



INVESTIGAÇÃO, IDENTIFICAÇÃO E PROGNÓSTICOS DE ERROS DE SOFTWARE, FALHAS DE HARDWARE E COMPORTAMENTO DEGRADADO DE SISTEMAS ELETRÔNICOS EMBARCADOS

Projeto de Pesquisa apresentado a Universidade Federal de São Paulo - UNIFESP - para o concurso ao cargo de Professor(a) Adjunto(a) A, Nível I, Campus São José dos Campos, área/subárea: Engenharia Elétrica / Circuitos Eletrônicos e Controle de Processos Eletrônicos, Retroalimentação

Eloy Martins Oliveira Junior



Roteiro

- Apresentação
- Introdução e Justificativa
- Motivação
- Objetivos
- Resultados Esperados
- Meios e Métodos
- Recursos Necessários
- Disseminação e Avaliação
- Referências Bibliográficas

Apresentação

- Dr. Eloy Martins de Oliveira Junior
 - Engenheiro de Telecomunicações pela Universidade São Marcos – SP - 2007
 - Mestre em Engenharia e Tecnologia Espaciais / Mecânica Espacial e Controle – INPE – 2010
 - Estudo dos algoritmos welch-lynch (FTM), fault-tolerant average (FTA) e filtro de kalman (FK) para sincronização de relógios e suas influências sobre um sistema de controle.
 - Doutor em Engenharia e Tecnologia Espaciais / Mecânica Espacial e Controle – INPE – 2015
 - Estudo dos efeitos da sincronização sobre o transitório e a estabilidade de sistemas de controle por rede.

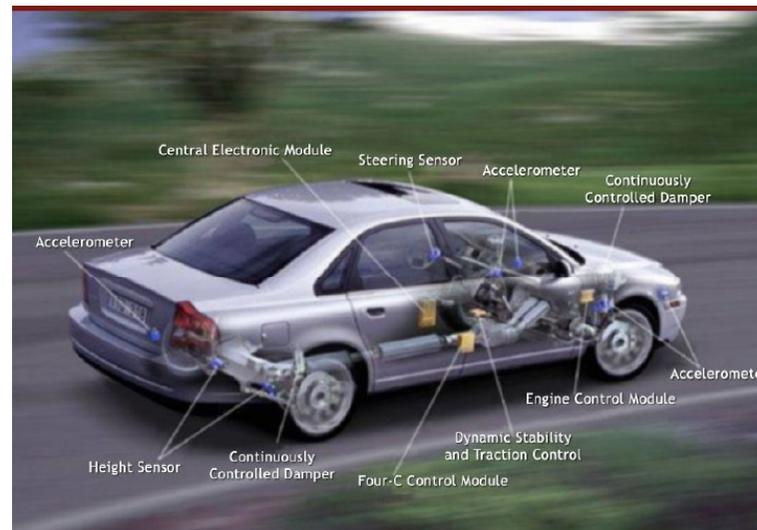
Apresentação

- Projetos de Pesquisas:
 - Integração de hardware para o Laboratório de Simulação (LabSim) para realização de testes do subsistema de ACDH (Controle de Atitude e Gerenciamento de Dados) dos satélites Amazônia 1 e Lattes
 - INPE – São José dos Campos/SP
 - Sistema de Apoio a Decisões Médicas (SADM) –
 - Konatus – São José dos Campos/SP

Introdução

- Sistemas embarcados estão cada vez mais sendo usados e tornando-se cada vez mais complexos e com alta integração da comunicação, da computação, do controle e elementos de informação, conhecidos como sistemas cibernético-físico.
- Estes sistemas alcançam altos níveis de dificuldade para o projeto e operação dos mesmos.
- Isso acontece com satélites, aviões, automóveis, redes inteligentes, interfaces homem-máquina, braços robóticos e outros.

