Thoughts on Information Operation Detection as a Nonlinear, Mixed-Signal Identification Problem: A Control Systems View

John James, John@JRJames.com

Abstract-- Information Operations is a new area of responsibility for military units and a new area of interest for military institutions. This interest is motivated by the realization that increased reliance on benefits accruing from expanded use of information system technologies creates *opportunities* for offensive information operations capabilities and *vulnerabilities* for defensive information operations capabilities. Commercial enterprises face similar opportunities/vulnerabilities in the electronic commerce area. Information Operations are characterized by both the wide range of target/defended system dynamics as well as by the increased complexity of interaction of system components. This paper presents two related notions: (1) higher-level, relatively slow decision support systems can benefit from treating (i.e. modeling and identifying) feedback control properties of relatively fast system processes, and (2) Information Operations is a category of decision support systems that requires explicit treatment of the attack detection problem as a mixed-signal identification problem. Such a view of large-scale systems is a *control system view* since the fundamental characteristic of control system science is the study of feedback loops. The paper will (1) assert that the Information Operations Vulnerability/Survivability Assessment (IOVSA) problem is a "system of systems" problem containing feedback loops, (2) discuss *detecting* Information Operation attacks as a mixed-signal system identification problem, (3) review several current design environments which support a "system of systems" approach, and (4) discuss ideas on a test bed framework for conducting experiments to achieve on-line detection and reaction to Information Operation attacks.

Index Terms—information assurance, information operations, system identification, mixed-signal

I. The Information Operations Vulnerability/Survivability Problem

Use of reference architectures for component-based design and analysis of large-scale systems has become fairly widespread. Considering major system components as systems in their own right has led to the characterization of their composition into the implementation architecture of the overall system as the "system-of-systems" problem. The approach taken here is to consider the IOVSA problem as a "system-of-systems" problem and also to consider the components of the problem domain models and architectures as containing contain feedback loops.

As enterprises rely more heavily on the benefits of electronic commerce, the problems associated with security of proprietary data has become a major issue. Recently, the United States, represented by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) has concluded an international agreement on assessing the status of information system security, the Common Criteria [16,17]. Current DoD guidance on assessing the status of information system security is found in [15]. A discussion of the importance of information operations to critical DoD command and control systems and also recommendations for improving the status of information systems security is found in [14]. A critical observation contained in [14] is that an acceptable level of security is driven by a ***risk assessment*** in which a perfect security solution is recognized as unattainable while an ***80% solution*** will normally be acceptable. A similar recognition of the need for the information security process to be driven by a *risk assessment* is formally included in the Common Criteria discussed in [16, 17]. Commanders need a solution for achieving a level of trust that information system components are functioning properly and meeting the needs of the unit.

Adaptive network security is advocated by Internet Security Systems, a prominent provider of commercial products for network security, as a necessary approach for securing commercial enterprise networks against malicious attacks. ISS recommends a Detect, Monitor, Respond sequence for managing network attacks. Since military communication architectures are deliberately designed to change over time, degradation and enhancement of network information processing capability over time will be a characteristic of unit operations. Consistent with the discussion of the preceding paragraph, a unit's ability to *detect, monitor, and respond* to IO attacks should be based on: a ***risk assessment*** of unit vulnerabilities, a deliberate decision concerning an ***acceptable level of risk***, and methodologies to achieve that level of risk in unit information systems.

This paper describes work partially supported by the Physical Science Laboratory, New Mexico State University. The opinions expressed here are those of the author and do not reflect official positions of PSL, NMSU, or the United States Army.

For example, a detect, monitor and respond capability is a necessary element of the Autonomous Information Assurance [8] project of the Defense Advanced Research Projects Agency (DARPA). The AIA project envisions a reactive capability to respond to an IO attack (see Figure 1) predicated on an ability to estimate the current state of the battlefield processes being monitored.

