SANDIA REPORT

SAND2016-0428
Unlimited Release
Printed 15 December 2015

Integration of Dynamic Simulation for Infrastructure and Full Hardware Testing Capability into SCEPTRE

Jason Stamp, Ph.D. and Derek Hart
Sandia National Laboratories

Bryan Richardson
Fortalice Solutions

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energys National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from:

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@adonis.osti.gov
Online ordering:	http://www.osti.gov/bridge

Available to the public from:

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.fedworld.gov
Online ordering:	http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2016-0428
Unlimited Release
Printed 15 December 2015

Integration of Dynamic Simulation for Infrastructure and Full Hardware Testing Capability into SCEPTRE

Jason Stamp, Ph.D.
Special Cyber Initiatives Department

Derek H. Hart
Military & Critical Systems Security Department

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0671

Bryan T. Richardson

Fortalice Solutions
809 W Hill Street
Charlotte, NC 28208

Abstract

Sandia National Laboratories has an existing capability for hybrid control systems testing called SCEPTRE. This article proposes an architecture to add dynamic simulation capability for the underlying physical process (e.g. the power grid). Dynamic simulation for SCEPTRE will enable very accurate simulation, and allow the full integration of analog control systems hardware.

Abbreviations and Acronyms

Acronym	Meaning
ACD-HAIO	Automated configuration and deployment for HAIO
ACT	Absolute clock time
AEQ	Analog equipment
AGMC	Automated grid management and control
CM	Configuration management
CSAM	Cyber security awareness and management
CRT	Continuous real time
DEQ	Digital equipment
DIO	Digital I/O
DRT	Discontinuous real time
EMS	Energy management system
FICSS	Federated infrastructure – control systems simulation
GPS	Global positioning system
HAIO	Hardware analog input/output
HIS	Human-interactive simulation
HITL	Hardware-in-the-loop
HFS	High-fidelity simulation
HMI	Human-machine interface
HV	High voltage
LFS	Low-fidelity simulation
LVC	Live – virtual – constructive
MRS	Multi-resolution simulation
OS	Operating system
PLC	Programmable logic controller
R&D	Research and development
RT	Real time
RTU	Remote telemetry unit
SCADA	Supervisory control and data acquisition
SE	Simulation engine
SEP	Stable equilibrium point
SOE	Sequence of events
VAIO	Virtualized analog input/output
VPN	Virtual private network

Variable	Meaning
C	Set of control identifiers
S	Set of signals
t	time
T	Time interval
U	Control vector
X	System state vector

Executive Summary

SCEPTRE has proven to be a great benefit when examining cyber security issues for control systems. However, its infrastructure modeling capability is limited to only calculating the static character of the system, without the important dynamics that could be crucial for analysis.

Integrating dynamic simulation is a significant challenge for SCEPTRE. The approach depends on developing a taxonomy of needed capabilities and components, which is needed to explain the planned simulation flow. The process itself depends on simpler simulation whenever feasible, and transitions to dynamic simulation only when necessary (as a way to reduce delays in the execution).

Along with the transition to dynamic simulation, SCEPTRE gains the ability to incorporate control hardware that depends on dynamic simulation (like power system relays). This integration is included in the new SCEPTRE execution flow. Finally, the new capabilities allow wider application of SCEPTRE. Many more power system analysis questions can be simulated using the enchanted simulation.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Federated simulation of infrastructure systems (e.g. electric power, pipelines, water, refineries, rail/port facilities, etc.) and their associated control systems (e.g. SCADA, EMS, plant automation, protective relaying, etc.) is a difficult subject. Ongoing R&D is focused on the feedback and effects between the two areas, often concerned with cyber security issues. The complex differential-algebraic models employed for infrastructure systems do not integrate well with event-driven networking and control system representations, although Sandia has demonstrated the effective integration of steady-state solvers for infrastructure within a networked simulation (SCEPTRE [1]).

Any federated infrastructure – control systems simulation (FICSS) like SCEPTRE encompasses three fundamental domains:

- Infrastructure
- Communications and networking
- Control systems

Examples for each of these domains are shown in Table 1.1 assuming electric power as the subject infrastructure.

Table 1.1: Examples of domain elements.

Infrastructure	Comms/networking	Control Systems
Generator	Router	SCADA
Transformer	Firewall	EMS
Bus	Wireless channel	Database
HV line	VPN	Relay
Load	Microwave	Workstation
Breaker	Switch	HMI
Insulation	Fiber optic cable	PLC

Within each domain, the elements may be modeled with varying approaches at different levels of accuracy and precision, and at different time scales. One framework for modeling at different complexities is LVC (live – virtual – constructive). Live means an actual, physical representation of a component, while (at the other extreme) constructive suggests a stimulus-response model at some effective level of detail. In between, virtual elements can consist of actual software (operating systems, applications, router OS, etc.) on virtualized hardware.

1.1 High- and Low-Fidelity Simulation

In power systems, simulations are run at the transient, dynamic, and steady-state time scales, with timing of milliseconds, seconds, and minutes respectively. Each of these can be run synchronized to wall clock time (real time) or not, depending on the size of the system. Generally, only small systems can run in transient simulation at real time, and larger (but still size-restricted) ones in dynamic simulation. In either case, the federation required for a grid simulator within any FICSS necessitates ongoing data exchange with the software, and this is an uncommon capability. These limitations will make integrating dynamic or transient simulations into a FICSS very difficult.

