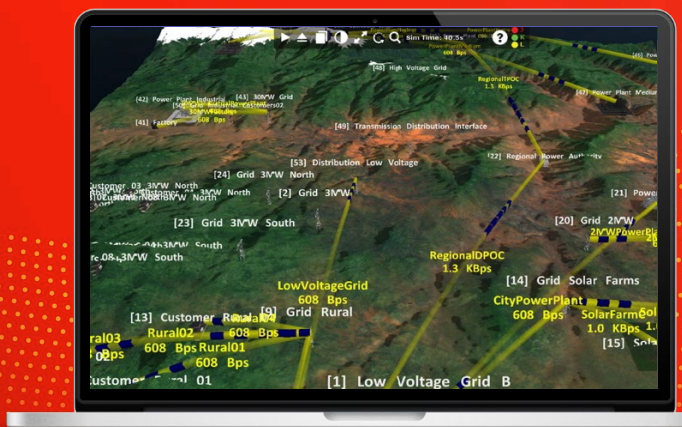
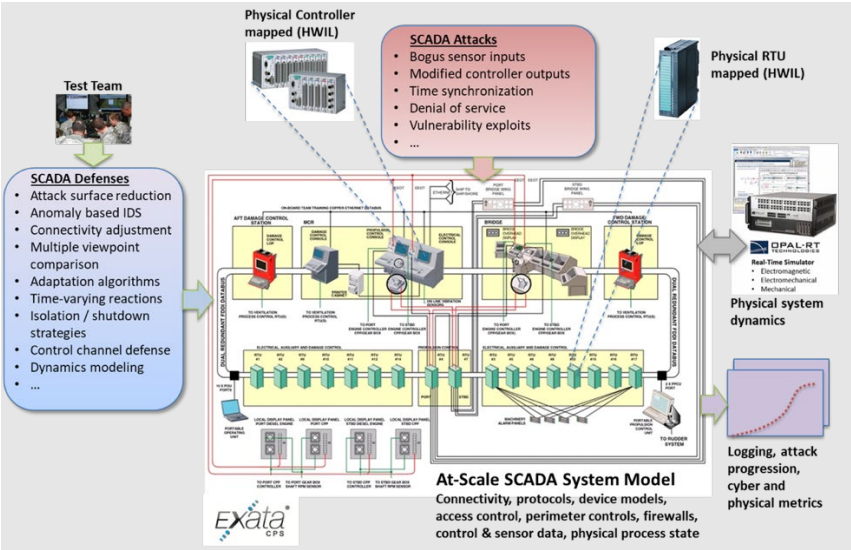


TECHNICAL OVERVIEW

EXata Network Modeling – Critical Infrastructure

EXata for Cyber-Physical Systems

Connecting Supervisory Controls and Data Acquisition (SCADA) systems and Operational Technology (OT) devices via the Internet has significantly improved accessibility, automation, and efficiency, but it also introduces vulnerabilities. Every communication line is a potential attack surface. Because of this, cyber threats against public utilities and other critical infrastructure are just as ubiquitous as attacks on government and corporate computing infrastructures. By causing loss, denial of access, or manipulation of system view and control, cyber attacks against SCADA systems, i.e., power generation and distribution systems, water treatment plants, and transportation facilities, can cause widespread disruption of commerce and daily life.



1 Top 5 Critical Infrastructure Cyber Attacks. https://www.cbronline.com/cybersecurity/top-5-infrastructure-hacks
2 The Top 20 Cyber Attacks Against Industrial Control Systems. https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_DEC_17/Waterfall_top-20-attacks-article-d2%20-%20Article_S508NC.pdf