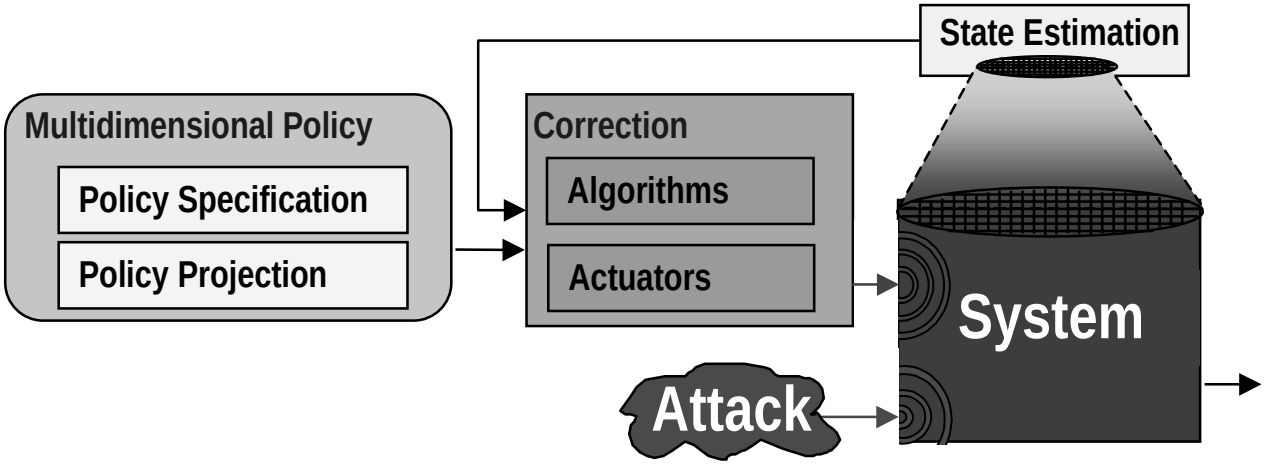

Figure 1. Feedback control concept for Autonomic Information Assurance

Thus, IO process analysis is necessarily preceded by an ability to *identify* normal current system architecture activities, and then enabled by an ability to *detect* new or previously-encountered anomalous activities, *monitor* anomalous activities, and *respond* to IO attacks. Following the reasoning presented in [9], the partitioning of the overall system into smaller system components is assumed to require consideration of feedback loops present in system processes. This is not a new position. Indeed, the component aggregation and disaggregation problem has been repeatedly studied. A good summary with references is found in [12]. Furthermore, the problem domain of at least one of the system components (e.g. the target engagement problem or the quality-of-service-based bandwidth allocation/reallocation problem) is assumed to be a "mixed-signal" problem.

For an analysis framework, prudent resource management (as well as practical engineering concerns) requires that minimal required effort be expended to achieve "close-enough" models of system dynamics, similar to the philosophy of Professor Lotfi Zadeh's soft-computing effort. A major hurdle in such an endeavor to reactively determine what is "close enough" is to determine what is "timely enough". In this regard, the ideas of E. Douglas Jensen [18] concerning "soft-real-time" system analysis as a necessary compliment to "hard-real-time" analysis are especially appropriate. Finally, an analysis framework for IO must be capable of capturing the military decision-making process that begins with receipt of a mission, continues to analysis of alternative courses to action to accomplish the mission, generates an operations plan to execute the chosen course of action, and monitors the execution of the plan, replanning as necessary. For Army operations, the timeliness of Battlefield Operating Systems is dynamically determined by the synchronization matrix produced during the military decision-making process (MDMP).

II. Detecting Information Operations Attacks

Information Operations are those operations which affect the cognitive processes of command or the systems that support these processes. Information operations can be offensive or defensive. The Army has categorized expected threats to information systems by level of hostility, adversaries, and adversary options. Commanders have used Defense Condition (DEFCON) notices for many years to alert units to changes in levels of hostility. Recently, Information Condition (INFOCON) levels have been established to enable commanders to alert units to changes in likelihood of information operation attacks which correspond to the changes in the levels of hostility. Identification of the major components of a large-scale, distributed system is a daunting task. The approach taken here is to leverage existing knowledge of the problem domain to greatly simplify that task by breaking the overall problem down into more manageable sub-problems. Consider the problem domain to be the *detection* of Information Operation attacks directed against the First Digitized Division (FDD) to be fielded by the U.S. Army in the next eighteen months. A key feature of the FDD is implementation of a tactical local area network (LAN) to support Information Dominance of friendly forces over opposing forces. The discussion below of the Information Operation detection problem simply takes advantage of the tremendous effort being expended by the Army to apply the concepts of product-line, system-of-systems architectures and reusable component. The Army Enterprise Architecture (AEA) [7] provides guidance on the digitization of Army tactical and installation information systems. The AEA directs construction of a single Army information system architecture with three views: *Operational, System, and Technical* (Figure 2).