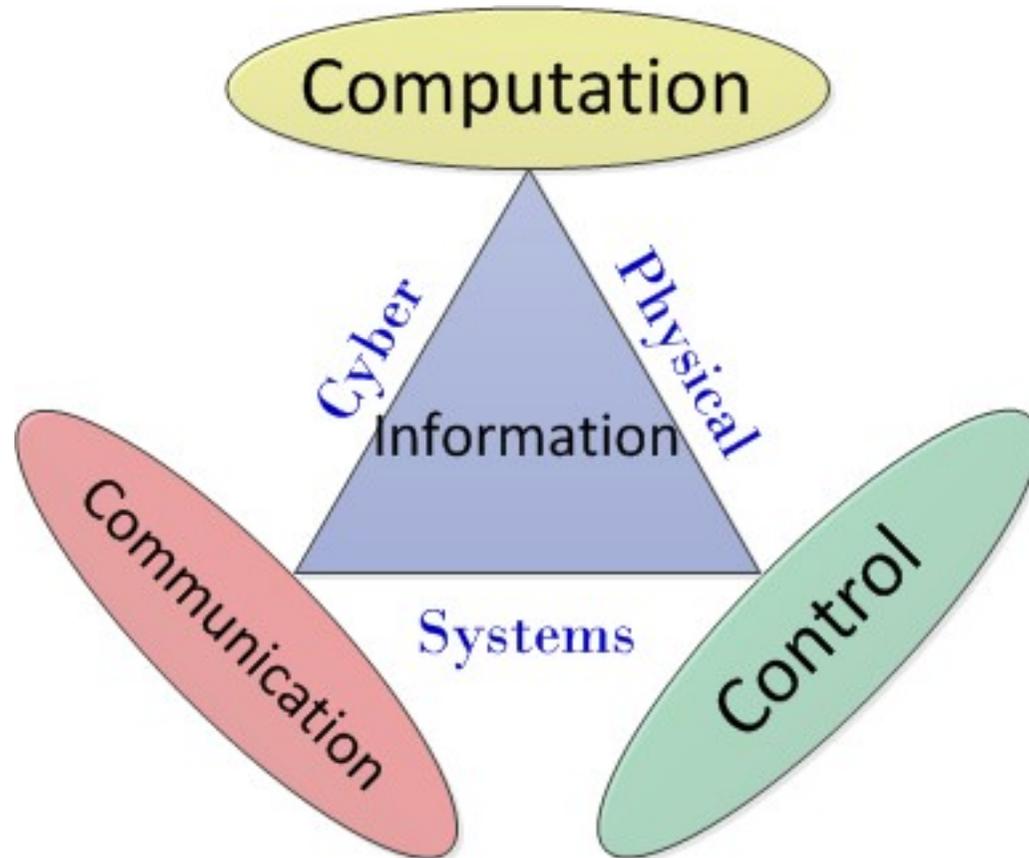
Introdução



90% da inovação são baseadas em sistemas embarcados!

[*Holistic Analysis and Optimization of Heterogeneous Fault-Tolerant Embedded Systems* - <https://www.slideshare.net/paupo/holistic-analysis-and-optimization-of-heterogeneous-faulttolerant-embedded-systems> - Acesso em 06/05/2017]

Introdução



Fonte: <http://www.intechopen.com/source/html/17868/media/image1.png>

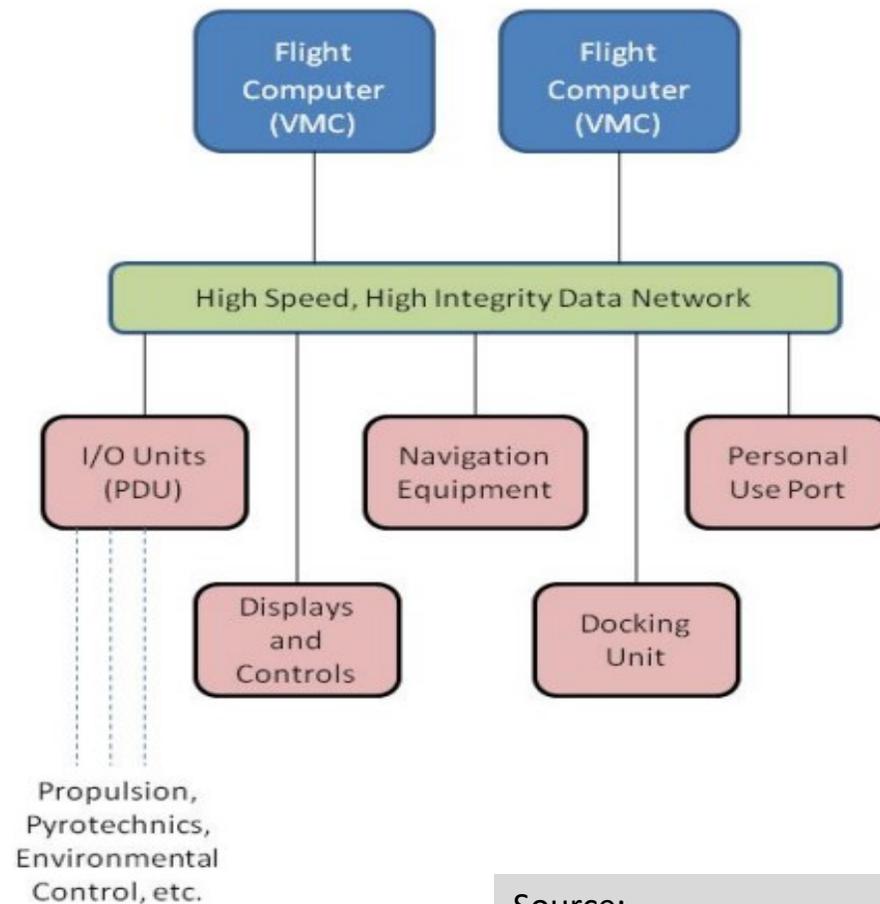
Introdução

- Com o crescimento do uso de sistemas cibernético-físicos embarcados, os problemas de erros de software, falhas de hardware e degradações de comportamento tem efeito sobre o sistema que são refletidos sobre a resposta dinâmica do sistema degradando:
 - Transitório;
 - Coordenação
 - Sincronização
 - Habilidades do sistema, tais como a estabilidade, controlabilidade, observabilidade e sensibilidade.

