TR instruments, Ltd.

TEST & MEASURING INSTRUMENTS & SYSTEMS

CYBER SECURITY IN SMART GRIDS AND THREADS MITIGATION

Jiri Kalvoda
Managing director




COMPANY INTRODUCTION

- *Sales of T&M instruments*
- *Supplies of measuring systems & turnkey solutions*
- *Activities in CR, SR and Central Europe since 1991*
- *EN ISO 9001:2009*
- *Cooperation with 30+ manufacturers mostly on exclusive basis*
- *Wide market coverage, customers in Industry, telecommunications, education, research institutions*

TEST EQUIPMENT FOR TELECOMMUNICATION AND IT NETWORKS

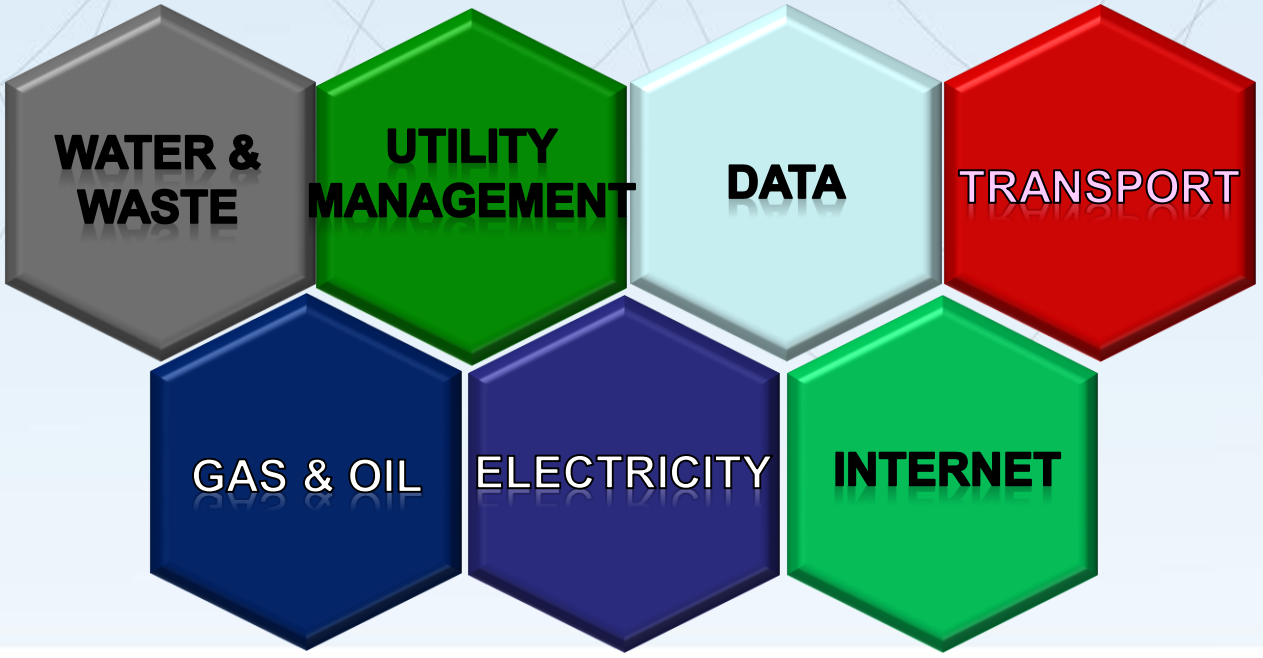
- *Handheld testers for copper, fiber and wireless networks*
- *IP traffic generators, virtual testers*
- *Simulators of DSL lines, IP networks, RF channels and GNSS signals*
- *Monitoring systems and traffic recorders, QoS, QoE test solutions*
- *Mobile Networks test solutions*
- *Synchronization systems NTP, PTP…*
- *Monitoring TAPs, aggregators, Packet brokers*
- *Testing automation*

TURNKEY SOLUTION

- *Environment parameters monitoring*
- *Wireless systems*
- *Multichannel measuring systems*
- *Synchronization systems*
- *Monitoring of telecommunication networks*
- *Performance testing of network technology*
- *Supplies of complete equipment for labs and testing facilities*

THE ULTIMATE SMART GRID

A Smart Grid is an grid that uses information and communications technology to gather and act on information in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity.
In the meantime Smart Grid technology is also used for a broader range of distributed facilities such as water and waste, gas and oil, traffic control etc.
Connecting these Smart Grids will conclude in the ultimate smart grid that offers maximum flexibility and value.