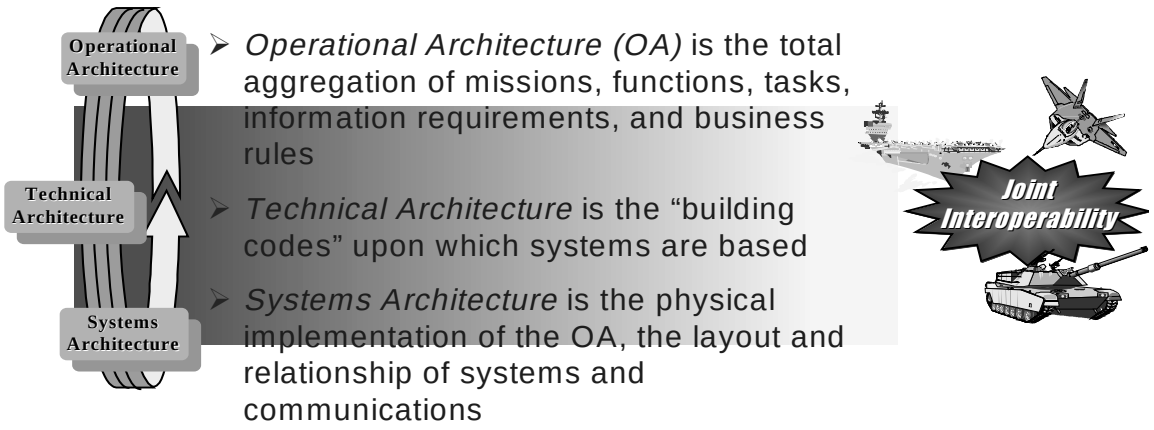

Figure 2. Army Enterprise Architecture

Thus, we expect to observe in fielded implementation architectures (i.e. the hardware and software present in units vary according to *System Architectures* for specific units) a ***"normal"*** flow of information corresponding to the battlefield processes of a given unit (i.e. the input-output characteristics correspond to the *Operational Architecture* specified for the unit) which complies with the implementation standards required for the signal being observed (i.e. the transmission characteristics comply with the *Technical Architecture* of the unit being observed). The AEA provides the framework for life-cycle system management of Army information technology systems, including Army Command, Control, Communications, Computers, and Intelligence (C^4I) systems.

Our identification problem is then to filter the observed signals into appropriate sets of data for the unit being analyzed and to compare known patterns for separable components to patterns observed in the data being analyzed. Metrics are needed to determine closeness of observed patterns to expected patterns. Anomalous activity is then indicated (detected) when differences exceed some user-determined threshold.

Each of the divisional *system architectures* will be different and will change as new equipment is introduced. As each division deploys to conduct operations, each operations order (OPORD) executed by units will comply with the *operational architecture* of the AEA with changes as needed to accommodate current circumstances. The *technical architecture* will change slowly to accommodate new technologies. Thus, the majority of the new work is to create an analytical framework for analysis of the Army IO problem as a "system of systems" problem of composition of dynamical decision components which change over time. For example, consider the issues surrounding detecting and reacting to Information Operation attacks during a battalion (Task Force XXI) deliberate attack. Two documents produced either separately during the MDMP or as part of an Operations Order (OPORD) are the Task Organization and the Signal Annex. The Task Organization provides the hierarchy of units conducting the operation and the Signal Annex provides the description of the mobile, fixed, and local area-network communications used during the operation.

A test bed is being constructed that will initially use an existing attrition-based simulation model to provide command and control message traffic (e.g. verbal reports and orders) and situational awareness data traffic (e.g. position, status and activity data) corresponding to an operational scenario. The test bed will use a set of intelligent agents to model unit activities and detect information operation attacks. The Task Organization and Signal Annex network knowledge can be used to apply evaluation technologies to enable the agents to make an assessment of whether the status of the operation execution is normal (Green), somewhat abnormal (yellow), or definitely anomalous (red).

An initial set of activities for the agents will be to determine the center of mass of the units in the Task Force XXI organization using the situational awareness (SA) output of an attrition-based model.

For example, a subset of a particular maneuver concept for a unit *mission* might be to seize a particular *objective* after securing a critical *intermediate objective*. Intelligent agents can be used to determine whether a sensed sequence of battlefield activities are *close enough* for successful execution of the commander's *Concept of the Operation* to achieve the commander's *intent* stated in the unit OPORD. Engagement of multiple targets by multiple weapons platforms is a difficult problem where detection, identification, prioritization, selection, engagement, and re-engagement tasks must be made under severe time and uncertainty constraints. A mixed-signal model of the problem has been previously developed.