Exemplo Motivacional 1

- **Aeroespacial Orion**

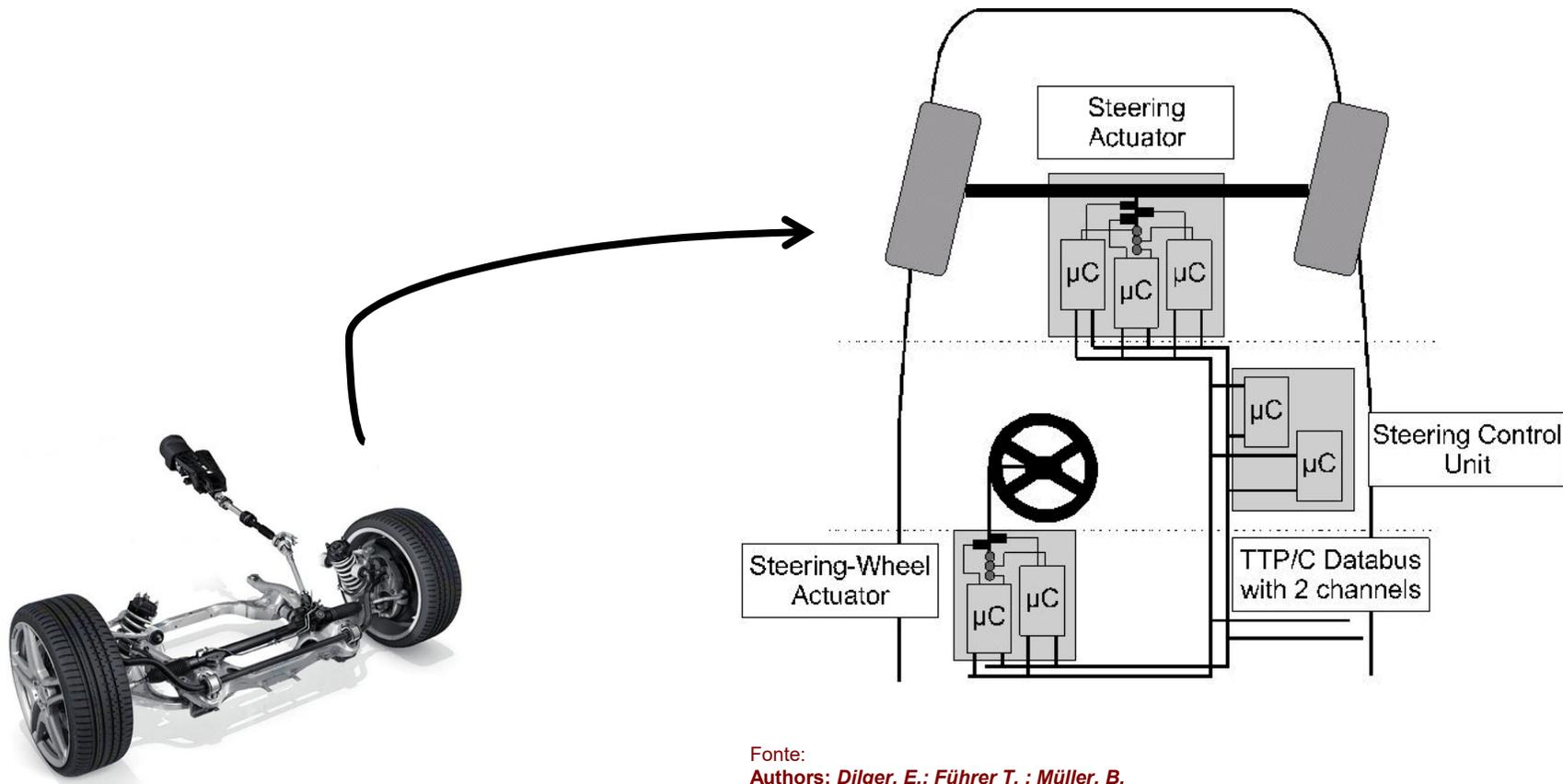
- *Veiculo de exploração espacial*
- *Rede de comunicação critica e sensivel ao tempo*
- *Protocolo TTEthernet*
- *Requer sincronização de tempo;*



Source:
Orion Mission

Exemplo Motivacional 2

- Automotivo – (*Steering-by-wire*) Direção por fio:



Fonte:

Authors: Dilger, E.; Führer T. ; Müller, B.

