Webinar: HIL Testing for Power System Cybersecurity

Tuesday, June 30, 2020

Questions and Answers

Note: In this document and in general, the terms "GTNET" and "GTNETx2" are used interchangeably. These terms refer to the RTDS Simulator's network interface card, which is used for creating a closed-loop interface via communication protocols. GTNET is the original version of the card, and GTNETx2 is the most recent version. The main difference is that the GTNETx2 can run two protocols simultaneously instead of one. For more information, visit https://www.rtds.com/technology/communication-protocols/.

Q1: Will the slides/recording/RSCAD case files be made available?

Yes. The presentation and webinar recording are available to all participants. A link has been included with this document in the post-webinar email. A package including the NS-3 examples repository, the RSCAD case files for the demo, and some other instructional documents is available to RTDS Simulator users. Logging into your user account at support.rtds.com and clicking on "Downloads" allows access to these files. Please contact support@rtds.com if you have any issues.

Q2: Jitter delay is used to accomplish what attack in the microgrid? Can you elaborate?

It can be a Denial of Service (DoS) attack on one of the routers or any intermediary equipment. It will cause excessive delays and packet drops. You can increase the delay it to a high value to make the client or server request retransmission which adds to the problem. Otherwise, you can also use the random packet drops in the Linux Transmission control tool, tc, to drop a percentage of packets randomly to mimic the buffer overflows in intermediary equipment because of the Denial of service attack.

Q3: What is the limit on data retrieval through sockets? Number of data points, size, etc.

The RTDS Simulator's TCP/UDP socket firmware (the GTNET-SKT protocol) is capable of sending and receiving up to 300 data points per packet, with each point defined over 4 bytes. The data transmitted can be of either integer or floating-point (IEEE 754) type. Note that these are the capabilities for a single instance of a GTNET-SKT firmware license installed

RTDS Technologies Inc.
150 Innovation Drive
Winnipeg, MB R3T 2E1
CANADA
+1 204 989 9700

on the GTNETx2 card. Additional instances of GTNET-SKT would increase the data transmit/receive capabilities accordingly.

Q4: What is the number of external communication simulators that can be interfaced to the RTDS Simulator?

Theoretically there is no maximum. What needs to be considered is the capabilities of the RTDS Simulator's GTNETx2 card to send and receive data via TCP/UDP sockets. As per the previous question, each installation of the GTNET-SKT firmware is capable of sending up to 300 data points per packet, with each point defined over 4 bytes. The user can purchase additional GTNETx2 cards to scale the socket capabilities. In this sense, theoretically multiple external emulators could be interfaced.

Q5: Please discuss the system's behavior upon changing the microgrid feeder frequency from 60 to 49 Hz via DNP3 protocol.

If there are any frequency-critical loads, they will be tripped. In this case, loads 206 and 208 are frequency sensitive and were disconnected. The reactive loads will draw higher current.

Q6: Can you go over how to add delay on GOOSE packets?

For goose packets there are two options. One is connecting inline packet modifier in the publisher side and using the Linux Tc to delay them. The other is overriding the changed value using fake goose messages and after sometime stop sending these. However, the actual publisher would still be sending the previous StNum. Therefore, if the goose client blocks goose replays this will not work. In that case the inline packet modifier should be configured to send the actual set value with an updated StNum.

Q7: Is the packet modifier software – the GUI that you used to emulate the attacks – available?

The software is still in the development phase and not available for download yet. Watch the RTDS Newsletter (https://mailchi.mp/rtds/subscribe) and release notes of new RSCAD software versions for news of the release.

Q8: Are you also presenting a use case with NS-3?

RTDS Technologies Inc.
150 Innovation Drive
Winnipeg, MB R3T 2E1
CANADA
+1 204 989 9700

Today our demo is based on SNORT and not NS-3, but we have done in-house cases using NS-3, and we have an online respository with files available for you. You can access the repository at: https://github.com/chamara84/ns3_cybersec.git. A document explaining our work with emulating attacks via NS-3 is also available, and the .pdf is included for RTDS Simulator users in the post-webinar email.

Q9: I am wondering whether we can display the waveform of the measured data (e.g., frequency in the demo) in real-time ?e.g., dispaly it in a separate monitor?

The screen you were looking at is our RunTime interface which displays output data in real time. You can design this screen to look however you like. You can also save/export data for use in other programs.

Q10: What hardwares and softwares other than the RTDS Simulator is used in today's demo?