However, there are advantages to including transient or dynamic simulation – very often, the non-steady-state behavior is a key driver for the performance of the power grid. Many disturbances affect frequency and voltage, and might lead to service curtailment if they become unacceptable for brief durations. Put another way, a new stable equilibrium point (SEP) might *exist* at a new time step, but the path to it might involve dynamics that ensure that *it its never reached*, and a different SEP is the ultimate destination for the system. An analyst looking at successive steady-state solves could easily overlook the temporary problem and infer inaccurate conclusions.

Therefore, an optimally effective FICSS would leverage high-fidelity simulation (HFS, using transient or dynamic solvers) as necessary for accuracy and precision, while employing low-fidelity simulation (LFS, here meaning steady-state) where possible for speed. Such capabilities are referred to as multi-resolution simulation (MRS) [2, 3, 4]. However, the state of the art in MRS assumes event-driven time management, which is not suitable when differential-algebraic models for infrastructure elements are included (unsurprisingly, systems with continuous variables – like the voltages, currents, and frequency in the power grid – are anathema to more computer- and communications-oriented simulation approaches). Therefore, the goal is multi-resolution, multi-time-scale simulation that successfully integrates HFS as a type of MRS capability for SCEPTRE.

Some situations may require real time (as a specific case of multi-time-scale). However, real time (RT) simulation for large systems can be expensive [5], therefore an effective HFS-SCEPTRE will use it selectively. Two possibilities are crucial:

- Hardware-in-the-loop (HITL) for analog equipment (AEQ) using HFS
- Human-interactive simulation (HIS)

AEQ refers to infrastructure control devices that depend on measuring analog signals for their functionality, like a protective relay for the power grid. Other equipment (called digital equipment – DEQ) instead functions based on typical information systems communications, like packetized data (which can be called digital I/O – DIO). All HITL simulations demand RT, although there are varying degrees of difficulty with HITL (especially for AEQ). In many cases, HITL functions perfectly well with LFS (as applied in the current SCEPTRE); occasionally, the behavior of an AEQ component depends on RT-HFS data.

If the AEQ were not HITL (i.e. it was simulated or emulated), then the element might be instantiated with adequate accuracy using some descriptive modeling language, following which HFS data can be used to gauge its behavior via virtualized analog input/output (VAIO). Therefore, the non-HITL AEQ might possibly be simulated in non-RT with HFS data. However, if the actual, physical AEQ is a necessary FICSS element for accuracy or precision, then the overall simulation construct will necessarily require some HITL support with hardware analog input/output (HAIO); note that until live (or physical) infrastructure elements are incorporated into SCEPTRE, all HAIO is "born" as VAIO.

For situations requiring HFS, VAIO is obviously preferred for better simulation economy, although it is still a complex problem (besides needing HFS simulation, simulated or virtual AEQ will require myriad signals with varying time decimation and state variables to work directly). Conveniently, many HITL devices are generally content with LFS-derived HAIO and DIO, like components in utility SCADA and EMS.

Also regarding HAIO, there is a need for an automated configuration and deployment process, ACD-HAIO, to support SCEPTRE starting HITL/HAIO evaluations based on HFS conditions that may not be fully known until that specific point in the simulation. Given the experiential nature of SCEPTRE, any particular sequence of events (SOE) that might instigate HFS to gauge the response of some equipment requiring HAIO is most likely not discernible *a priori* (because of the presumed computational infeasibility of enumerating the space of potential – or even likely – SOE). Therefore, SCEPTRE itself must be capable of configuring HAIO as necessary depending on the current SOE. (Note that the analogous ACD-VAIO is not called out as a specific capability, as the ability to manage VAIO is presumed to be a necessary element of HFS. Translating VAIO into HAIO is expected to be a significant challenge.)

There is an additional important subtext here. If a FICSS drives control devices in chunks of discontinuous real time (DRT) using HFS, then the overall absolute clock time (ACT) may be lost (limited FICSS resources could also cause the simulation environment to run slower than RT). In many cases, controls and other devices need to understand what the actual wall clock time is, as opposed to just how much time has elapsed from some arbitrary moment. The FICSS may need to set time as an initial condition for these. ACT could be especially crucial when evaluating cyber attack forensics, as the correlation will no doubt be highly dependent on time (other examples might be synchrophasor applications or the use of GPS signals in substations).

It is expected that some AEQ HITL using HAIO might require continuous RT (CRT) at a time scale that cannot be supported without the use of application-specific simulation hardware. As currently envisioned, the HAIO capability would permit DRT after a complete cycle for an individual AEQ component – once through the output (stimulus) into the AEQ and then its reaction (captured as input). In specialized applications where the speed and interactivity of the needed CRT application is critically important, the HFS-enabled FICSS would transfer a subset of the HFS model to some RT-capable hardware for the required duration to ensure overall accuracy. HFS-RT is envisioned as necessary only for limited instances of HITL AEQ.