Paper: *The X-By-Wire Concept: Time-Triggered Information Exchange and Fail Silence Support by new System Services*

Site: <http://www.vmars.tuwien.ac.at/projects/xbywire/projects/new-bosch.htm>

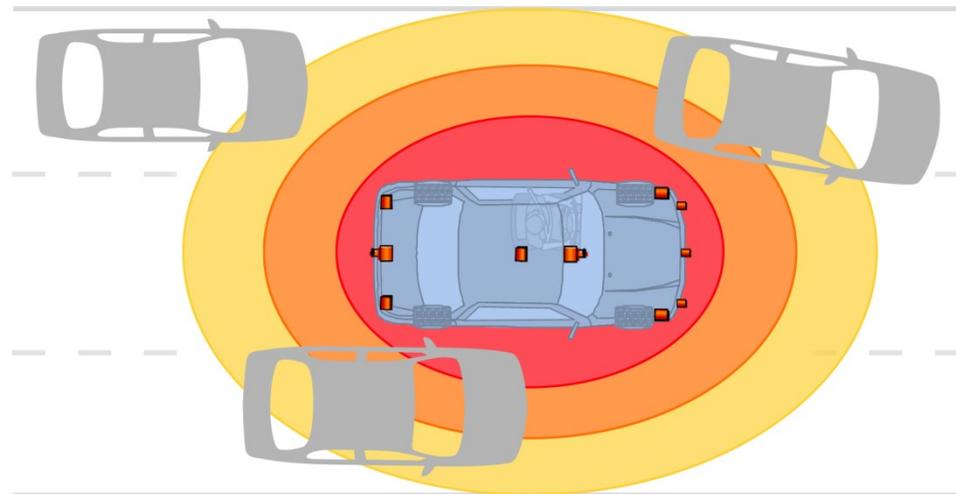
Exemplo Motivacional 3

- Automotivo – Direção Assistida



SENSOR FUSION HELPS DEVELOPMENT OF ACTIVE SAFETY, DRIVER ASSISTANCE SYSTEMS

Integrating cameras, radar, laser radar, sensors, GPS and digital mapping is intended to make drivers more aware and help avert crashes.

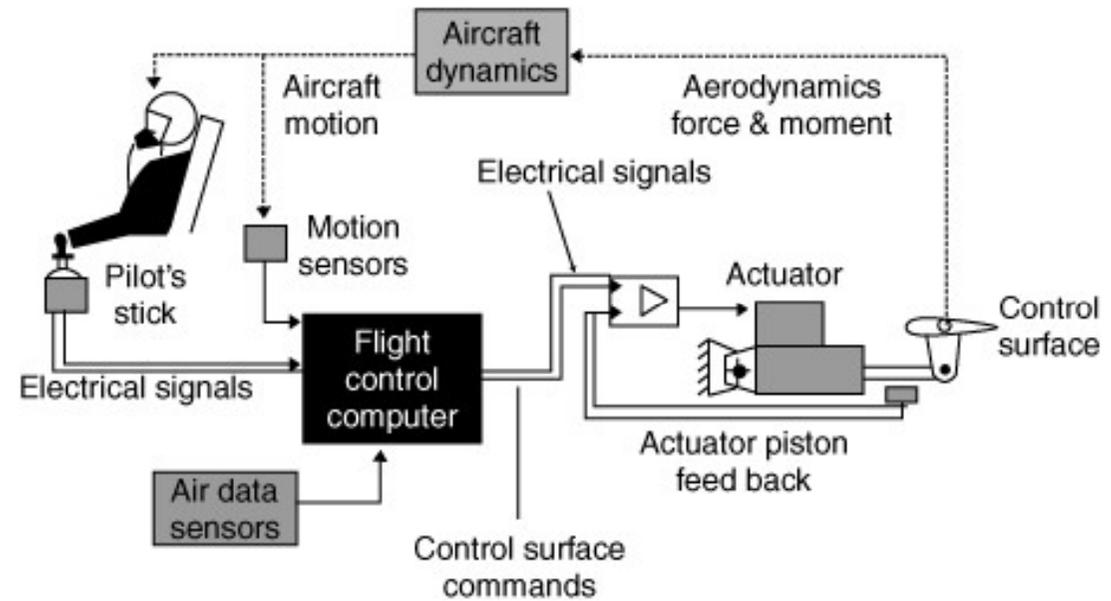
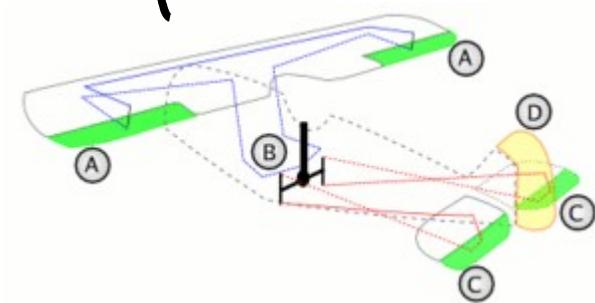


Fonte:

http://caddyinfo.com/wordpress/wp-content/uploads/2012/02/GM_SensorFusion.jpg

Exemplo Motivacional 4

- Aeronáutico
Fly-By-Wire



Fonte:
<http://airguardian.net/projects/fly-by-wire-project/>

Exemplo Motivacional 5

Software

Julho 2019

Airbus A350 software bug forces airlines to turn planes off and on every 149 hours

Patch your darn metal bird, sighs EU aviation agency

By Gareth Corfield 25 Jul 2019 at 10:02

160  SHARE ▼



An Airbus promotional picture of an A350-1000. Its sister type, the A350-941, is the affected model of airliner

Some models of Airbus A350 airliners still need to be hard rebooted after exactly 149 hours, despite warnings from the EU Aviation Safety Agency (EASA) first issued two years ago.