Today we made use of the RTDS Simulator's NovaCor hardware generation, with the GTNETx2 card and GTNET-SKT, GTNET-GSE, and GTNET-DNP protocols. Other than this, we used a Linux machine with 5 ethernet interfaces, the SNORT software, Wireshark software (optional), and a microgird controller with the necessary control code and vendor software. We also used the proprietary GUI for packet modification via SNORT, which is currently under development and will be available for the RTDS Simulator in the future.

Q11: What is the compatibility of GTNET and THE previous generation of the simulator and the ones use in the demo (GTNET2x and NovaCor)?

Both the GTNET (previous generation) and the current GTNETx2 are compatible with the NovaCor processing hardware. Both generation of GTNET(x2) cards can also be used with the previous generation of processing hardware (the PB5 card).

Q12: Does the packet modifier also fully block original values from microgrid controller?

For the TCP/UDP based protocols like DNP3, MODBUS etc. it will block the original packet. For the Multicast protocols like GOOSE and SV it will not block the original. It will send a fake message with updated StNum, SqNum and Time stamp for goose and updated smtCount and time stamp for SV.

RTDS Technologies Inc.
150 Innovation Drive
Winnipeg, MB R3T 2E1
CANADA
+1 204 989 9700

Q13: Is the SNORT information manual that Chamara mentioned available?

This document is under development and may be available to existing RTDS Simulator users upon request.

Q14: In real scenarios there are controls for avoiding GOOSE replay or Goose modification. Does your scenario have any such controls?

There is not goose replay protection in place. That is why the controller switched the BESS to V,f mode as soon as we stopped sending the fake goose messages. The legitimate message still has the previous StNum. We send the fake goose message as a new status with an incremented StNum and resetted SqNum and the current time stamp.

Q15: Do you also support the IEEE 2030.5 communication protocol, used for communication between DER devices and aggregators/utilities?

The RTDS Simulator does not currently offer direct support for IEEE 2030.5. If you are an existing customer requiring direct support for a project, please contact marketing@rtds.com and we can start a discussion.

Q16: For what all applications these Cyber Physical Simulations are Important? Is it only limited to Micro-Grid Simulations, IEC61850 GOOSE and Sampled Values (or) any protection related misoperations?

It is certainly not limited to just microgrids. We focused on microgrid communication protocols during this webinar due to high levels of interest in microgrids as an application and perceived issues with vulnerability in communication protocols. There are many aspects to power system cybersecurity, which could be at various levels of power system protection and control (in both the transmission and distribution space) – SCADA, wide-area, disgruntled employee action, GPS spoofing, etc.

Q17: Any timeframe on capability test and deal with encrypted data?

RTDS Technologies does not currently directly support encrypted communication protocol data. If you are an existing customer requiring direct support for a project, please contact marketing@rtds.com and we can start a discussion. Also, I believe SNORT is able to decrypt the packets if the private key is available.

RTDS Technologies Inc.
150 Innovation Drive
Winnipeg, MB R3T 2E1
CANADA
+1 204 989 9700

Q18: Does the tutorial explain the use of the GTNETx2 card to simulate HIL within the RTDS, without the microgrid controller?

There is a Sample case available in RSCAD which includes the Banshee microgrid case (substantially similar to what we used in our demo) but without any external controllers or GTNET cards. All of the protection and control functions in this case are provided by software components. This would not be termed HIL (hardware in the loop) simulation as no external hardware would be connected to the simulation.

Q19: Do we have to generate the code?

In the Snort based packet modifier you only need to enter the values for the data to be modified. So without doing a DoS attack or an MITM attack we are mimicking the net effect it has on the system in terms of data modification and introducing network impairments. For NS-3 we developed an application to carry out ARP spoofing attacks and modify SKT and DNP3 packets. There you need to write to code to setup the network and applications.

Q20: For both the attacks, it is assumed that the attacker has gained access to switch, correct?

Yes, we assume the network is already penetrated and the packets run through the devices controlled by attackers.

Q21: Can you mitigate against the man-in-middle attack using the GTNET?

At this point, the GTNETx2 card is not used for attack mitigation. The main purpose of using this card is for transmitting data between the simulator and external devices (whether that be a network emulator or an external protection/control device). This makes it essential for simulating a man-in-middle attack. For mitigation, you would need to test your mitigating strategy or device by integrating or connecting it to the RTDS Simulator.

RTDS Technologies Inc.
150 Innovation Drive
Winnipeg, MB R3T 2E1
CANADA
+1 204 989 9700