Graduate Research Day 2013
Florida Atlantic University

College of Engineering and Computer Science

Automation of the SHIELD Methodology for System Hazard Analysis and Resilient Design

Anthony Marcus, Gabriel Alsenas, Ionut Cardei, Ph.D.

Computer Science; Florida Atlantic University

The System Hazard Indication and Extraction Learning Diagnosis (SHIELD) methodology was developed as a novel method to perform system hazard analysis and resilient design. In the predecessor to this project, we described SHIELD conceptually and outlined the details necessary to conduct the analysis manually. This approach integrates state space examination into the analysis process in order to facilitate efficient and comprehensive identification of undiscovered risks and hazard scenarios. SHIELD requires that three phases (decomposition, evaluation and prescription) be performed serially to achieve a system hazard evaluation.

The first phase of SHIELD, decomposition, breaks the system down hierarchically and recursively into smaller components so that the state space associated with each component is more manageable for the user. In the evaluation phase, typically experts would analyze the associated state space and transitions for each component, recursively, bottom-up. In the final phase of the analysis, prescription, we apply a set of heuristics to the results from the preceding phase. The concept is such that with these heuristics we incite ideas in the design team to find solutions to the resulting hazardous state combinations from the evaluation phase.

Our main contribution in this project is the automation of the methodology such that the temporal parameter associated with the analysis will be greatly reduced without sacrificing accuracy or overlooking hazardous state combinations.

FAU COLLEGE OF ENGINEERING & COMPUTER SCIENCE Florida Atlantic University

Automation of the S.H.I.E.L.D. Methodology for System Hazard Analysis and Resilient Design

SNMREC Southeast National Marine Renewable Energy Center

TECORE NETWORKS Wireless and Mobile Communications Florida Atlantic University

Anthony Marcus, Ph.D. Candidate in Computer Science

Advisor: Ionut Cardei, Ph.D. *SNMREC Program Manager:* Gabriel Alsenas

The Department of Computer and Electrical Engineering and Computer Science & the Southeast National Marine Renewable Energy Center

Florida Atlantic University

IEEE Systems Council 2013 IEEE International SYSTEMS CONFERENCE April 15-18, 2013 Hyatt Regency Grand Cypress Orlando, Florida USA

AutoSHIELD Main Features

Decomposition:

- decompose top-down the system hierarchically in subsystems
  - currently done with an XML file
  - future work with graphic modeler
- include environmental factors affecting components in the design specification (e.g. channel noise, ocean state)
- describe state space for subsystems where available
- generate Bayesian Network from system structure
  - state random variable node for each component
  - environmental factor
- describe
  - dependencies between subsystems
  - conditional probability tables (CPT)
- generate CPT for trivial or template subsystems
- generate reduced state space based on impact factor and CPT

Evaluation:

- state and IF prediction
- hazard state diagnostic
- subsystem hazard impact ranking
- 3 main user query types
  - Global system impact diagnostic
  - Global system root diagnostic
  - Sub-component impact diagnostic

Prescription:

- heuristic suggestions based on the system being analyzed
- system reevaluation after additional components have been added to the system design

Published and Submitted Article Citations:

- "*Resilient System Design for Prognosis and Health Monitoring of an Ocean Power Generator*", Marcus, A., I. Cardei, T. Tavtilov, G. Alsenas; IEEE Systems Conference 2012 (2012): 1-8. IEEE, 2012.
- "*Automation of the SHIELD Methodology for System Hazard Analysis and Resilient Design*", Marcus, A., I. Cardei, G. Alsenas; IEEE SysCon 2013 Conference.

Overview

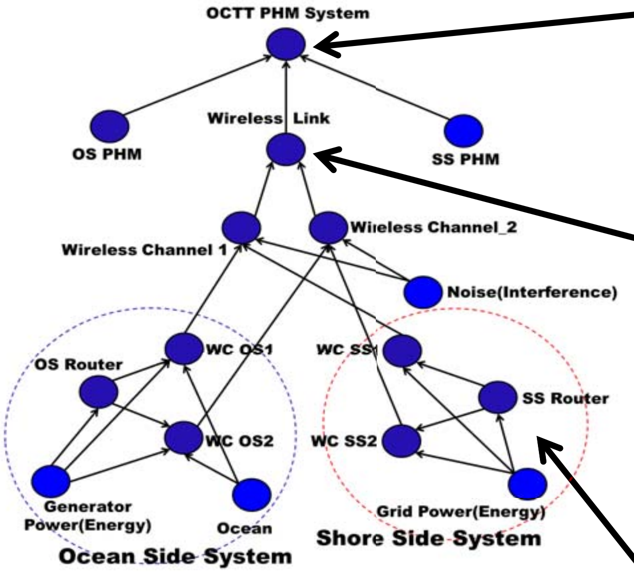
Problem:

How do we protect and insure that the Ocean Current Turbine Testbed (OCTT) will operate autonomously and at optimum efficiency even facing disruptive or traumatic events?