In a mandatory airworthiness directive (AD) reissued earlier this week, EASA urged operators to turn their A350s off and on again to prevent "partial or total loss of some avionics systems or functions".

Concerningly, the original 2017 AD was brought about by "in-service events where a loss of communication occurred between some avionics systems and avionics network" (sic). The impact of the failures ranged from "redundancy loss" to "complete loss on a specific function hosted on common remote data concentrator and core processing input/output modules".

Fonte: https://www.theregister.co.uk/2019/07/25/a350_power_cycle_software_bug_149_hours/

Março 2018

TESLA'S AUTOPILOT WAS INVOLVED IN ANOTHER DEADLY CAR CRASH



 TESLA

"The crash, in other words, was Brown's fault." "After Brown's death, Tesla modified Autopilot to rely more on data from its radar, and less on the camera, to spot obstacles in the car's path. It also sent out a software update that sharply curtailed the length of time a driver can let go of the wheel, and introduced brighter, flashing warnings. That length of time varies according to speed and road conditions, but can still be a few minutes."

<https://www.wired.com/story/tesla-autopilot-self-driving-crash-california/>

Motivação

- “...sistemas embarcados que sofrem de degradação graciosa (*graceful degradation*) devem ser capazes de tolerar múltiplas combinações de falhas de componentes automaticamente e assim estender sua capacidade e ciclo de vida.”

Shelton et. al (2003)

Degradação graciosa é quando o sistema vai degradando seus componentes reduzindo sua funcionalidade e desempenho, até chegar a reduzir sua funcionalidade e desempenho por completo.

Objetivos Gerais

- **Objetivos Gerais:**
 - Analisar e caracterizar diferentes erros de software, falhas de hardware e degradações de sistemas embarcados e seus efeitos sobre a resposta dinâmica, o transitório, a coordenação, a sincronização e as habilidades do sistema, tais como a estabilidade, controlabilidade, observabilidade e sensibilidade.
 - Propor novos métodos e algoritmos para prover o prognóstico e reduzir efeitos indesejáveis que degradam o desempenho do sistema.

Objetivos Específicos

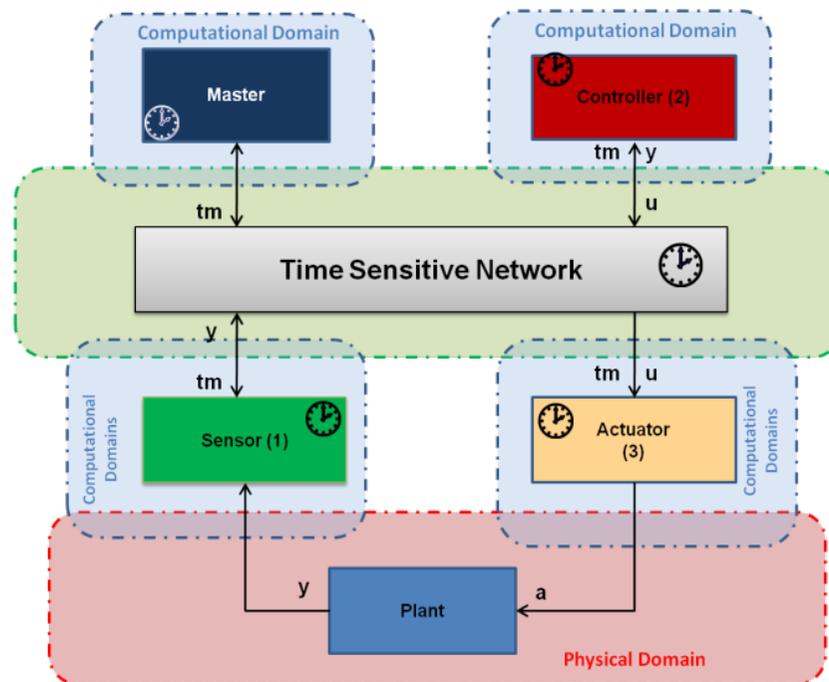
- Objetivos Específicos:
 - **A)** Escolher um sistema embarcado cibernético físico, com integração da comunicação, computação e controle, para ser usado como estudo de caso a todas as etapas subseqüentes;
 - **B)** Modelar os sistemas e subsistemas do estudo de caso escolhido utilizando técnicas de MBSE (Model Based System Engineering), ferramentas de modelagem, matemática contínua, discreta e teoria de controle;
 - **C)** Verificar, validar e analisar os modelos desenvolvidos na etapa, via simulação, e quando disponível, experimentalmente;

Objetivos Específicos

- Objetivos Específicos:
 - **D)** Identificar e caracterizar diferentes padrões de comportamentos e modos de operação, classificando os erros de software, falhas de hardware e degradações oriundas de diferentes domínios e níveis do através de técnicas de modelagem, simulação e análise de dados, do estudo de caso escolhido;
 - **E)** Propor novos métodos e algoritmos para prover o prognóstico dos erros de software, de falhas de hardware e degradações, para reduzir os efeitos indesejáveis que degradam o desempenho do sistema. Os métodos devem ser gerais, podendo ser aplicados em diferentes sistemas.

Resultados Esperados

- Definição de um estudo de caso que seja de interesse da Universidade e comunidade científica.
 - Envolvendo diferentes domínios.



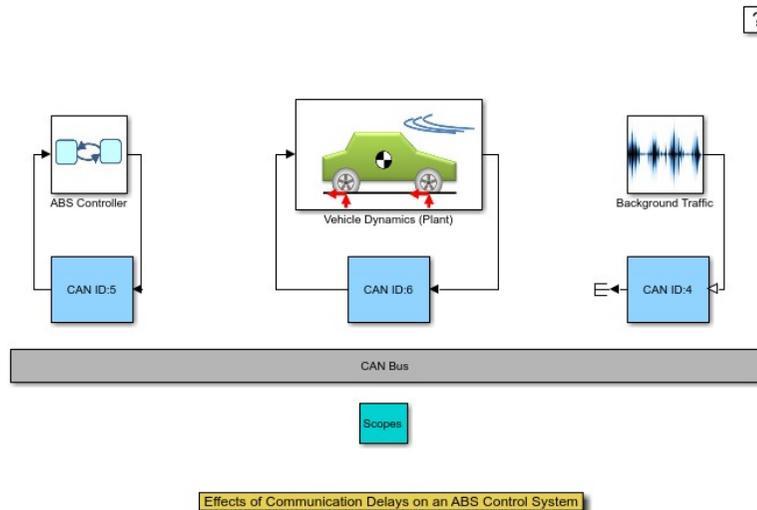
Resultados Esperados

- Modelos computacionais e matemáticos (discreto e contínuo) heterogêneos e híbridos (integração da comunicação, computação e controle) do estudo de caso; e também de outros sistemas de embarcados que venham a ser de interesse da Universidade;
- Verificar e validar os modelos desenvolvidos:
 - Simulações computacionais;
 - Análise computacional e matemática destes modelos quanto a transitórios, estabilidade, controlabilidade, observabilidade, sensibilidade, sincronização e coordenação;
 - Quando disponível, desenvolvimento de protótipos;

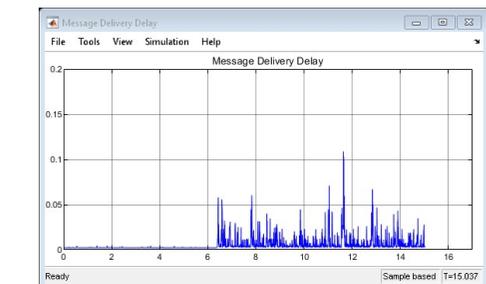
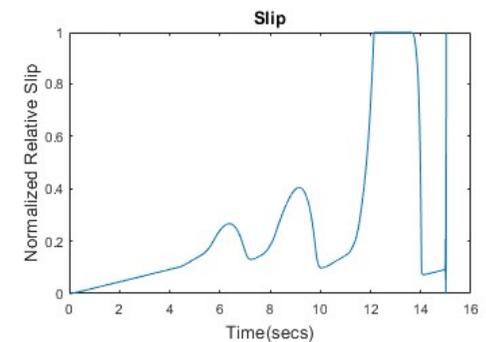
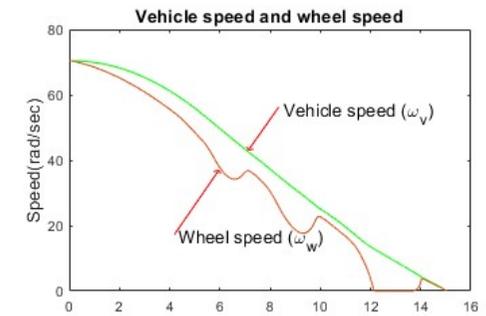
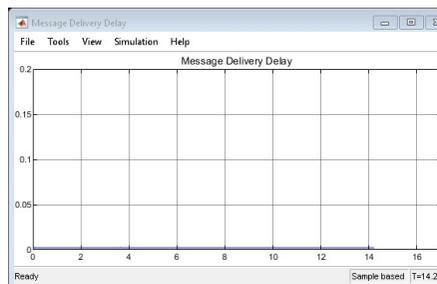
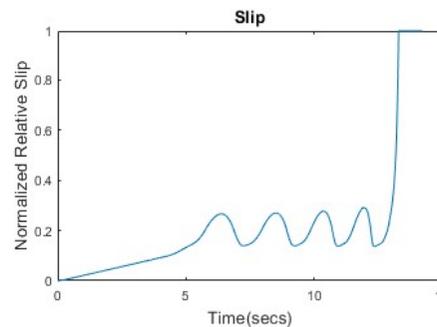
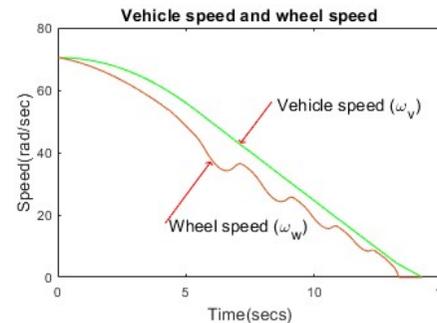
Resultados Esperados

Exemplo de um Modelo

Modelos computacionais e matemáticos (discreto e contínuo) heterogêneos e híbridos (integração da comunicação, computação e controle)



Copyright 2007-2015 The MathWorks, Inc.



Resultados Esperados

- Identificação e caracterização dos diferentes comportamentos do estudo de caso escolhido, identificando e classificando em:
 - Erros de Software;
 - Falhas de Hardware;
 - Degradações de comportamento;
- Novos:
 - Métodos e algoritmos que façam o prognóstico de erros de software, de falhas de hardware e degradações;
 - Com isso, novas capacidades de reconfiguração e adaptabilidade ao sistema;
 - Estabelecer *thresholds* e métricas para tomada de decisão do sistema embarcado

Meios e Métodos

A)	1) Avaliar Criticamente a literatura existente; 2) Definir e especificar o sistema escolhido;
B)	3) Desenvolver modelos híbridos e heterogêneos utilizando principalmente, linguagens e metodologias de modelagem tais como OPM (<i>Object Process Methodology</i>), SysML (<i>Systems Modeling Language</i>), métodos formais e teoria de controle (matemática discreta e contínua) dos sistemas especificados.
C)	4) Verificar e validar os modelos utilizando métodos formais, métodos analíticos e métodos probabilísticos e/ou estatísticos; 5) Comparar os dados simulados com os dados reais ou provenientes de experimentos; 6) Refinar os modelos.

Meios e Métodos

D)	<p>7) Categorizar os diversos tipos de comportamento;</p> <p>8) Identificar resposta padrão em operação normal e falhada dos sistemas para diferentes domínios;</p> <p>9) Mapear: 9.1) erros de software relevantes do sistema; 9.2) comportamentos degradados; 9.3) os modos de falhas de hardware do sistemas;</p> <p>10) Classificar os comportamentos de acordo com os padrões definidos;</p>
E)	<p>11) Propor novos métodos e algoritmos para prognosticar: 11.1) erros de software; 11.2) comportamentos degradados; 11.3) falhas de hardware;</p> <p>12) Otimização dos métodos e algoritmos desenvolvidos.</p>

Recursos Necessários

- Acesso a livros e artigos sobre identificação de padrões de dados, sistemas de tempo real, sistemas embarcados e sistemas cibernético-físicos;
- Softwares de simulação, tais como Matlab, Octave, SciLab e outros;
- Software de desenvolvimento de linguagens C/C++ e outras;
- Acesso a computadores e laboratórios de desenvolvimento computacional;
- Dados significativos para a validação dos modelos e hardware de prototipagem;
- Resultados da caracterização e identificação dos comportamentos do sistema;
- Engajamento de alunos de graduação e pós-graduação;
- Integração do projeto aos grupos de pesquisas da Universidade

Disseminação e Avaliação

- Disseminação:
 - Produção de relatórios internos, relatórios técnicos e artigos em periódicos e revistas que não interfiram em possíveis registros de patentes e/ou software, em consonância com a Universidade.
- Avaliação:
 - Publicações alcançadas,
 - Alunos de graduação e pós-graduação engajados;
 - Possíveis patentes dos algoritmos desenvolvidos.
- O projeto deve identificar também, demandas para novas disciplinas e cursos de pós-graduação.

Matriz Curricular

- Disciplinas que atendem ao perfil do projeto:
 - Circuitos Digitais
 - Circuitos Eletrônicos
 - Análise de Sinais
 - Sistemas de Controle
 - Laboratório de Eletrônica Digital
 - Matemática Discreta
 - Modelagem e Simulação de Sistemas

Recursos

- Consideram-se três estratégias para captação de recursos para este projeto de pesquisa:
 - 1. editais de agências de fomento de pesquisa;
 - 2. parceria com empresas; uma vez que este projeto está alinhado com a necessidade de empresas automotivas, aeronáuticas, computacionais e o futuro da indústria, portanto alinhado com a captação de recursos de parcerias privadas.;
 - 3. financiamento coletivo, com engajamento de ex-alunos;

Recursos

*Para a estimativa foi utilizado: US\$ 1 = R\$4,10

Item	Descrição	Quant.	Custo
1	(Material Permanente Nacional) Computadores para simulação e Desenvolvimento prototipos. Intel Core i7, 16GB DDR4 2400Mhz, NVIDIA GTX 1060 de 6gb, HD 1 TB + 128 SSD 2 Monitores de 34” Cotação de referência da Dell: R\$12.582,00	5	R\$ 62.910,00
2	(Material Permanente Nacional) Roteador Wi-Fi	1	R\$ 300,00
3	(Material Permanente Nacional) Matlab/Simulink e 12 toolboxes Cotação para duas (2) licenças individual perpetua	2	R\$ 90.414,00
4	(Material Permanente Nacional) Kit de Desenvolvimento de Prototipo - Kit Arduino Advanced Cotação de Referencia do Site da FlipFlop: R\$294,00	2	R\$ 588,00
5	(Material Permanente Nacional) Sensores e acessórios para arduino Cotação de Referencia do site da FlipFlop R\$ 169,75	2	R\$ 339,50
6	(Despesas com Diárias no país e no exterior) 2 eventos nacionais por ano para os três alunos e o proponente (Referência LADC 2019 : 9th Latin-American Symposium on Dependable Computing) (4 pernoites) - Diária: R\$555,00 1 evento internacional por ano para um aluno e o proponente (Referência 9th International Conference on Advances in Computing and Information Technology) (6 pernoites) * Diária: US\$400,00 – R\$ 1640,00	5 (anos)	R\$ 142.800,00

Recursos

*Para a estimativa foi utilizado: US\$ 1 = R\$4,10

Item	Descrição	Quant.	Custo
7	(Despesas de Transporte) 2 eventos nacionais por ano para os três alunos e o proponente (Referência CBEB – Congresso Brasileiro de Engenharia Biomédica) Voo local média: R\$800,00 (ida e volta) 1 evento internacional por ano para um aluno e o proponente (Referência - ACITY - 9th Latin-American Symposium on Dependable Computing) Voo para o próximo ACITY (Sydney): R\$5900 (Ida e Volta)	5 (anos)	R\$ 75.000,00
8	(Despesas com inscrições de eventos) 2 eventos nacionais por ano para os três alunos e o proponente (LADC 2019 : 9th Latin-American Symposium on Dependable Computing) * inscrição professor: R\$2400 * inscrição aluno: IC: R\$460 / Pós: R\$ 960 1 evento internacional por ano para um aluno e o proponente (Referência ACITY) * inscrição professor: US\$ 1087 - R\$4456 * inscrição aluno: US\$ 530 - R\$2173	5 (anos)	R\$ 54.545,00
9	(Despesas com publicações de artigos) Referência de custo de publicação (Open Access) de um artigo na IEEE Transactions on Aerospace and Electronic Systems: US\$2045,00 – R\$8384,50	5 (anos)	R\$ 41.922,50
10	(Bolsas de Iniciação Científica Vinculadas ao Projeto) - 2 Alunos Valor tabela FAPESP: R\$ 676,80	5 (anos)	R\$ 81.216,00
11	(Bolsas de Mestrado Vinculadas ao Projeto) - 2 alunos Valor tabela FAPESP: R\$ 1.988,10	4 (anos)	R\$ 191.817,60
12	(Bolsas de Doutorado Vinculadas ao Projeto) - 1 Aluno Valor tabela FAPESP: R\$ 2.929,80	4 (anos)	R\$ 140.630,40
Total em 5 (anos)			R\$ 882.483,00

Referências Bibliográficas

- GUNES, V.; PETER, S.; GIVARGIS, T. Modeling and Mitigation of Faults in Cyber-Physical Systems with Binary Sensors. IEEE 16th International Conference on Computational Science and Engineering (CSE). [S.l.]: IEEE. 2013. p. 515-522.
- KOPETZ, H. Sparse time versus dense time in distributed real-time systems. Distributed Computing Systems, 1992., Proceedings of the 12th International Conference on. Yokohama, Japão: 10.1109/ICDCS.1992.235008. 1992. p. 460-467.
- KOPETZ, H. Real time systems: design principles for distributed embedded applications. 1. ed. Norwell: Kluwer Academic Publishers, 1997. 378 p. ISBN 978-1-4419-8237-7.
- LEE, E. A. The past, present and future of cyber-physical systems: A focus on models. Sensors, 15, n. 3, 26 Fevereiro 2015. 4837-4869.
- OLIVEIRA JUNIOR, E. M. Estudo dos efeitos da sincronização sobre o transitório e a estabilidade de sistemas de controle por rede. Instituto Nacional de Pesquisas Espaciais (INPE). São José dos Campos, p. 467. 2015.
- SHELTON, C. P.; KOOPMAN, P.; NACE, W. A framework for scalable analysis and design of system-wide graceful degradation in distributed embedded systems. Proceedings of the Eighth International Workshop on Object-Oriented Real-Time Dependable Systems. [S.l.]: IEEE. 2003. p. 156-163.
- WIKIBOOKS CONTRIBUTORS. Embedded Control Systems Design/Learning from failure. Wikibooks, The Free Textbook Project., 23 Julho 2015. Disponível em: <https://en.wikibooks.org/w/index.php?title=Embedded_Control_Systems_Design/Learning_from_failure&oldid=2979684>. Acesso em: 08 Novembro 2016.

Dúvidas??
Obrigado!

Eloy Martins de Oliveira Junior