POTENTIAL THREATS

- Delay, block, or alteration of the generation process of an electric generation facility, resulting in the alteration of the amount of energy produced.
- Delay, block, or alter information related to a process, thereby preventing a bulk energy provider from obtaining production metrics that are used in energy trading or other business operations.
- Fraudulent information about demand or supply causing automatic measures taken which try to deal with non-existing power flows. Result may be a blackout and/or high financial losses.
- Deliberate energy market manipulation by changing smart grid information about the power demand or supply in a stressed market.
- A physical and/or cyber attack on a (small set of) single-point-of-failure smart grid component(s).
- Organised crime manipulating larger sets of consumer premises smart grid components or at the data concentrators, e.g. turning a large set of smart appliances off.
- The AMI being an entrance point to the smart grid network for hackers/criminals.

Operators Need to Strengthen Defenses to Ensure Network Security

- Perimeter defense systems against threats
  - Firewalls, UTM, IPS/IDS, Network security and Web/Email gateways
- Core infrastructure against unknown weaknesses
  - Critical Infra systems, Unified Communcation systems, Web servers

How to test the security of a network that is faced with…

- DDoS attacks
- Cyber-security attacks
- Known vulnerabilities
- Viruses, malware, SPAM, unwanted content
- Malformed traffic
- In the face of
  - Cloud enablement
  - Data center consolidation
- Without affecting your users and valid applications

WHAT YOU NEED TO TEST ?

Performance

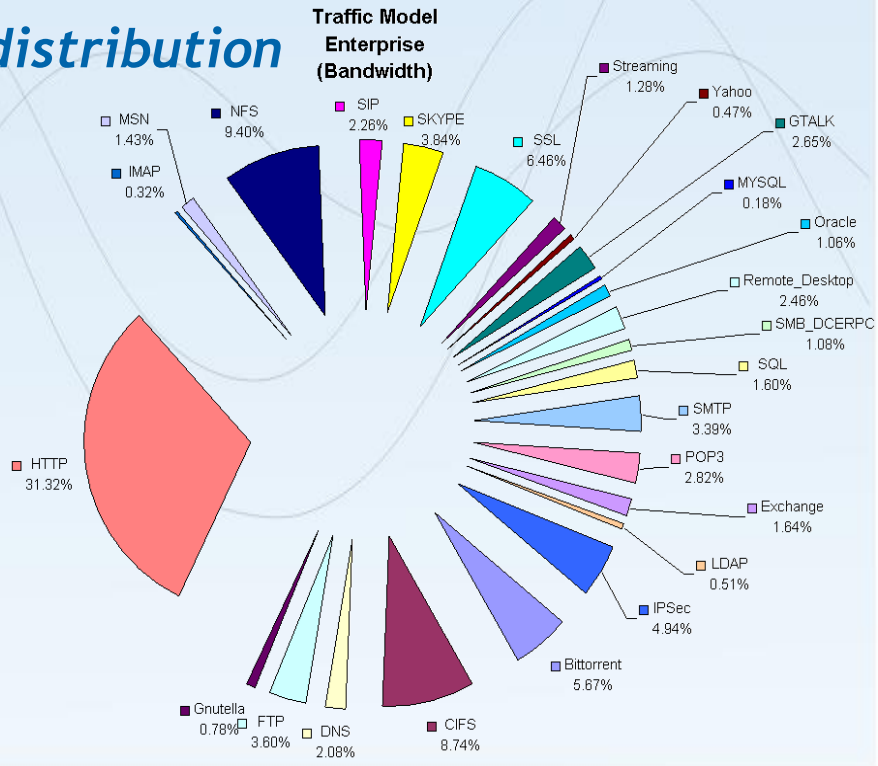
Availability

Scalability

Security

Performance Testing

- RFC 3511 Firewall Benchmarking
  - TCP connections per second
  - TCP open Connections
  - HTTP transactions per sec
- RFC 2544 Packet forwarding capacity
- Mix traffic bandwidth
  - Network modelled traffic distribution



Availability

- *Fail over/traffic recovery*
- *Bandwith with DDoS attack*
- *Access Control*

Scalability

- *Open concurrent connections*
- *Simultaneous users*
- *Bandwith*

Security

- *Published Vulnerability Assessment*
- *DDoS*
- *Fuzzing*
- *Malware*
- *Identity control*