Solution:

Build a tool which integrates resilience engineering and hazard analysis into complex system design for use by system designers and domain experts

The Bayesian Network used for evaluating the OCTT PHM architecture and the prototype AutoSHIELD system



Global System Root Diagnostic Query:

- **Problem:** What is the probability for the system as a whole to be in a 'high-risk' state?
- **How:**
  - compute the probabilities associated with each state of the root component
- **Result:** Root Component Probabilities

Cases shown for Single and Redundant Wireless Channels

	OCTT PHM System State	
	Faulty	Not Faulty
1 Wireless Channel	6.59%	93.41%
2 Wireless Channels	1.99%	98.01%

- **Conclusions:**
  - OCTT PHM System error 6.59% with a single wireless channel
  - we added a redundant component to boost system resilience
  - reevaluation of the system
  - OCTT PHM System error 1.99% with redundant wireless link
  - redundant component boosted the overall system resilience by 4.6%

Global System Impact Diagnostic Query:

- **Problem:** which states have the greatest impact to a 'high-risk' root component state?
- **How:**
  - set the root component into an error state
  - compute marginal probabilities for the first level subcomponents
- **Result:** Marginal Probabilities

Case shown for OCTT PHM System State == Faulty

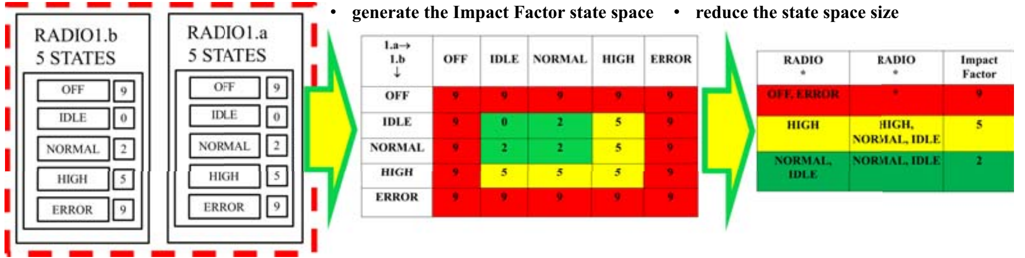
Subcomponents	Subcomponent Data			
	Error State	IF	Normal State	IF
OS PHM	7.59%	9	92.41%	0
Wireless Link	93.96%	9	6.04%	0
SS PHM	0.35%	5	99.65%	0

- **Conclusions:**
  - 93.96%, an error in the wireless link is the most probable contributor
  - with an IF = 9, the wireless link will cause total system failure
  - user may add new components to increase the resilience of the system
  - reevaluate the system until probabilities are within acceptable bounds

State Space Reduction Using System Impact Factor

How:

- take 2 serially connected components
- generate the Impact Factor state space
- combine the subcomponent states having the same IF
- reduce the state space size



1.a→ 1.b ↓	OFF	IDLE	NORMAL	HIGH	ERROR
OFF	9	9	9	9	9
IDLE	9	0	2	5	9
NORMAL	9	2	2	5	9
HIGH	9	5	5	5	9
ERROR	9	9	9	9	9

RADIO *	RADIO *	Impact Factor
OFF, ERROR	*	9
HIGH	HIGH, NORMAL, IDLE	5
NORMAL, IDLE	NORMAL, IDLE	2

Sub-Component Impact Diagnostic Query:

- **Problem:** What subcomponent states have the greatest impact to a component in a 'high-risk' state?
- **How:**
  - compute probabilities of all subcomponents associated with a 'high-risk' component state
- **Result:** Sub-Component Probabilities (right)

Case shown for Wireless Channel 2 == Faulty

Component	State	Percentile	IF	State	Percentile	IF
Noise(Interference)	Yes	38.39%	3	No	61.61%	0
SS Router	Error	30.54%	9	Normal	69.46%	0
Ocean	Rough	29.52%	5	Calm	70.48%	0
OS Router	Error	28.33%	9	Normal	71.67%	0
Generator Power	Off	5.83%	9	On	94.17%	0
Grid Power	Off	5.33%	9	On	94.67%	0

- **Conclusions:** *IFF* wireless channel 2 is faulty:
  - 38.39% probability of noise
  - 29.52% probability of a rough ocean
  - little ability to change either component
  - however both routers have ~30% probability to be in an error state
  - use data to boost the systems capability or margin of tolerance to these disruptive states
  - reevaluate system probabilities