Finally, HIS presents a unique challenge. Already, SCEPTRE is a FICSS that allows for HIS using LFS. Transitioning to HFS might easily lead to situations where DRT is necessary due to system simulation limitations. If the HIS characteristics necessitate CRT at the same time as HFS, then there must be a workaround.

Table 1.2 summarizes the needed capabilities discussed in this section. For each entry, examples (mostly relating to the power grid) are provided.

Table 1.2: Technical capabilities of FICSS and current status within SCEPTRE (with examples from power grid analysis).

Acronym	Definition	Interpretation	Example(s)	In SCEPTRE now?
LFS	Low-fidelity simulation	Load flow	Voltages change when a line is lost	Yes
HFS	High-fidelity simulation	Dynamic or transient simulation	Frequency or voltage oscillate post-disturbance; generator regulator	No
HFS-RT	HFS in real time	Real time transient simulation	Relays interact with part of the HFS model hosted by specialized hardware	No
DRT	Discontinuous real time	Simulation time advances according to resource scheduling	Pausing the FICSS to allow necessary computation	No
CRT	Continuous real time	Simulation time advances with wall clock	Current SCEPTRE operation	Yes
DEQ	Digital equipment	Conventional IT	Router, SCADA SW, virtualization environment	Yes
AEQ	Analog equipment	Infrastructure-specific embedded devices	RTU, PLC, relay	Yes (simulated & prototype HITL)
DIO	Digital I/O	IT-style communications	SCADA data packets, domain security services	Yes
VAIO	Virtual analog I/O	Measurements and controls, encapsulated within DIO	Simulated RTUs get bus voltages via Ethernet from LFS; relay in Simulink gets bus voltage signal from HFS	Yes (LFS only)
HAIO	Hardware analog I/O	Signals on actual wires	Physical relay sends/receives measurements and trip decisions using actual voltages and currents	Yes (prototype, LFS only)
ACD-HAIO	Automated configuration & deployment for HAIO	Same as HAIO	Physical relay sends/receives measurements and trip decisions using actual voltages and currents	Yes (prototype, LFS only)

1.2 The Importance of HFS, Advanced HITL, and RT

To better understand the potential impacts of attacks and exploits, Red Team personnel have often used SCEPTRE as a testing environment. Attacks against communications, SCADA, and field devices propagating into the modeled infrastructure have greatly improved the understanding of likely impacts. However, the current SCEPTRE is limited to LFS. Threat analysis suggests that attacks that depend on the dynamic character of the system are likely, necessitating the move to HFS. As an example, in previous work Sandia showed the effects of an attack against a SCADA system that tripped several lines and generators, but the available LFS modeling only showed the effects from subsequent overloads and undervoltages on the system. A better approach using HFS would also factor the resulting frequency oscillations into account, particularly as they lead to trips by under- and over-frequency relays.

Continuing from that example, the relays themselves (and other embedded devices like PLCs and RTUs) could come under attack by subtle adversaries with advanced capabilities. Exploits against devices that react depending on the dynamic character of the infrastructure will necessitate HITL and HFS capabilities for these elements. Currently, SCEPTRE supports HITL for field devices via HAIO, but only for LFS (also, this capability is only at the prototype stage). Adding HAIO support for HFS and HITL is a necessary development. To maintain necessary automation of the simulation, the HAIO process must be automatically configurable and managed by SCEPTRE to the degree necessary to answer questions about HITL response caused by HFS. This capability may be incorporated into a generalized automated configuration scheme, such as those being developed for SCEPTRE SCADA/EMS deployment.

Finally, the question of the degree of RT depends on the expected use case. The current expectation is that HFS will result in DRT, which is deemed acceptable for Red Team experiments (provided elements that need ACT can be accommodated) – with one significant exception. The training effectives of Red Team personnel could be severely impacted if limited to DRT; therefore, the enhancement of SCEPTRE with HFS and advanced HITL must allow for some degree of scenario playback in CRT to support this key use case. (A scenario is defined as a sequence of experiments that run in CRT to support training of Red Team personnel with respect to a particular sequence of attacks.) Given that hardware limitations will likely require DRT for any open-ended experimental analysis, CRT training scenarios will depend on known equipment responses to decrease or eliminate the need for HFS which causes DRT. The use cases in this section are summarized in Table 1.3.

Table 1.3: Use cases for HFS in SCEPTRE.

RT Type	Use Case	Comments
DRT	Red Team experiments	Time management is done by SCEPTRE software, supporting HITL, HIS, and ACT as necessary
CRT	Red Team scenarios	Depends on known HFS responses and scripted events to reduce HFS and eliminate DRT

Chapter 2

Planned Approach for Integration of Dynamic Simulation

2.1 Current SCEPTRE Operation

Currently, SCEPTRE relies on a series of successive load flows to approximate the behavior of the power grid. A load flow solves for the system's SEP. Within SCEPTRE, if a new SEP is not easily calculable, or does not exist, then the system fails to an error condition (see Figure 2.1).