III. Design Environments Supporting a "System of Systems" Approach for Nonlinear Systems Identification:

Most large, complex automation systems (e.g. finance, transportation, maintenance) are built and reliably maintained while applying an underlying assumption that each individual component is independent of all other components (i.e. the next state and output of each component depends only on the current component state and the current input to the component). However, for a large class of systems, the presence of feedback loops

among sets of system components invalidates the independence assumption for those coupled components and, therefore, reliable system construction requires explicit identification of process feedback loops and their use in the system development process. Also, for large systems, event-based decisions make the models highly non-linear, with possible emergent dynamics dependant upon choices made by humans-in-the-loop. One widely-used set of nonlinear models for approximating military systems is the Lanchester-based attrition models [12] used for estimating battle outcomes. Actual warfare is considerably more nonlinear than the relatively well-behaved Lanchester equations which are normally the primary continuous-system component of an event-based military systems simulation environment. The discussion found in [12] is an excellent summary of the challenges present in aggregation and disaggregation of military models. The problem of nonlinear, mixed-signal system identification occurs widely in control system science and engineering. Such models can lead to chaotic system state and chaotic system response. While most applications seek to avoid the conditions for onset of chaos, others have discovered that physical system data (especially in biological sciences) exhibit chaotic behavior. While electronics engineers continue to use the mixed-signal term, in the past ten years control engineers have began to refer to mixed-signal problems as ***hybrid systems*** problems [10,11].

Control engineers are especially interested in avoiding unstable regions where unpredictable signals occur. Electrical engineers use the term "mixed-signal" to refer to the problem of simultaneously analyzing both digital and analog signals to design, build and test a system or a system's components. In a *hybrid system* formulation, as well as in other abstractions of physical systems, a careful distinction must be made between the *hybrid system state*, which is a computable approximation of the actual system values, and the *physical system state*, which is the true set of values of system variables. In fact, the "true" set of variables of a given system may not even be known, much less the values of those variables. Control engineers normally realize the costs associated with accurate sensing of physical system values and make a conscious decision to select a limited set of variables whose values can provide a "close enough" approximation of the physical system state. Thus, metric spaces are a necessary requirement for representational mechanisms and the choice of variables, metrics spaces, and metrics is a central part of both the science and the art of control system engineering. Artificial Intelligence (AI) researchers have referred to the analog-to-digital portion of the mixed-signal problem as the "signal–to-symbol" problem or the "pixel-to-predicate" problem. The term "mixed signal" is more generic since it encompasses both the digital-to-analog portion of the problem as well as the analog-to-digital portion of the problem. Both transformations are necessary to implement digital control systems since system analog signals must be transformed into digital signals to have a computable representation of the system state and computed control laws (i.e. digital control signals) must be transformed into analog servomechanism control signals to actuate the commands in the physical system. As the cost of digital signal processors has decreased, there has been a corresponding increase in their use to control a wider variety of devices. Some companies are now predicting an era of "ubiquitous computing" to indicate use of embedded, networked devices in a wide range of home, recreation and office appliances. A variety of software environments have recently been developed to deal more effectively with modeling hybrid dynamical systems.

The web page of the IEEE Control System Society (CSS) Technical Committee on Hybrid Dynamical Systems [20] has links to several active research groups and also to some computer packages for modeling hybrid systems. In addition, environments at the University of California at Berkeley [2] and Georgia Tech [1] support efforts in a Software-Enabled Control (SEC) initiative funded by the US Department of Defense. The SEC sites discuss use of software-enabled control to control autonomous air vehicles.

The Spatial Aggregation Language (SAL) has been developed by Feng Zhou to support analysis and design of hybrid systems [3]. The approach is being investigated at XEROX Palo Alto Research Center (PARC) as an environment for complex system design.

A systems-level modeling language is being developed by an IEEE committee [24]. However, the Modelica language [21] has been under development for several years in Europe and now has a commercial implementation for control systems, as do the VHDL-AMS (now IEEE Standard 1076.1) [22] and Verilog [23] languages used for electronic design and implementation. However, the emphasis on explicit modeling of system communication components in [9] is certainly different than many large-scale systems modeling efforts. Moreover, the range of system dynamics, together with explicit support for adapting goals and methods of the higher-level control plan is, if not unique to the military problem domain, certainly not the problem normally encountered in mixed-signal control analysis and design.