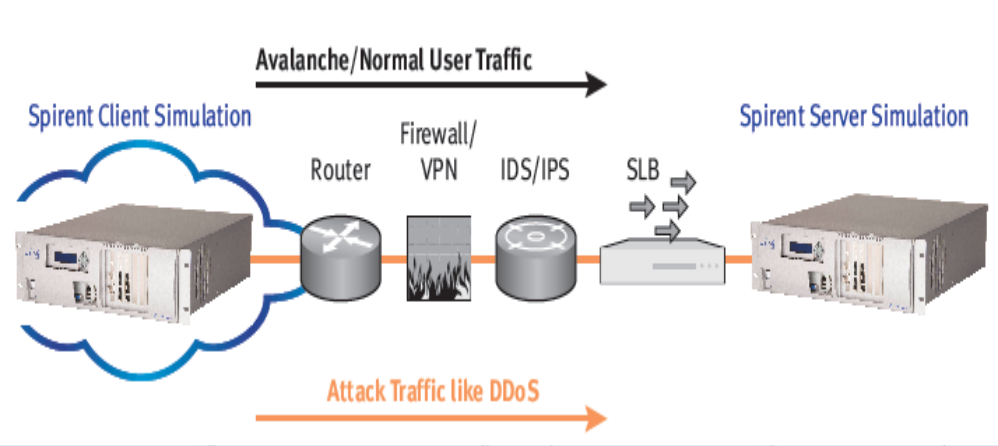
SPIRENT AVALANCHE – C100 PLATFORM

Converged platform for:

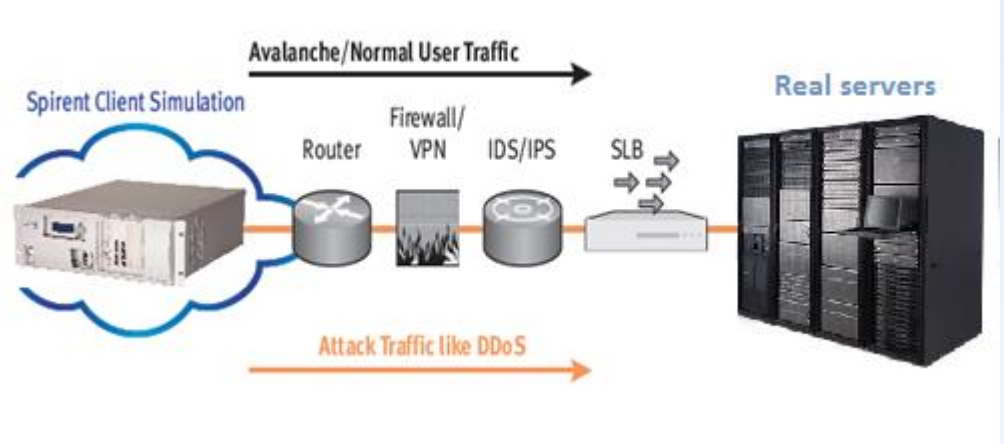
- *testing on L4-L7 layers*
- *testing at speeds from 10Mbps to 10Gbps*
- *testing of application servers, FW, network infrastructure…*
- *emulation of user groups of different services and application servers (HTTP/HTTPS, FTP, Telnet, SIP, Video…)*
- *emulation of large type of applications – Skype, Facebook, WhatsApp, Games (Angry Birds, Mafia Wars, FarmVille)…*
- *emulation of attacks and security threats including access to an extensive database of attacks with the ability to create own customized attacks*
- *ability to emulate the „useful" and malicious traffic from the same user*
- *Avalanche Virtual for SDN and NFV testing*

EXAMPLES OF POSSIBLE TEST SETUP

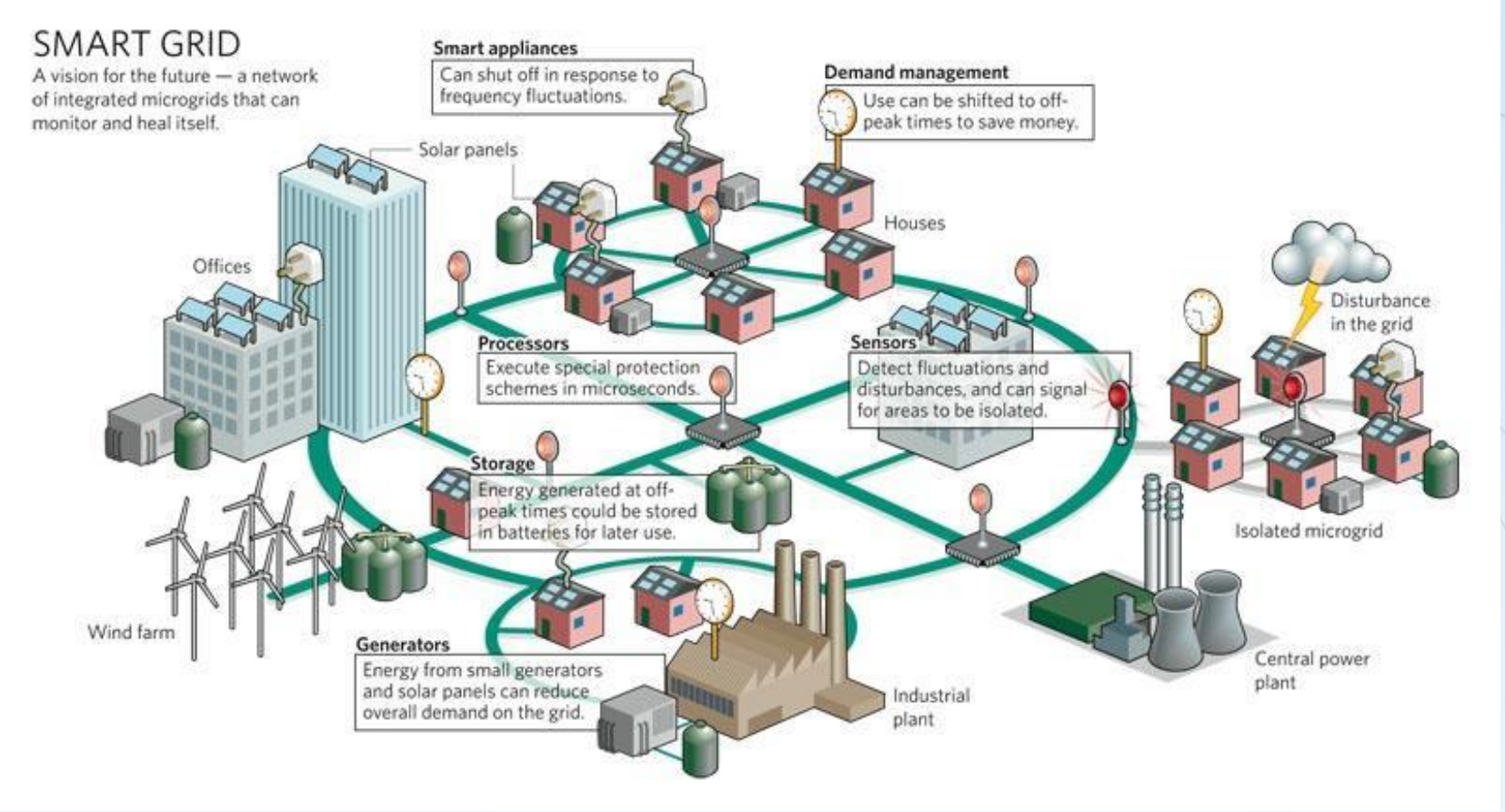
- *Testing of infrastructure between the simulated client side and servers – „pass through“*



- *Testing of infrastructure and real servers – „one arm“*



Time sync is critical for smart grid



GNSS based systems vulnerability

- GPS, GLONASS, Galileo, BeiDou
- GNSS provides
  - position – navigation
    - guidance
    - tolling
  - time – financial
    - communications networks
    - power networks
    - authentication
  - velocity – guidance
    - navigation

Main problem – weak signals subject to interference

Interference - non intentional

- intentional → jamming

→ spoofing

Defence applications - special robust codes

Civilian applications – very limited receivers immunity, must use different protection techniques.

GNSS receivers need to be tested !!!

SPIRENT GSS8000 SIMULATOR

Main features:

- support of GPS, GLONASS, Galileo, BeiDou-2 and SBAS systems
- up to 3 carriers in a single chassis
- up to 48 channels in a chassis plus up to 192 additional programmable multipath channels (total 240 channels per chassis)
- one or two RF outputs per chassis

Additional features:

- trajectory simulation for automotive,
- military, aerospace, navy applications
- Ionosphere and Troposphere modeling
- antenna gain and phase pattern
- DGPS corrections
- simulation of terrain obscuration
- extension for interference and spoofing (SimSafe) testing, sensor simulation (SimSensor - accelerometers, gyroscopes…), LAAS testing…

Thank you for your attention