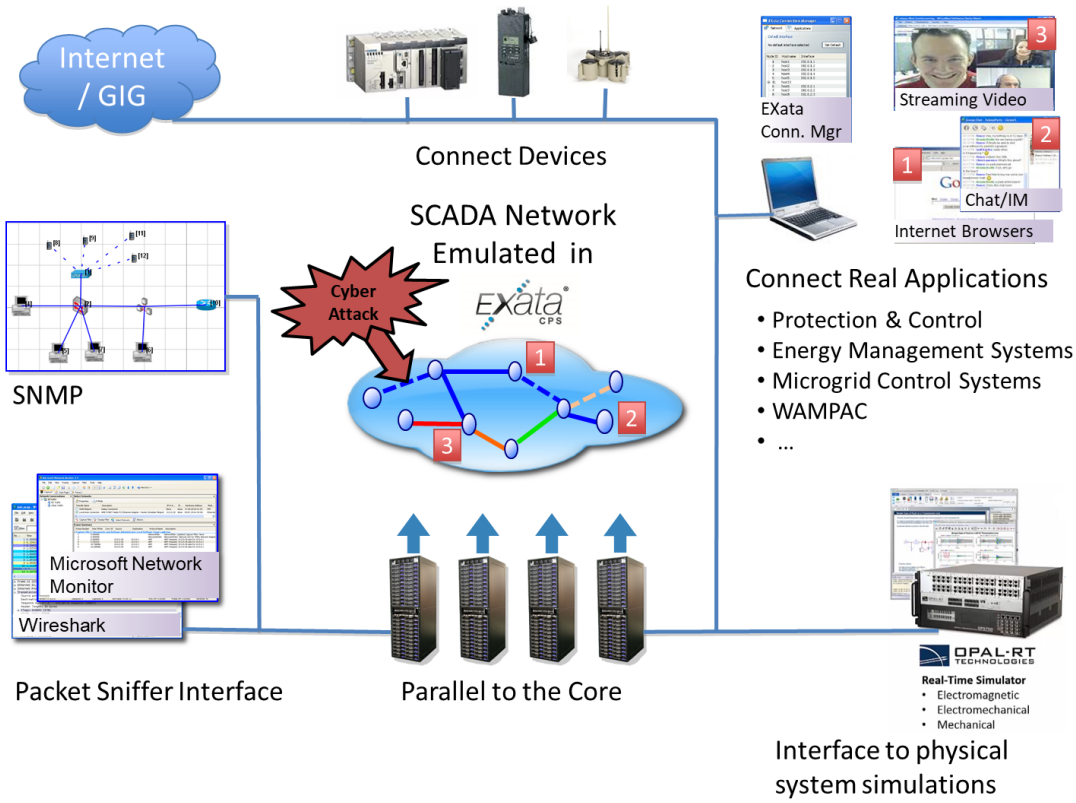
KEYSIGHT TECHNOLOGIES

There is a pressing need for operators of SCADA systems to determine how resilient their operational systems are to cyber attacks and to develop plans to mitigate the associated risks.

Simulating these cyber-physical systems in a lab is a safe way to investigate their vulnerabilities and develop defenses without compromising the real systems. To test the cyber resilience of such a system, it is important to simulate the dynamics of both the physical system and the underlying communication fabric, i.e., the communication system used by the cyber-physical system, which can be the target of cyber attacks.

Keysight Network Technologies has developed a high-fidelity network emulator, EXata – Critical Infrastructure, to simulate the underlying communication fabric of electrical grids and test the cyber resilience of such systems. EXata – Critical Infrastructure is integrated with OPAL-RT's HYPERSIM simulator on the same hardware (or box) to offer a complete real-time cyber-physical solution for the development, testing, and assessment of electrical grids with communication networks. HYPERSIM, which simulates the physical system, is the only real-time digital simulator with the power to simulate electromagnetic transients of large-scale power systems, tackling operational and reliability issues threatening a power system's cybersecurity. This integration of EXata – Critical Infrastructure and HYPERSIM provides a way to test the resilience of power systems to cyber attacks and improve their cyber defenses, thereby helping to ensure cybersecurity, reliability, and efficiency of such systems.

SCADA Network Emulated in EXata



Because EXata – Critical Infrastructure and HYPERSIM reside in the same box, they can employ low-latency communications at Layer 2 (MAC or link layer) to analyze cyber threats that can be injected at these lower layers in the physical system. An example is an attack on a power grid control system that modifies sensor messages to the controller, reporting less power than is actually available, leading the controller to shed power by stopping service to some residential consumers. Another example is an attack that delays a message from a controller to an actuator to shut down a generator, possibly leading to overloading and damaging parts of the grid.

EXata – Critical Infrastructure provides a way to more effectively identify and visualize the impact of cyber attacks on monitoring and control systems used by power systems. With EXata – Critical Infrastructure, specific environments can be replicated in a lab and “what-if” scenarios can be quickly evaluated to determine what happens to power systems if they are subjected to cyber attacks.

EXata – Critical Infrastructure leverages Keysight’s EXata simulation/emulation software, which is a tool for planners, analysts, IT technicians and communication specialists to create software models of all types of communication networks. The models are used to study the performance of networks under different operational conditions to identify and find solutions to potential problems and to investigate the resiliency of the network to cyber threats. The models are comprised of nodes representing network elements and endpoints (e.g., routers, switches, radios, sensors, PCs, servers, firewalls and other security equipment) and the links that connect the nodes (e.g., buses, LAN segments, radio transmissions, Wi-Fi signals, LTE connections, etc.). Hardware elements (live or simulated by HYPERSIM) can be integrated into the EXata – Critical Infrastructure emulation by means of the system-in-the loop capability. Since EXata – Critical Infrastructure uses an efficient kernel designed to leverage multi-core and parallel processors to dramatically increase the event processing rate and hence simulation execution speeds, it can run emulations of networks comprised of thousands of nodes at real-time speeds with real-world high fidelity.