The Discrete Event Simulation System (DEVS) developed by Professor Bernard Ziegler has been widely used for simulation of military systems and has recently been modified to be compliant with the Department of Defense (DoD) High Level Architecture (HLA). Neither HLA or DEVS has explicit support for hard-real-time systems simulation but both have been used for soft-real-time-simulation. Several engineering design groups have been working on a system-level language that supports partitioning of functionality between hardware and software modules [24].

As with other hybrid control problems, the central, enduring difficulty has remained that, while we are able to simulate the composed problem, we are unable to discover all failure modes of complex, adaptive systems whose dynamics are approximated by the composed models. We are, thus, able to reliably react to known failure modes but are unable to guarantee a controlled response to undetected failure modes. Thus, similar to the development of the flyball governor for steam engine speed control and the electronic feedback amplifier for telephone line voltage control,

engineers have again progressed to the point of building useful and (normally) reliable systems whose performance capabilities exceed the analytical capabilities of current theoretical approaches to predict, verify and validate system performance.

IV. An Approach for Modeling Information Operations

This section provides an overview of a test bed operational concept. Indeed, application of the tools mentioned in section three to analyze processes summarized in section two subject to attacks stated in section one requires a framework for discerning normal operations from anomalous operations.

The framework is a subset of the Army operational architecture. The cognitive processes of command can be approximated by a set of planning and replanning activities to produce, update and execute OPORDs designed to achieve assigned missions. Commands at each level normally plan two levels down and one up when reviewing their alternatives. To place individual units at the right places and in the right sequences to occupy intermediate objectives and execute intermediate operations requires a series of coordinated movement, communication, engagement and other processes by different units, at different echelons of command working at different rates over different distances. These highly nonlinear processes are distributed in time and space and change over time. A primary goal of Information Operations is to degrade or interrupt the flow of information required to plan and execute operations.

To identify anomalous operation of the command and control system it is necessary to (1) understand normal operation of the relatively slow, more distributed battlefield processes, (2) understand normal operation of the relatively fast, more local battlefield processes, and (3) institute a framework for comparison of current system execution to normal system operation.

4.1 Relatively Slow Battlefield Processes

The relatively slow processes to be analyzed include:

- MDMP review of OPORD
- Propagation of an OPORD and changes to an OPORD
- Movement/Planning processes of higher echelons

4.2 Relatively Fast Battlefield Processes

The relatively fast processes to be analyzed include:

- Target engagement processes
- Communication processes (especially bandwidth control),
- Movement/Planning processes of lower echelons

4.3 A Framework for Comparison of Battlefield Processes

A framework for comparison of battlefield processes is based on exploitation of the Army effort to structure unit capabilities and assigned missions by battlefield operating system. For commanders and staff, the primary issue to be resolved during execution of an operation is whether the operation is proceeding successfully, and, if not, to alter the OPORD (replan) to ensure mission accomplishment. Thus, a framework for comparison of battlefield processes has two parts (1) an approach for automated "understanding" of an OPORD, and (2) an approach for determining whether the OPORD is being successfully executed.

4.3.1 "Understanding" an OPORD

The commander's intent is usually stated either verbally or in writing but the semantics of intent is not amenable to automated understanding at this time. However, the concept of operation is normally defined in terms of time and spatial constraints that are keyed to unit movement over terrain and which are amenable to automated "understanding" at different levels of detail. Specifically, for each operation it is possible to abstract:

- Activities by BOS and echelon, and
- Constraints on unit execution by phases of the operation

4.3.2 Estimating Execution of an OPORD

A structure to construct an estimate of execution of an OPORD is:

- Partition actions by BOS and echelon to reflect planning/replanning interactions at multiple levels of command
- For relatively higher echelons, focus on the use of the synchronization matrix produced during OPORD generation as the central tool for determining whether critical activities for plan success are being timely executed by each BOS
- For relatively lower echelons, focus on use of command and control messages to start and stop the flow of units, use of automated position, movement and status messages to maintain estimates of movement aggregations meeting expected rates and times of completion, and use of local synchronization matrices to coordinate calls for fire.
- At the lowest levels of execution, support dynamic prioritization of engagements (allocation of sectors of fire, determination of priority of effort, issue of alerts to enemy activity) for weapon system crews and dynamic prioritization of available bandwidth for information flow.

V. SUMMARY

The multidisciplinary aspect of control theory development and application has been widely recognized for decades and the control system design process has also recently been singled out by major manufacturers as the appropriate technology for integrating multidisciplinary production processes. This paper has discussed the Information Operation detection problem as a nonlinear, mixed-signal identification problem and has offered ideas on a test bed framework for conducting experiments to achieve on-line detection and reaction to Information Operation attacks.

VI. REFERENCES:

[1] Georgia Tech SEC web page: http://controls.ae.gatech.edu/projects/sec/

[2] Berkeley SEC web page: http://sec.eecs.berkeley.edu/

[3] Xerox PARC Spatial Aggregation Language (SAL) web page: http://www.parc.xerox.com/spl/members/zhao/stanford-cs329/sal-doc/index.html

[4] James, J. R., D. K. Frederick, and J. H. Taylor, "Use of Expert Systems Programming Techniques for the Design of Lead-Lag Compensators" *IEE Proceedings*, Vol. 134, Pt. D, No. 3, May 1987.

[5] James, J. R. and L. Rapisarda, " An Approach to Implementing a Knowledge-Based Controller," *Proceedings of the Third IEEE International Symposium on Intelligent Control""*, Arlington, VA 23-24 August, 1988.

[6] Headquarters, Department of the Army, FM 100-6, Information Operations, August, 1996.

[7] Office of the Director of Information Systems for Command, Control, Communications, and Computers (ODISC4), The Army Enterprise Architecture Master Plan, Vol.1, 30 September, 1997.

[8] DARPA Autonomous Information Assurance Program web page: http://web-ext2.darpa.mil/iso/IA&S/IASPIP990811Final.html

[9] James J. and R. McClain "Tools and Techniques for Evaluating Control Architecture," Proceedings of the 1999 IEEE International Symposium on Computer Aided Control System Design, Kohala Coast-Island of Hawai'i, Hawai'i, USA, August 22-27, 1999.

[10] Benveniste, A and P. Le Guernic, "Hybrid Dynamical Systems Theory and the SIGNAL Language", *IEEE transactions on Automatic Control*, 35(5), May 1990, pp. 535-546.

[11] Bencze, W. J., and G. F. Franklin, "A Separation Principle for Hybrid Control System Design," *Proceedings of the IEEE/IFAC Joint Symposium on Computer-Aided Control System Design*, March, 1994.

[12] Otter, M., and F.E. Cellier (1995), Software for Modeling and Simulating Control Systems, The Control Handbook (W.S. Levine, ed.), CRC Press, Boca Raton, FL, pp.415-428.

[13] Davis, Paul K, Aggreggation, Disaggregation, and the 3:1 Rule in Ground Combat, RAND Report MR-638-AF/A/OSD, http://www.rand.org/publications/MR/MR638

[14] Committee to Review DOD C4I Plans and Programs of the Computer Science and Telecommunications Board of the Commission on Physical Sciences, Mathematics, and Applications of the National Research Council, *Realizing the Potential of C4I - Fundamental Challenges*, **National Academy Press,** Washington, D.C. 1999

[15] Depart of Defense Instruction Number 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)", 30 December 1997.

[16] Troy, Eugene F., NIST-ITL, "Common Criteria: Launching The International Standard," http://csrc.nist.gov/cc/info/cc_bulletin.htm 24 November 1998.

[17] Common Criteria for Information Technology Security Evaluation, Common Criteria Version 2.1 / ISO IS 15408 http://csrc.nist.gov/cc/ccv20/ccv2list.htm August 1999.

[18] Jensen, E. Douglas, "Real-Time for the Real World", http://www.real-time.org/no_frames/mitre.htm

[19] MIL3 – Third Millennium Technologies, OPNET – Decision Support Software for Networks and Applications, http://www.mil3.com/

[20] IEEE Control System Society Technical Committee on Hybrid Dynamical Systems, http://www.nd.edu/~lemmon/hybrid/index.html

[21] Modelica - A Unified Object-Oriented Language for Physical Systems

[22] Modeling http://www.dynasim.se/modelica.html

[23] VHDL-AMS, http://vhdl.org/, http://www.vhdl-ams.com/

[24] Verilog Hardware Description Language, http://www.cadence.com

[25] System-Level Design Language, http://www.inmet.com/SLDL/