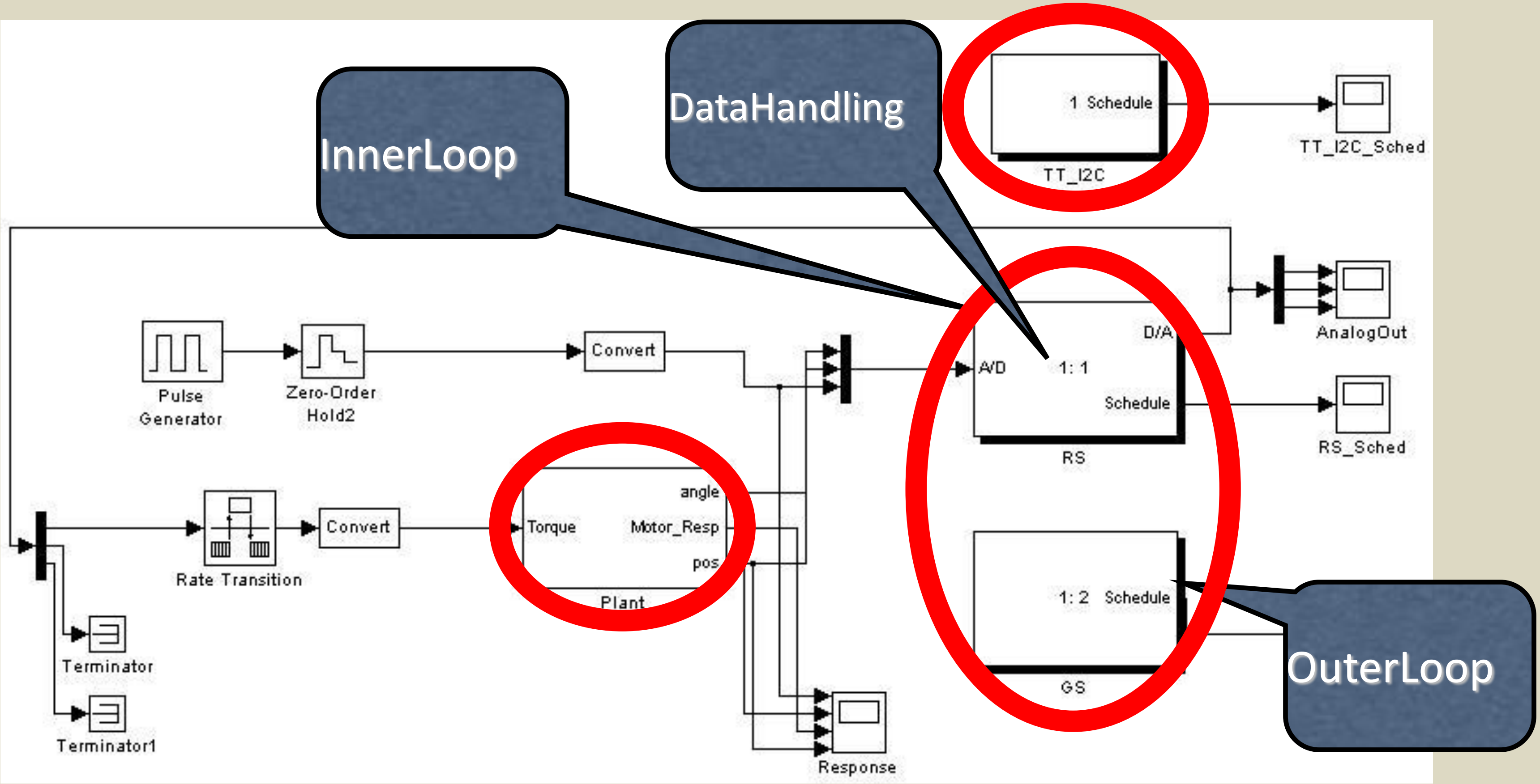


ESMoL Component

C-Code

TrueTime - New Model Synthesis

Based on the defined hardware configuration, a new Simulink model using TrueTime blocks and original plant block is created.



Questions?

Those interested in trying our tools can visit

https://wiki.isis.vanderbilt.edu/hcddes/index.php/The_ESMoL_Tool

References

[1] N. Kottenstette, J. Porter. Digital Passive Attitude and Altitude Control Schemes for Quadrotor Aircraft. IEEE 7th Intl. Conf. on Control and Automation (ICCA 2009). Christchurch, New Zealand, Dec. 2009.

[2] Porter, J., P. Volgyesi, N. Kottenstette, H. Nine, G. Karsai, and J. Sztipanovits, "An Experimental Model-Based Rapid Prototyping Environment for High-Confidence Embedded Software", Rapid System Prototyping (RSP'09), Paris, France, Jun. 2009.

[3] J. Porter, G. Hemingway, C. vanBusKirk, N. Kottenstette, G. Karsai, J. Sztipanovits. Online Dynamic Stability Verification Using Sector Search. ACM Intl. Conf. on Embedded Software (EMSoft) Grenoble, Oct. 2010.

[4] G. Hemingway, J. Porter, N. Kottenstette, H. Nine, C. vanBuskirk, G. Karsai, and J. Sztipanovits. Automated Synthesis of Time-Triggered Architecture-based TrueTime Models for Platform Effects Simulation and Analysis. Rapid Systems Prototyping (RSP), Jun. 2010.

[5] P. Zuliani, A. Platzer, E. M. Clarke. Bayesian Statistical Model Checking with Application to Stateflow/Simulink Verification. HSCC 2010 (Hybrid Systems: Computation and Control), Apr. 12-16, 2010, Stockholm, Sweden.

[6] LeBlanc, H., E. Eyisi, N. Kottenstette, X. Koutsoukos, and J. Sztipanovits, "A Passivity-Based Approach To Deployment In Multi-Agent Networks", Informatics in Control, Automation and Robotics (ICINCO 2010), Funchal, Madeira - Portugal, Jun. 2010.

[7] R. Thibodeaux. The Specification and Implementation of a Model of Computation. M.S. Thesis. Vanderbilt University, May 2008.

[8] N. Kottenstette, "Constructive Non-Linear Control Design With Applications to Quad-Rotor and Fixed-Wing Aircraft", Tech. Rpt., Inst. for Software Integrated Systems, Vanderbilt Univ., Jan. 2010. Nashville.

[9] S. Bensalem, M. Bozga, T. Nguyen, J. Sifakis: D-Finder: A Tool for Compositional Deadlock Detection and Verification. CAV 2009: 614-619