Benefits of EXata Critical Infrastructure

Some of the benefits of EXata – Critical Infrastructure are:

- Integration of emulated network with equipment and physical system dynamics simulation
- Packet-level emulation to predict system behavior under attack
- Scalability to represent the entire network while respecting timing constraints
- Run "what-if" scenarios of control systems under cyber attack without threatening operations
- Assess the effectiveness of tools, techniques, and architectures to ensure system availability
- Measure and improve system resiliency and develop plans to mitigate risks from cyber attacks

- Packaging of EXata – Critical Infrastructure and HYPERSIM in the same box enables fast communication at Layer 2, ensuring that the timing constraints of the overall system can be met

Communication Protocols Supported by EXata Critical Infrastructure

EXata -Critical Infrastructure communicates with HYPERSIM via the following protocols:

- Generic Object-Oriented Substation Events (GOOSE), subset of IEC61850
- C37.118 (over TCP/IP), used by synchrophasors
- DNP3 (over TCP/IP)
- Modbus (over TCP/IP)

EXata – Critical Infrastructure and Time-Criticality of Power Systems

Power systems often have stringent timing constraints. For example, the IEC61850 standard (global standard for electrical grids) has the following timing requirements:

- 4 ms message delay for grid protection
- Phasor Measurement Unit (PMU) every 33 ms (bypasses transport and network layers). PMUs are the most important measuring devices in the future of power systems.

Attacks on systems designed for monitoring and operating electric power grids often target the timing and synchronization, e.g., an attack may delay a message to a controller, which may result in a generator not shutting down when intended. Because EXata – Critical Infrastructure and HYPERSIM are deployed on the same hardware, they can communicate at Layer 2, which entails much shorter delays than communication at higher layers of the protocol stack; this ensures that the overall timing constraints of the system can be met.

Types of Attacks and Defenses

EXata – Critical Infrastructure can model a number of types of attacks. The most important attacks that impact power systems are:

- Denial of Service (DoS) attacks: These attacks can bring down or make unavailable a critical piece of equipment.
- Packet modification attacks: These attacks make changes to the payload of packets and can result in:
  - Bogus input data, such as modified sensor data, which can lead to erroneous decisions by the controllers
  - Bogus output data, such as manipulated or misleading data sent to controllers, which lead to unintended or incorrect actions
  - Disrupt time synchronization by delaying delivery, which lead to instability in the physical system

The other types of attacks that can be modeled in EXata – Critical Infrastructure include:

- Passive attacks:
  - Eavesdropping
  - Network scanning
  - Port scanning
  - SIGINT
- Jamming attacks
- Vulnerability exploitation attacks
  - Attacks to corrupt files and databases
  - Hacking attacks
- Virus and worm propagation attacks
- Rootkit attacks
- Botnet attacks
- Backdoors and holes in the network perimeter
- Communications hijacking and man-in the-middle attacks
- Coordinated attacks
- Adaptive attacks

EXata – Critical Infrastructure can model the following types of cyber defenses:

- Firewalls: The firewall model is based on iptables. Firewall rules can be modified dynamically while the simulation is running.
- Intrusion Detection System (IDS)
- Anti-Virus System (AVS)
- Security logs and audit trails

Components of EXata – Critical Infrastructure

The major components of EXata – Critical Infrastructure are:

Emulator/Simulator

At the heart of EXata – Critical Infrastructure is an emulator/simulator, which uses state-of-the-art techniques to run simulations of large networks at a fast speed without compromising accuracy. EXata – Critical Infrastructure is based on a highly specialized kernel and efficient memory management techniques that result in very high simulation speeds. Furthermore, EXata – Critical Infrastructure exploits the computing power available on multi-processor platforms by employing efficient parallel discrete event simulation techniques and smart partitioning, i.e., dividing the workload optimally among the processors.

EXata – Critical Infrastructure GUI

The EXata – Critical Infrastructure GUI provides an easy-to-use platform to create, visualize, and analyze network scenarios:

- **Design Mode:** This mode is used to create virtual network models via an intuitive point-and-click drag-and-drop graphical interface. Virtual network models can include communication devices, wired and wireless links, mobility patterns of wireless users, physical characteristics such as terrain and buildings, protocols at all layers of the stack, cyber characteristics of devices, etc. Different types of applications and services that run on the network can be applied.
- **Visualize Mode:** This mode is used to observe and analyze network behavior as the simulation is running. Users can watch packets at various layers flow through the network and view dynamic graphs of real-time statistics.
- **Analyzer:** After the simulation completes, Analyzer is used to plot and analyze a large number of statistics collected during the simulation.