As discussed previously [5], one method for integrating time-oriented infrastructure simulations with real-time communications and control is to ensure that adequate hardware is present to run quickly. However, this doesn't appear to be feasible with existing SCEPTRE packages like PowerWorld, and so different measures are necessary. In any case, the software does not allow reading of signals during simulation, so its interactivity is insufficient. An alternative will be suggested, based on the expected usage of the FICSS (equivalently, the HFS-SCEPTRE) capability.

2.2 Example for Dynamic Simulation Approach

Consider the simulation timeline shown in Figure 2.2. The system state is $\bar{X}_k^-$, and it is presumed operational and without any activity that would necessitate HFS simulation for time immediately prior to $t = t_k$. At that time, some part of the system experiences a change, corresponding to control input change from $\bar{U}_k^- \rightarrow \bar{U}_k$. The change could be as a result of other controls managing the infrastructure process, or might be directly caused by an experimenter, looking to stimulate the system and gauge the response. The simulation engine (SE) must determine if the change will:

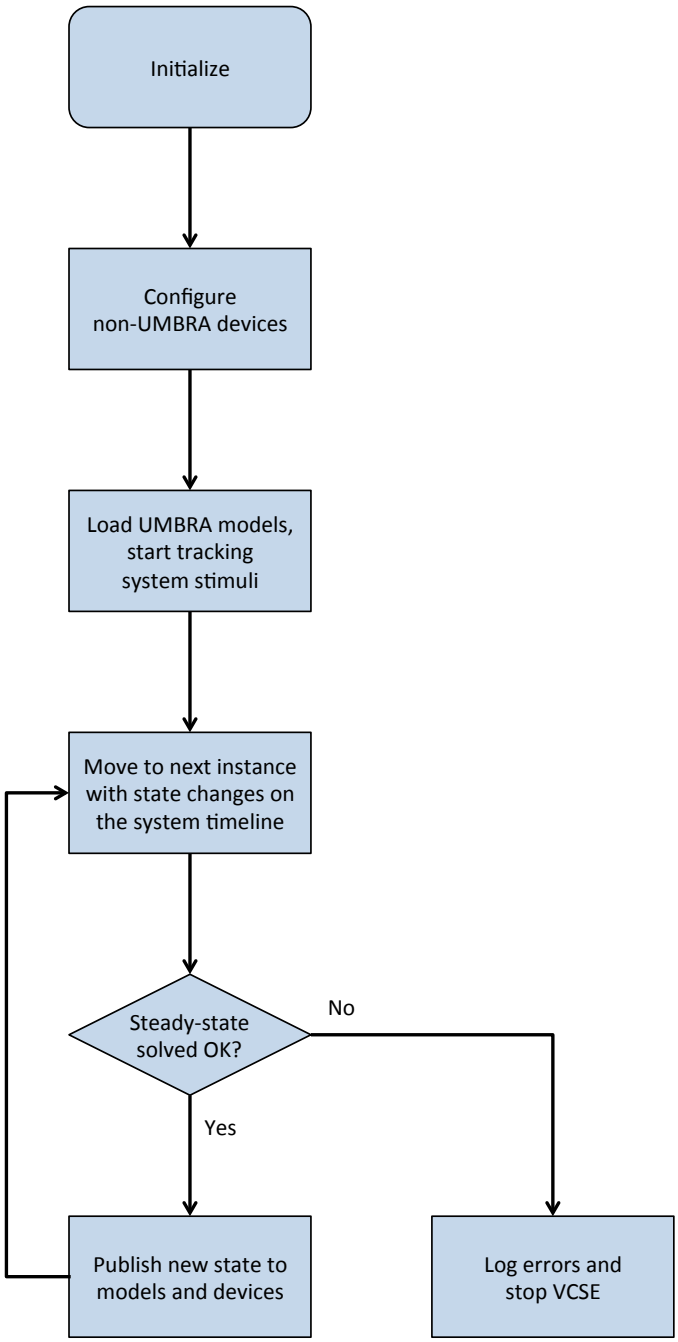

Figure 2.1: Flowchart for current SCEPTRE.

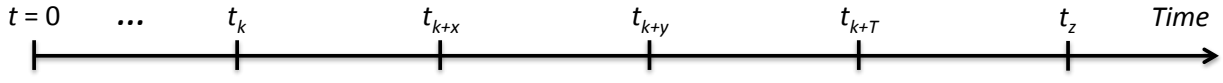

Figure 2.2: Simulation timeline.

1. Cause a significant change relative to the system state $\bar{X}_k^-$, and compute the new possible steady state $\bar{X}_z$ where $t_z > t_k$ is some unknown future settling time, and also ...

2. Cause a system transition from $\bar{X}_k^- \rightarrow \bar{X}_z$ that will necessitate HFS simulation to ascertain its true effects (i.e. either that state $\bar{X}_z$ is known to lead to other control action for $t_k \leq t < t_z$, or that the path from $\bar{X}_k^- \rightarrow \bar{X}_z$ will contain a path that will lead to further control action during the same interval.

If the answer to #2 is true (which will depend upon an analysis of the components in the system and a rough idea about the potential system behavior) then the SE must compute:

3. State $\bar{X}_k$, which will include changes to whatever state variables can change state instantly, and forms the necessary set of initial conditions for subsequent analysis

4. Time T which represents a sensible initial time horizon for system dynamics starting at $t = t_k$

5. The system dynamic response from time t_k until $t = t_{k+T}$.

Assume that the necessary system response functions are passed to subscribing model entities within SCEPTRE, and that analysis shows two responses (that could, but not necessarily, lead to further dynamic analysis) from devices X and Y, at times t_{k+x} and t_{k+y} respectively. If the control response $\bar{U}_{k+x}$ could lead to further dynamics of any kind, then we disregard point Y and re-enter the analysis at #3, with $t_{k+x} \rightarrow t_k$. Otherwise, consider if $\bar{U}_{k+y}$ could lead to further dynamics; if so, return to #3, otherwise move to time t_{k+T}, set $t_k \rightarrow t_{k+T}$ and then return to #3. If the system appears to have settled (i.e. T is very small or zero), then set $t_z = t_{k+T}$ and continue with the analysis.

2.3 Integrating HFS with SCEPTRE

The integration of HFS into SCEPTRE, or indeed developing an arbitrary hybrid simulation environment with HFS for the physical systems irrespective of SCEPTRE, is a complex issue. Together, Tables 1.2 and 1.3, Figure 2.1, and Section 2.2 represent the needed concepts. The planned flowchart for a new SCEPTRE with the HFS capability is shown in Figure 2.3. The left side represents the SE management and the (preferred) LFS execution, while the right covers the new HFS capability.

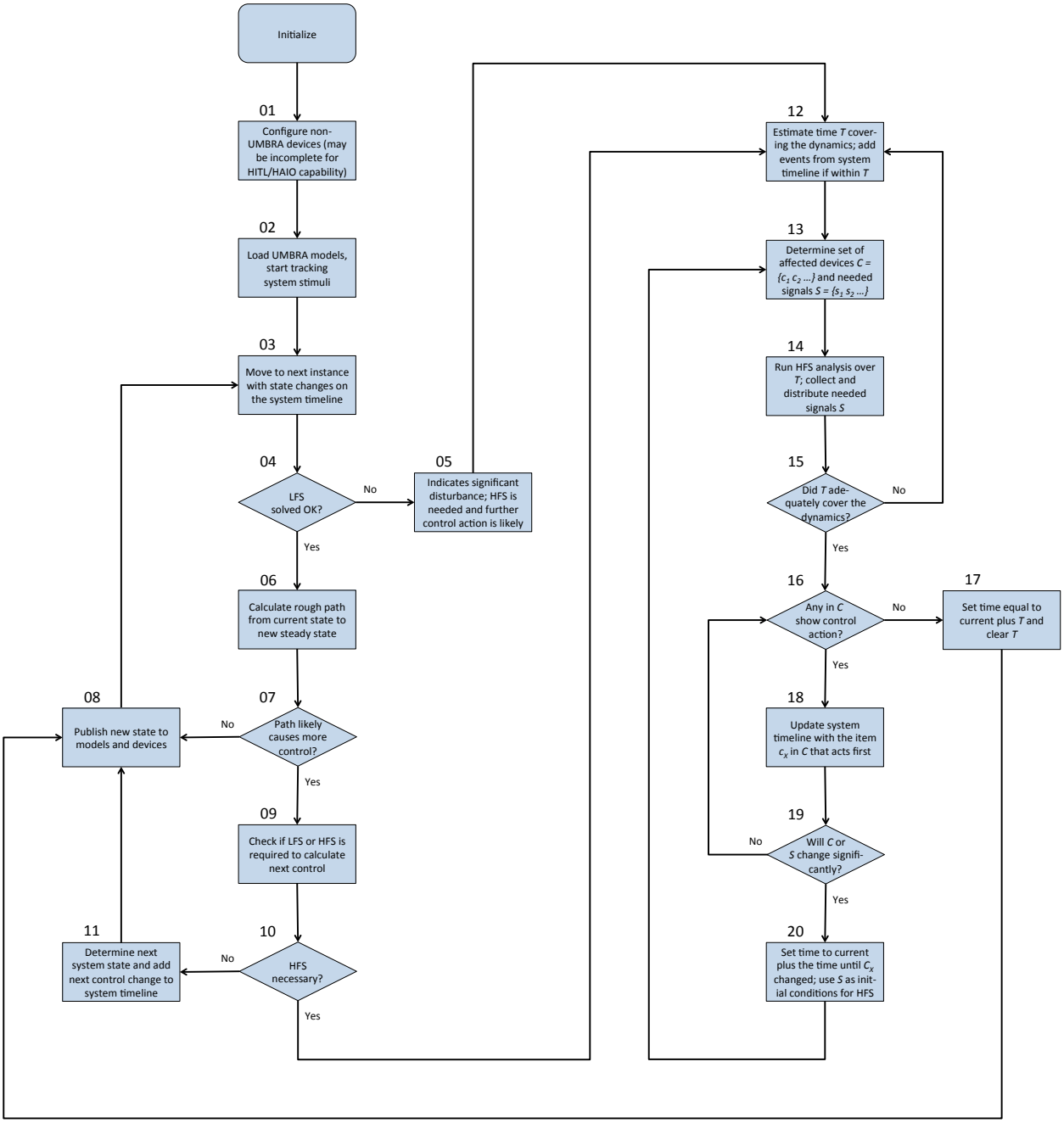

Figure 2.3: Flowchart for the planned HFS-SCEPTRE.

Each block is detailed in the following section, to support full understanding of the intended process. The Sandia-designed software Umbra acts as the SCEPTRE SE. Note that the flowchart corresponds only to the DRT use case; the adaption to CRT will be made later.

Block 01, activity: Configure non-Umbra devices (may be incomplete for HITL/HAIO capability)

Many elements in the hybrid simulation must be configured to run correctly, including networking/communications, virtual machines for control center software, security appliances, HITL relays, etc. Not all equipment can be completely configured; in particular, the HAIO setup may be initialized and connected, but the specific conditions that it will be simulating must wait until specific HFS conditions are known (the ACD-HAIO capability).

Block 02, activity: Load Umbra models, start tracking system stimuli

Umbra manages the system timeline. Umbra will also host models for several elements (at the ”simulated” or ”constructive” levels of abstraction). Finally, Umbra also tracks system stimuli entered by experimenters, as events on the system timeline. Users of SCEPTRE can enter events on the timeline by entering parameters into the SE, or possibly by interacting with the HITL elements within the running simulation (with the proviso that CRT is not guaranteed and DRT might result, particularly if HFS is necessary).

Block 03, activity: Move to next instance with state changes on the system timeline

The SE timeline supports event-driven simulation execution. The timeline is populated by event chains that result from stimuli entered by users, or naturally occurring changes in the system conditions (like changing load for the electrical grid throughout the day, or random loss of equipment due to reliability issues).

Block 04, decision: LFS solved OK?

The first step (as described in Section 2.2) is to attempt to calculate the next SEP for the infrastructure via LFS. The LFS calculation must be able to address common numeric or algorithmic issues (like poorly suited initial conditions for the variables that might affect convergence stability, or disconnectedness in the infrastructure graph). Then, if the calculation fails, then the nonexistence of a SEP can be assumed, which necessitates HFS.

Block 05, activity: Indicates significant disturbance; HFS is needed and further control action is likely

Given the lack of a SEP, the change that caused the abortive LFS solve represents a significant, stability-threatening event. The solution path will transition to HFS to support the probable stability-preserving control actions of the infrastructure controls.

Block 06, activity: Calculate rough path from current state to new steady state

The existed of a SEP as determined by LFS *does not necessarily* preclude the need for further analysis. Possibly, the transition to the new state might cause automated control action which could necessitate HFS on account of the potential infrastructure dynamics. Calculating the "rough path" without resorting to full HFS requires some R&D to understand the analysis tradeoff space and optimize the algorithm. However, SCEPTRE will need this capability to avoid full HFS for every event, which is necessary to preserve its efficiency.

Block 07, decision: Path likely causes more control?

If the "rough path" calculation does not lead to further control, then SCEPTRE can safely assume that the original stimulus event from step 03 is accurately characterized by LFS. Otherwise, there are additional considerations.

Block 08, activity: Publish new state to models and devices

The SE delivers various VAIO and HAIO to from the LFS to control system devices. This will very likely stimulate new DIO, but no additional automated control affecting the physical process.

Block 09, activity: Check if LFS or HFS is required to calculate next control

Provided that additional control action is likely given the original LFS calculation and "rough path" analysis, then another question arises: will LFS be sufficient to understand the evolving character of the infrastructure and associated devices? LFS is preferable due to its efficiency, although it is less precise and accurate than HFS. The issue will require analysis similar to, and building upon, the "rough path" analysis mentioned in Block 06.

Block 10, decision: HFS necessary?

The results from the analysis in Block 09 determine the direction of SCEPTRE. If LFS is insufficient to understand future control, then SCEPTRE will move toward HFS.

Block 11, activity: Determine next system state and add next control change to system timeline

Here, HAIO or VAIO that will lead to automated control (only based on LFS in this case) is delivered to infrastructure control devices, and the next control that results (with its timestamp) is captured and placed on the SE timeline as a part of the event chain corresponding to the original stimulus.

Block 12, activity: Estimate time T covering the dynamics; add events from system timeline if within T

Once the SE elects HFS, the first step is to estimate the time horizon of the dynamics, in order to support a transition back to LFS as soon as feasible. The estimation of this period *T* is another R&D question, similar to Block 06. Possibly, the value for *T* might encompass additional events from the system timeline (possibly resulting from Block 11 action or additional system stimuli); these events must be included recursively in the analysis for *T*.

Block 13, activity: Determine set of affected devices $C = \{c_1\ c_2\ \ldots\}$ and needed signals $S = \{s_1\ s_2\ \ldots\}$

As preparation for HFS and to bound the necessary analysis, the set of control devices *C* must be determined. This analysis is a third instance of an activity that is not fully detailed, although it has a similar character to the calculation for *T* in Block 12. Also, once the set of devices is enumerated, then the set of needed signals (voltage, current, pressure, temperature, switching, etc.) will be tabulated, to ensure that HFS produces all necessary calculations. The specification will also include the required time decimation for the signals in *S*. Note that may be delivered as VAIO or HAIO.

Block 14, activity: Run HFS analysis over T; collect and distribute needed signals S

The SE will link to some HFS capability and perform the needed analysis. Most often, an HFS evaluation will not provide the needed signals *S* until the HFS is completed. The distribution of *S* would preferably be via VAIO, as these may be asynchronous and possibly faster than RT (as VAIO suggests non-HITL simulation or virtualization for control devices). For HITL AEQ, HAIO will be generated and measured as necessary using the required ACD-HITL capability and / or HFS-RT if required.

Block 15, decision: Did T adequately cover the dynamics?

Once the HFS is completed, the SE must ensure that *T* was in fact sufficient. This determination requires that *T at least* extended beyond the first control action taken, or until all dynamics are damped below any reasonable expectation of relevancy. If there are still significant dynamics evident in *S* without any control action, then the SE must reconsider *T* in Block 12.

Block 16, decision: Any in C show control action?

The entire point of HFS is to accurately model the control response for the infrastructure system. However, the greater accuracy of HFS (was compared to the estimations made to this point) might lead to a result where *T* was sufficient, and yet no controls reacted.

Block 17, activity: Set time equal to current plus T and clear T

If no control action is forthcoming, then there are no additional entries to be made on the system timeline, and the system can revert to its pre-HFS state in Block 03 once the final conditions have been propagated to all devices in Block 08.

Block 18, activity: Update system timeline with the item c_x in C that acts first

All devices in C *might* react to their corresponding signals in S. However, it is unlikely to be clear in advance of the actual HFS calculation which one will react first, because until Block 14 everything has been only estimated. Therefore the initial determination for the HFS is the identification of the first reacting control c_x, with the assessment of the remainder of C to follow.

Block 19, decision: Will C or S change significantly?

There is a significant likelihood that the HFS signals in S that occur after (i.e. later in time) than the first control action will be inaccurate. The question depends on the impact that the action will have on S, or if it will lead to additional devices in set C. The determination will be made using techniques similar to the analysis in Block 13. If neither will change significantly, then the SE can re-use S after c_x reacts in order to determine the next control device that is affected (by returning to Block 16 – obviously, x is cleared). Otherwise, the SE must re-compute the HFS under the new conditions (caused by c_x).

Block 20, activity: Set time to current plus the time until c_x changed; keep old S to use as initial conditions for HFS

Given the need to recompute the HFS, the SE will advance the time appropriately and return to the HFS starting block. The previous set of signals S will be used as initial conditions for the subsequent HFS calculations.

2.4 Specific R&D Gaps

The development in this chapter has highlighted several capability gaps, which must be addressed before an HFS-enabled SCEPTRE can be fielded. The requirements are tabulated in Table 2.1.

As described previously, ACD-HAIO and HFS-RT are necessary to support HITL AEQ. Neither can be fully pre-configured; in both cases, although the *types* of the signals can be known beforehand, the values are not. Furthermore, the character of the infrastructure (as affected by the simulation stimuli) significantly impacts the HFS – and would drive the implementation of any needed HFS-RT. Both should be automated to the extent feasible (in order to minimize the impact on the overall simulation time) while still preserving the extensibility and openness of the SCEPTRE architecture. The likelihood is that the addition of key domain-specific networking protocols to SCEPTRE will enhance the degree of automation by allowing the SE to interact directly with either the HFS-RT hardware or AEQ.

Table 2.1: Use cases for HFS in SCEPTRE.

Block	R&D Need	Comments
04	LFS calculation stability	The HFS software (e.g. PowerWorld) must be well enough automated that calculation failures are attributable to large disturbance dynamics
06	LFS "rough path"	The path analysis from prior SEP to new must support the determination of likely control caused by the transition
09	LFS / HFS determination	Building on the path estimation, the determination of HFS/LFS also depends on the character of the likely set of impacted controls
12	HFS interval estimation	To avoid running an open-ended HFS, the SE must estimate the interval T as the shortest but most reasonable interval likely leading to automated control action
13	HFS controls estimate	Rather than generating an arbitrarily large set of signals to support all controls, the HFS calculation time can be limited by selecting the most likely subset of affected controls, according to the situation – although this is not a capability that currently exists
14	HFS automation	The automated configuration and execution of the HFS, and distribution of the HFS results as signals via VAIO and HAIO will require significant integration work (the ACD-HAIO and HFS-RT capabilities will also be challenging)
19	Post-HFS analysis	Once an initial automated control reaction is identified, the SE must determine the usability (if any) of the remaining HFS analysis results

2.5 Adaptation to RT Scenarios

The discussion in the preceding sections have referred to the DRT implementation of the HFS-capable SCEPTRE (with the notable exception of brief periods of HFS-RT as needed for AEQ HITL). However, the discussion in Table 1.3 clearly indicates the need for some sort of CRT HFS capability to support the Red Team scenario use case.

The intended solution for this apparent incompatibility is to reduce the freedom allowed to Red Team personnel during CRT simulations by limiting them to a preordered set of actions (the "scenario"). The need for HFS can be eliminated by ensuring that key parts of the scenario that would otherwise have led to HFS-induced periods of DRT are calculated and stored prior to the scenario exercise.

This approach has the advantage of simplicity, as the only needed development is the ability to generate scenarios from DRT experiments. In turn, this can be realized though a careful databasing strategy the operates during DRT testing, and the construction of a scenario assembly algorithm that draws from the data store. The down side is the lack of flexibility in the options for the Red Team personnel, but the fixed nature of the planned CRT scenario support is quite amenable to the stated intent of training.

Chapter 3

Specific Applications of Dynamic Simulation to the Power Grid

Controls and data for the electric power grid (EPG) can be broadly categorized into five groups:

- Automated grid management and control (AGMC): frequency, voltage, load management, etc (anything automated, except for protection)
- Supervisory control: human-in-the-loop grid management (i.e. system operators at the control center)
- Protective relaying: detection of abnormal or hazardous conditions (also automated, with time sensitivity on the order of cycles)
- Configuration management (CM): device (re)configuration, downloading fault data, engineering configuration, security settings, etc.
- Cyber security awareness and management (CSAM): Feedback on current security conditions from host- or network-oriented sensors

The applicability of the key SCEPTRE technologies identified in Chapter 1 are summarized in Table 3.1. Included examples span all five groups, with additional detail where appropriate.

Table 3.1: Use cases for various capabilities in HFS-SCEPTRE.

Capability	Comment
LFS	Line and equipment trips that do not affect stability; negatively affecting system data flows to inhibit situational awareness or correct operation; effects of overloads or heating from phase unbalances; fault studies to understand protection performance with various settings (like aggressive overreaching on distance relays); accelerated equipment wearing
HFS	Effects to equipment that lead to local or wide instabilities (frequency or voltage); machine stability; process control (e.g. turbines, steam, coolant, lubrication), point-on-wave switching effects (including synchronism issues); arcing behavior
HFS-RT	May be used for AEQ HITL involving high-precision analysis of transient stability; protection performance (detection and clearing time); machinery/process effects (VFDs and motor control, asynchronous switching, etc)
DRT or CRT	In most cases (not including scenario-based training), DRT is entirely appropriate, with the proviso that devices that rely on ACT are carefully managed (examples may include GPS-dependent synchrophasors, tertiary optimizing control that is triggered by the ACT, and cyber security detection and logging countermeasures embedded in the control systems)
VAIO	Already, the majority of SCEPTRE-simulated devices get data via VAIO, but only from LFS; devices like PLCs involved in process control, and over/underfrequency relays would benefit from HFS-derived VAIO; newer technology for grid automation allows VAIO over standardized protocols
HAIO	Only relevant for AEQ HITL, but particularly important given the likelihood that the AEQ is included as a key element in the analysis; HAIO for HFS would drive relay or PLC inputs and hide the simulation artifice, ensuring confidence in the AEQ behavior

Chapter 4

Conclusions

The process for achieving the HFS-SCEPTRE and robust HFS-RT/ACD-HAIO is complex, but will be extremely valuable to support Red Team analysis for control systems. The overall approach is to minimize the need for CRT and HFS, in order to optimize time and resource usage for the simulation. The key developments and technical requirements were discussed in this article; some of these are considerable R&D questions, while others are significant technical challenges. However, a well-engineered HFS-SCEPTRE will be essential for understanding cyber security issues with realistic responses from the underlying physical system.

Bibliography

[1] Jason Stamp, Vince Urias, and Bryan Richardson, *Cyber Security Analysis for the Power Grid Using the Virtual Control Systems Environment*, Power and Energy Society General Meeting (24-29 July 2011).

[2] Keqiang Su and Wenxing Fu, *Designing Hardware-in-the-loop Simulation System for Missile with High Level Architecture*, 2011 International Conference on Mechatronic Science: Jilin, China (19-22 August 2011).

[3] Anand Natrajan, Paul F. Reynolds, Jr., and Sudhir Srinivasan, *Guidelines for the Design of Multi-resolution Simulations*, DMSO Proposal (03 Jul 1997).

[4] Paul F. Reynolds, Jr., Anand Natrajan, and Sudhir Srinivasan, *Consistency Maintenance in Multiresolution Simulations*, ACM Transactions on Modeling and Computer Simulation, Vol. 7, No. 3, pages 368-392 (Jul 1997).

[5] Derek Hart and Bryan Richardson, *Real-Time Simulation of Electric Power Systems Using Steady-State Solvers*, Sandia National Laboratories report: Albuquerque, New Mexico (22 Dec 2011).

Appendix: Sandia National Laboratories Contact Information

Table 4.1: Contact Information

Name	Organization
Jason Stamp *Technical Lead*	Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0671 jestamp@sandia.gov
Derek Hart *Project Lead*	Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0671 dehart@sandia.gov
Jennifer Depoy *Sandia Program Manager*	Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0671 jdepoy@sandia.gov

Report Distribution

1 Bryan Richardson
Fortalice Solutions
809 W Hill Street
Charlotte, NC 28208

1 MS0671 Derek Hart, 5624
1 MS0671 Neeta Rattan, 5623
1 MS0671 Jason Stamp, 5623
1 MS0671 Jennifer Depoy, 5628
1 MS0899 RIM-Reports Management, 9532 (electronic copy)

Sandia National Laboratories