Scenario Player

Scenario Player provides very high-quality 3D visualization effects while a simulation is running. As in EXata – Critical Infrastructure GUI's Visualize mode, packets at different layers can be traced as they traverse the network. In addition, detailed information on the dynamic state of communication devices can be observed, including their cyber assurance states, i.e., if a node has been compromised and, if so, the extent of the compromise.

Statistics Database

In addition to a statistics file, EXata – Critical Infrastructure provides a high-performance database interface that allows time-series and statistical data to be stored in a database during the emulation run. Statistics can be collected at different levels of granularity from summary statistics at the system level to detailed statistics at the event level.

External Interfaces

EXata – Critical Infrastructure has the capability to federate seamlessly with other simulators, e.g., kinetic battlefield simulators, via High Level Architecture (HLA), Distributed Interaction Simulation (DIS), AGI's System Tool Kit (STK), and Socket interfaces.

System-in-the-Loop Capability

This capability allows other software or hardware elements to be integrated into a network model, e.g., EXata – Critical Infrastructure can include a real hardware device or its software model (modeled by a co-simulator) in a simulation.

Human-in-the-Loop (HITL) Capability:

Both EXata – Critical Infrastructure GUI's Visualize Mode and Scenario Player have an HITL interface, which enables users to interact with a simulation while it is running, e.g.,

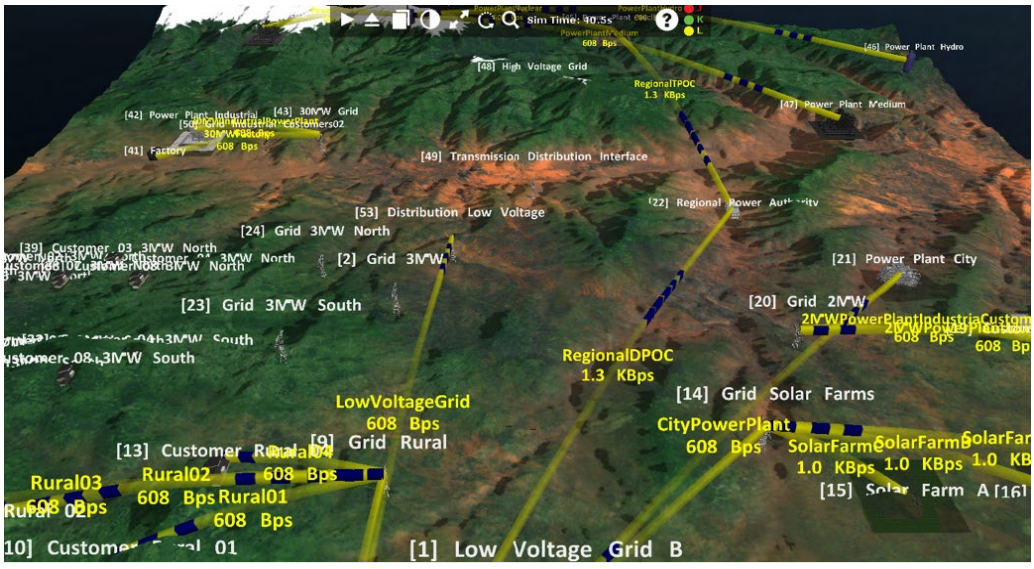
users can activate/deactivate nodes, launch and terminate cyber attacks, and modify firewall rules via the HITL interface.

Model Libraries

EXata – Critical Infrastructure includes an extensive set of high-fidelity models of communication devices, wired and wireless links, communication protocols, cyber-attacks and defenses, environmental factors such as terrain and buildings, and real-world applications.

These models are divided into a number of standard and optional libraries:

- Standard libraries
  - Cyber
  - Developer
  - Multimedia and enterprise
  - Wireless
- Optional libraries
  - Advanced wireless
  - Cellular
  - Federation interfaces
  - LTE
  - Military radios
  - Sensor networks
  - TIREM propagation interface
  - TIREM propagation interface
- al Mobile Telecommunications Service (UMTS)
  - Underwater communication networks
- Urban propagation



By using the models in these libraries, models of a large variety of communication networks can be built easily.

System Requirements for EXata – Critical Infrastructure GUI and Scenario Player

CPU

Dual-core 64-bit (x86-64 compatible),2.5 GHz processor or better

MEMORY

4 GB

VIDEO CARD

- For EXata – Critical Infrastructure GUI:
  Discrete graphics card with at least 128 MB memory supporting hardware 3D acceleration
- For Scenario Player:
  A graphics card with the following specifications:
  - 512 MHz or more core speed
  - 1 GB or more memory size
  - 1.5 GHz or more memory speed

DISPLAY

1024 x 768 or better resolution

OPERATING SYSTEM

Windows 10 Home or Windows 10 Pro (64-bits only)

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications, or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus