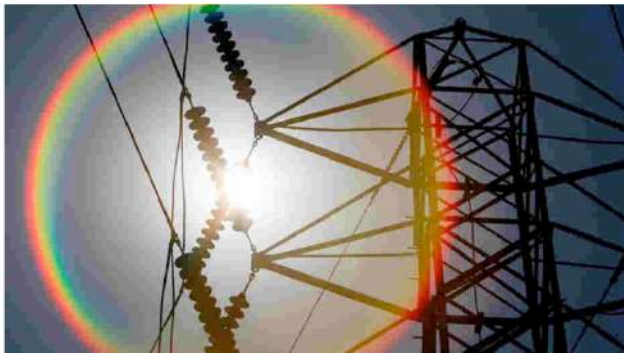
Exceptional service in the national interest

Sandia National Laboratories

energy.sandia.gov





An Overview of Threats to the Power Grid

Juan Torres

Deputy Program Area Director

Renewable Systems and Energy Infrastructure

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

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 Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000

Acknowledgements

This presentation was developed with input from the DOE Grid Modernization Laboratory Consortium (GMLC) Security and Resilience Team

- Arjun Shankar, ORNL
- Chris Strasburg, Ames Lab
- Craig Rieger, INL
- Jamie van Randwyk, LLNL
- Jim Cale, NREL
- Jim Kavicky, ANL
- Joe Cordaro, SRNL
- Pat Looney/Stephanie Hamilton, BNL
- Paul Skare, PNNL
- Sean Peisert, LBL
- Tim McPherson, LANL

Outline

Sandia National Laboratories

- Malicious Threat Matrix
- Physical Threat
- Cyber Threat
- Accidental Failures
- EMP and GMD

Outline

Sandia National Laboratories

- Malicious Threat Matrix
- Physical Threat
- Cyber Threat
- Accidental Failures
- EMP and GMD

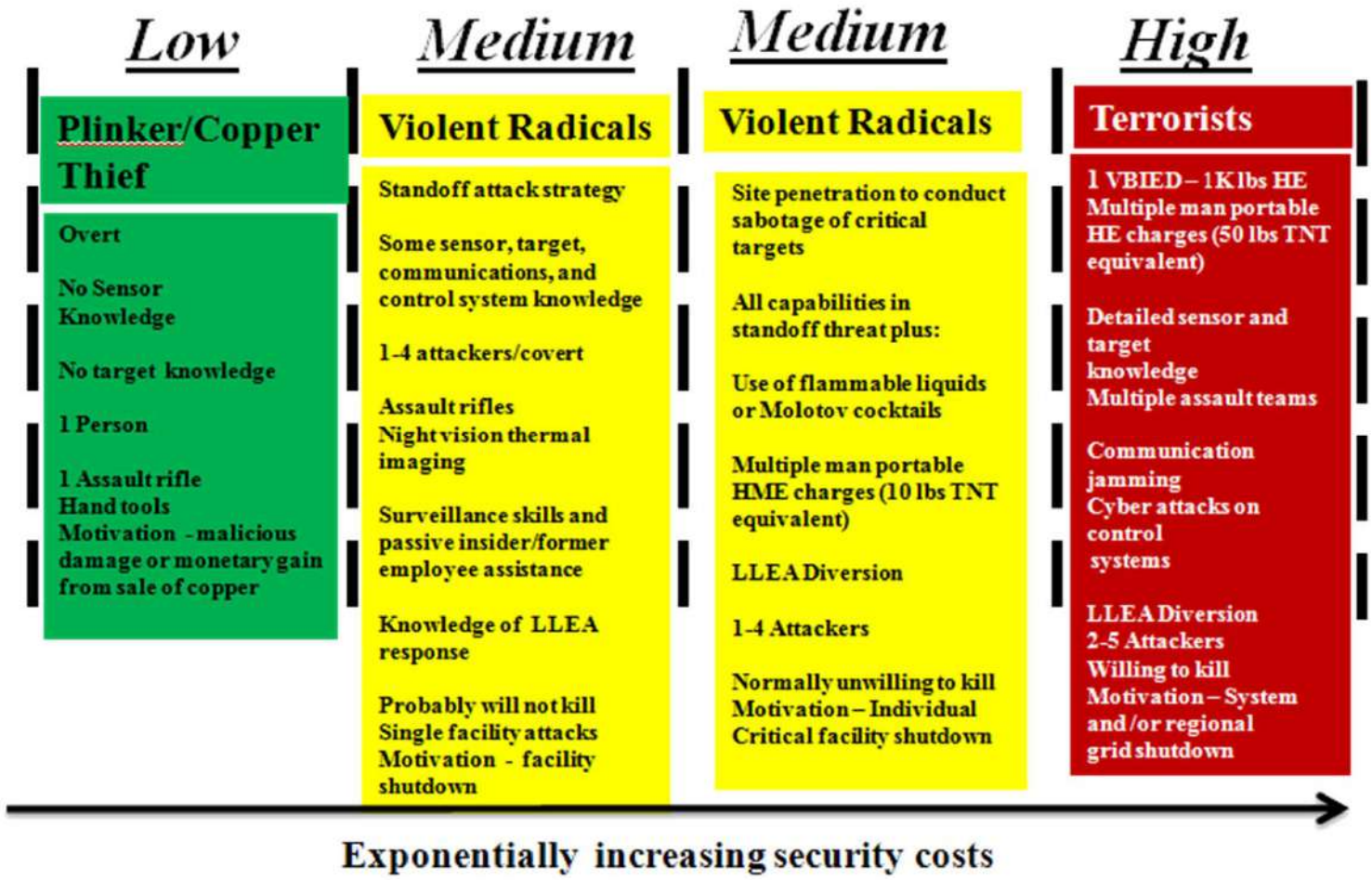
Example: Malicious Threat Capability Matrix

Sandia National Laboratories

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	KNOWLEDGE		ACCESS
					CYBER	KINETIC	
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

Example: Generic Design Basis Threat

Sandia National Laboratories



Outline

Sandia National Laboratories

- Malicious Threat Matrix
- Physical Threat
- Cyber Threat
- Accidental Failures
- EMP and GMD

Physical Security/Resilience Threats to the Grid are Real

- People have attacked the grid in notable ways in recent years (Metcalf and Arkansas)

- Significant monetary loss thus far but no long-term local or regional outages

HV Transformers at Risk

Sandia National Laboratories

"The main risk from a physical attack against the electric power grid—primarily towers and transformers—is a widespread power outage lasting for days or longer…Experts have long asserted that a coordinated and simultaneous attack on multiple HV transformers could have severe implications for reliable electric service over a large geographic area, crippling its electricity network and causing widespread, extended blackouts. Such an event would have serious economic and social consequences."

Physical Security of the U.S. Power Grid:
High-Voltage Transformer Substations
Paul W. Parfomak
June 17, 2014

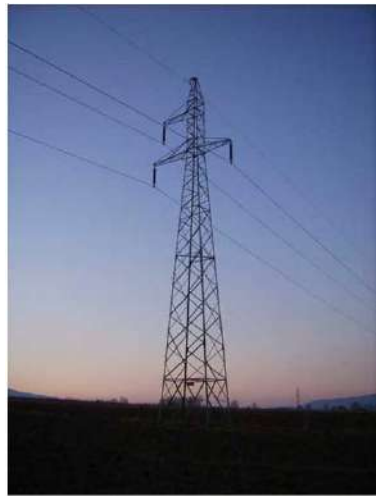
Source: http://fas.org/sgp/crs/homesec/R43604.pdf

Arkansas Transmission Line Attack

Sandia National Laboratories

"According to the FBI:

- In the early morning hours of September 29, 2013, officials with Entergy Arkansas reported a fire at its Keo substation located on Arkansas Highway 165 between Scott and England in Lonoke County. Fortunately, there were no injuries and no reported power outages. Investigation has determined that the fire, which consumed the control house at the substation, was intentionally set. The person or persons responsible for this incident inscribed a message on a metal control panel outside the substation which reads, 'YOU SHOULD HAVE EXPECTED U.S.'"



http://www.forbes.com/sites/williampentland/2013/10/07/weekend-attacks-on-arkansas-electric-grid-leave-10000-without-power-you-should-have-expected-u-s/

Physical-Cyber Security Nexus

Sandia National Laboratories

- Physical and cyber protections are often organized as two completely separate areas. In reality, the two must work in concert.
- Defense against cyber attack is achievable only if networks are 1) physically secured and 2) managed securely through physical and operational controls.
- Comprehensive security requires continual assessment of all potential adversarial pathways — physical and electronic.

Outline

Sandia National Laboratories

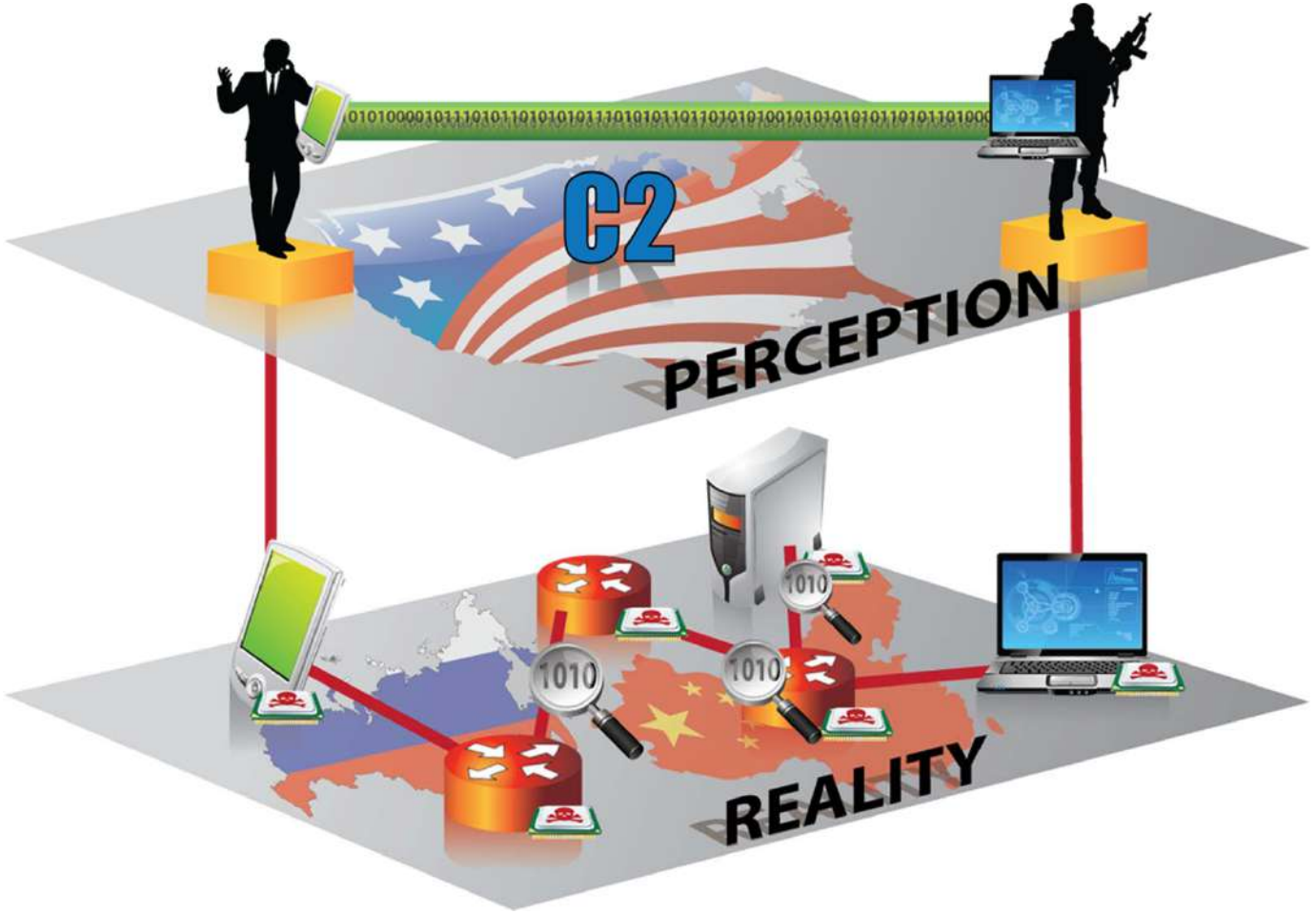
- Malicious Threat Matrix
- Physical Threat
- Cyber Threat
- Accidental Failures
- EMP and GMD

Supply Chain in a Globalized Economy

Sandia National Laboratories

Potential Impact of Supply Chain on National Security

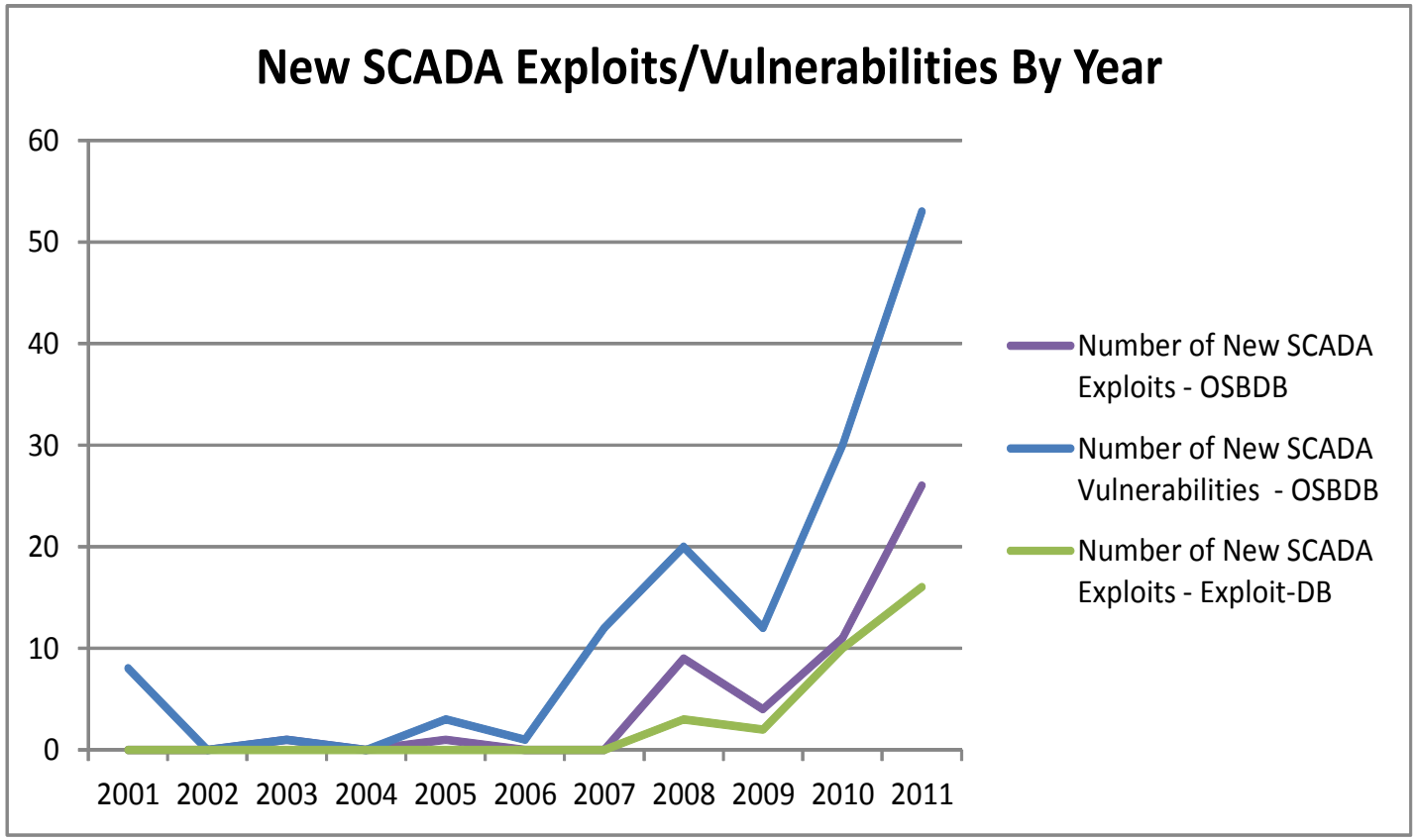
Sandia National Laboratories



Indications of SCADA Vulnerability

Sandia National Laboratories

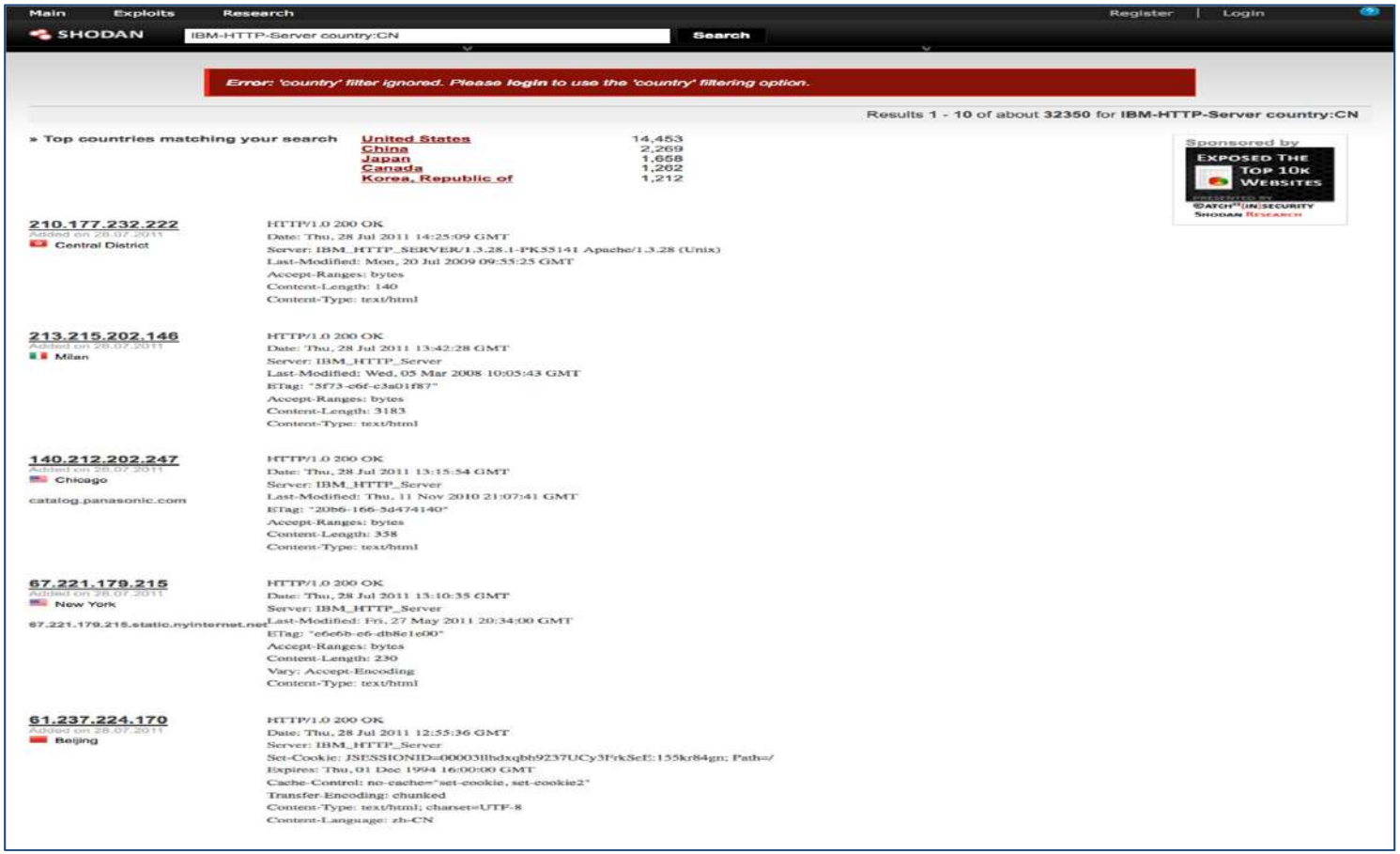
The Open Source Vulnerability Database (OSVDB) is an independent and open source database created by and for the security community.



Indications of Vulnerability (example)

Sandia National Laboratories

SHODAN Database makes it possible to find systems of a given type in a given country that are vulnerable to a given exploit, which makes it easy to locate vulnerable Internet-facing SCADA systems.



Cyber Tool Development
(Product Example)

Sandia National Laboratories

Cyber Tool Development
(Product example)

Sandia National Laboratories

SCADA+ Pack

This is an attempt to collect ALL publicly available SCADA vulnerabilities in one exploit Pack.
SCADA and related vulnerabilities are very special due to its sensitive nature and possible huge impact involved to successfull exploitation.
SCADA Systems are also "hard to patch", so even old vulnerabilities are actual.

The SCADA+ Pack features:

- Growing value
  Due to low real systems patch rank
- 100% public SCADA vulns coverage
  Including old and newly discovered bugs
- 0 Days for SCADA
  We conduct our own in depth research
- Focused on Industrial software & hardware environment
  Not only SCADA, but also Industrial PCs, smart chips and industrial protocols are reviewed.
- Weak points analyses
  Many industrial things suffer from weaknesses like hardcoded password and etc.

Licensing:

- Standard - restrictive (no derivative works or any disclosures allowed) 1 seat license
- Step Ahead - unrestrictive license, with powerfull features more

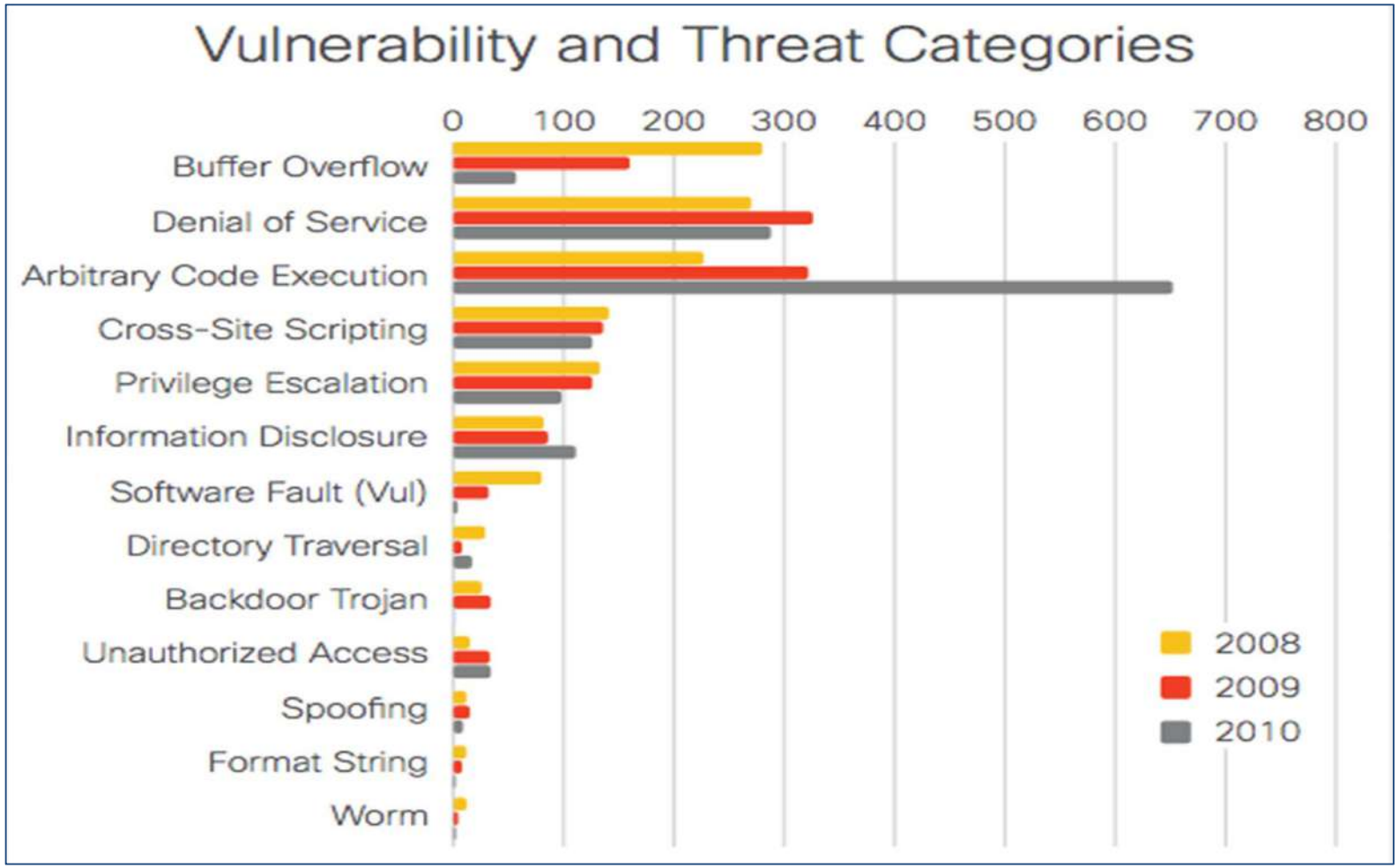
Some SCADA+ demos could be found here on our pentesting.ru site:
List of featured modules available instantly via Step Ahead :

For how to buy information - refer here

Cyber Tool Development

Adversaries are becoming more capable

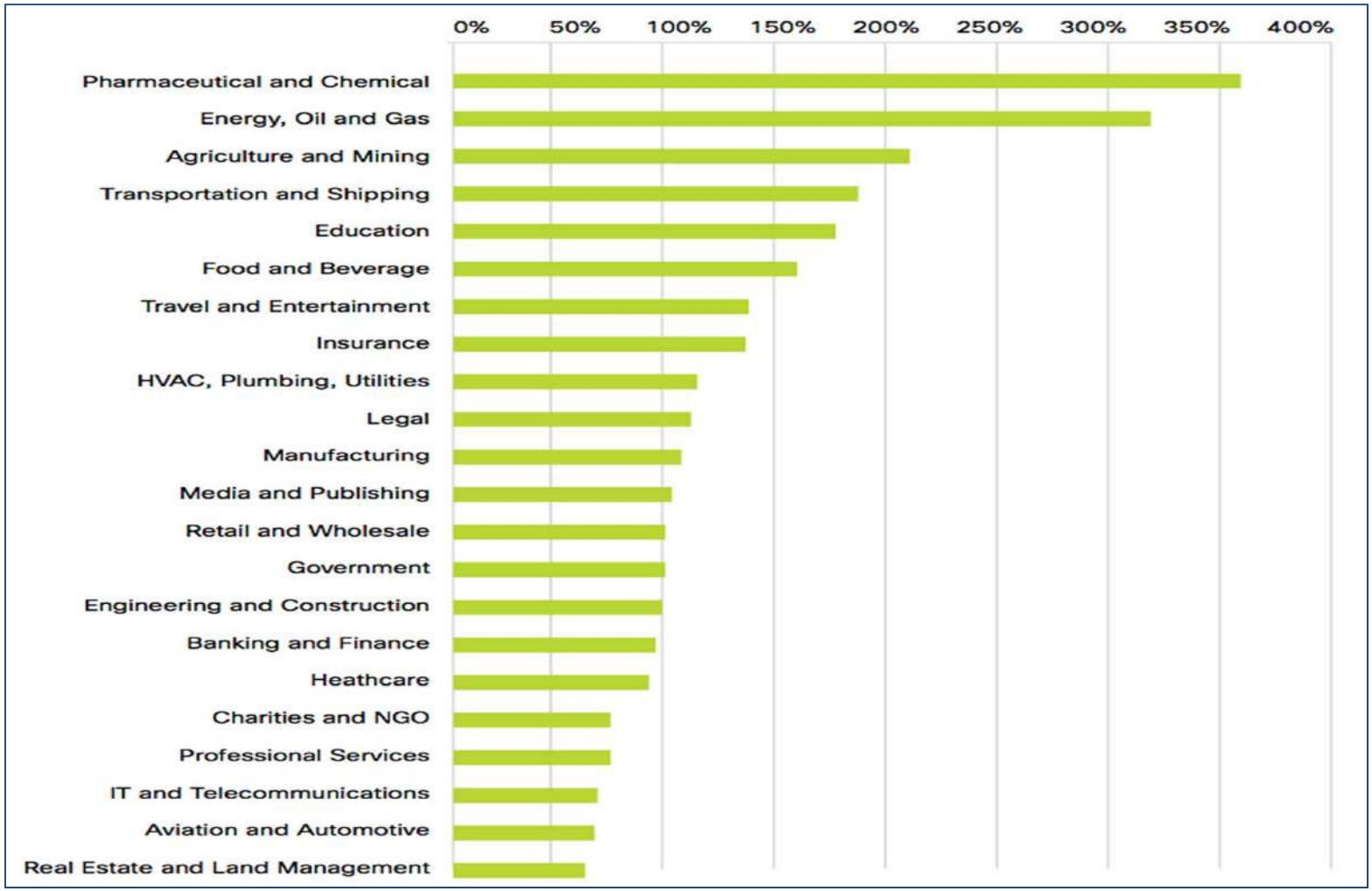
Sandia National Laboratories



R. Festag, SCADA Attack System, final report, George Washington U., April 2011

Indications of Adversary Interest

Sandia National Laboratories



ScanSafe, Annual global Threat Report 2010

Outline

Sandia National Laboratories

- Malicious Threat Matrix
- Physical Threat
- Cyber Threat
- Accidental Failures
- EMP and GMD

Accidents and Inadvertent Errors

Sandia National Laboratories

- Accidental cyber errors also can be destructive:
  - Misconfiguration of marginal turbine for AGC load tracking at Sayano-Shushenskaya hydro plant (Russia, 2009) contributed to failure of multiple turbines.
    - Two 711 MVA generators exploded; other extensive damage to turbines
      - 75 deaths
      - 40 tons of transformer oil released
      - Repair of hydro station est. at 5+ years and $1.2B.
- *Lessons:* "insider" mistakes are hard to distinguish from attacks. Either can be as destructive as external attacks.

Accidents and Inadvertent Errors

Sandia National Laboratories

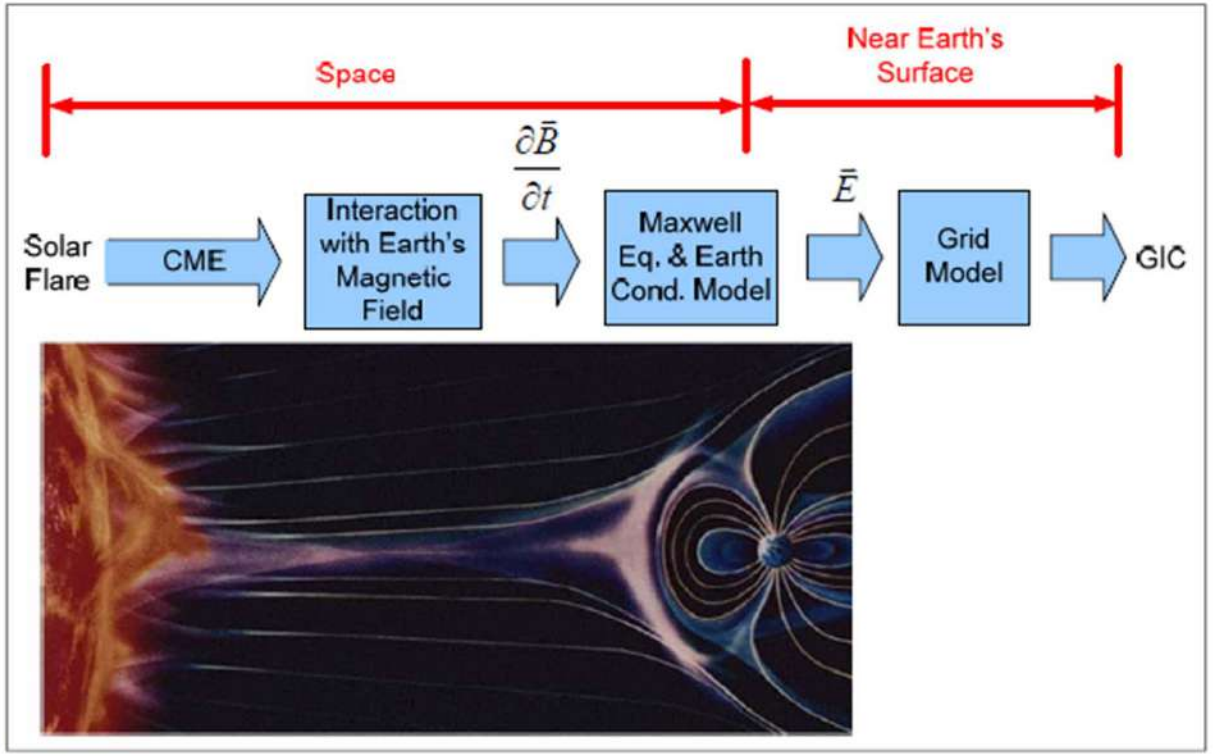
Outline

Sandia National Laboratories

- Malicious Threat Matrix
- Physical Threat
- Cyber Threat
- Accidental Failures
- EMP and GMD

Risks to the Grid from Geomagnetic Disturbance

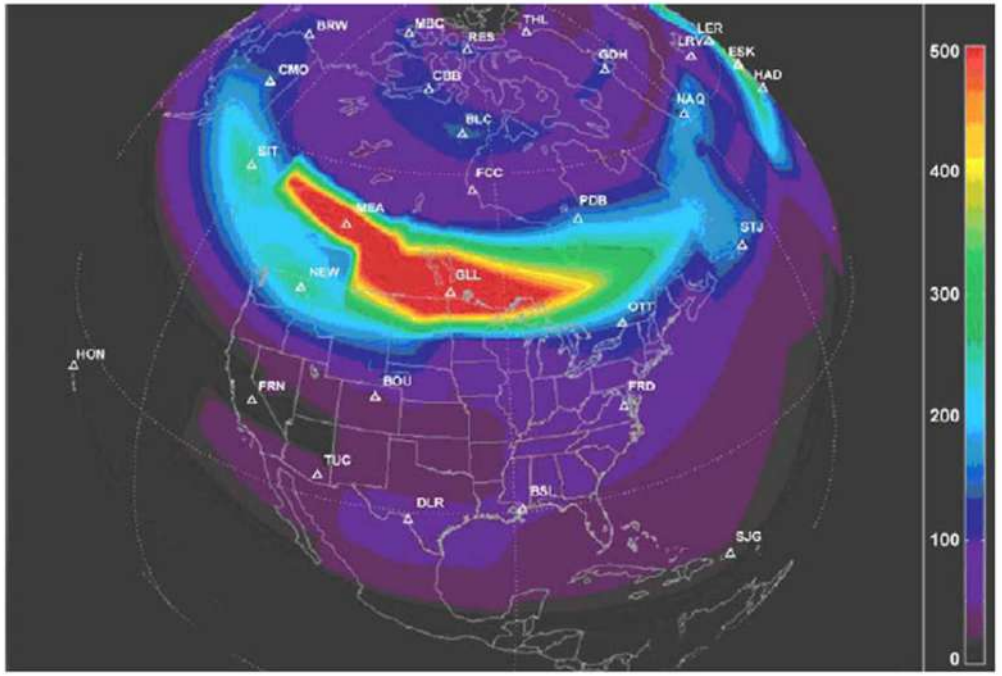
- Damage to bulk power system assets, typically associated with transformers
- Loss of reactive power support, which could lead to voltage instability and power system collapse.



Source: NERC 2012 Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System

Solar Storm Example

- 1989 Hydro-Quebec outage due to solar storm
- 6M people affected
- 9 hour outage



Geomagnetic intensity–March 1989 storm

Source:
NERC 2012 Special Reliability Assessment Interim Report:
Effects of Geomagnetic Disturbances on the Bulk Power System

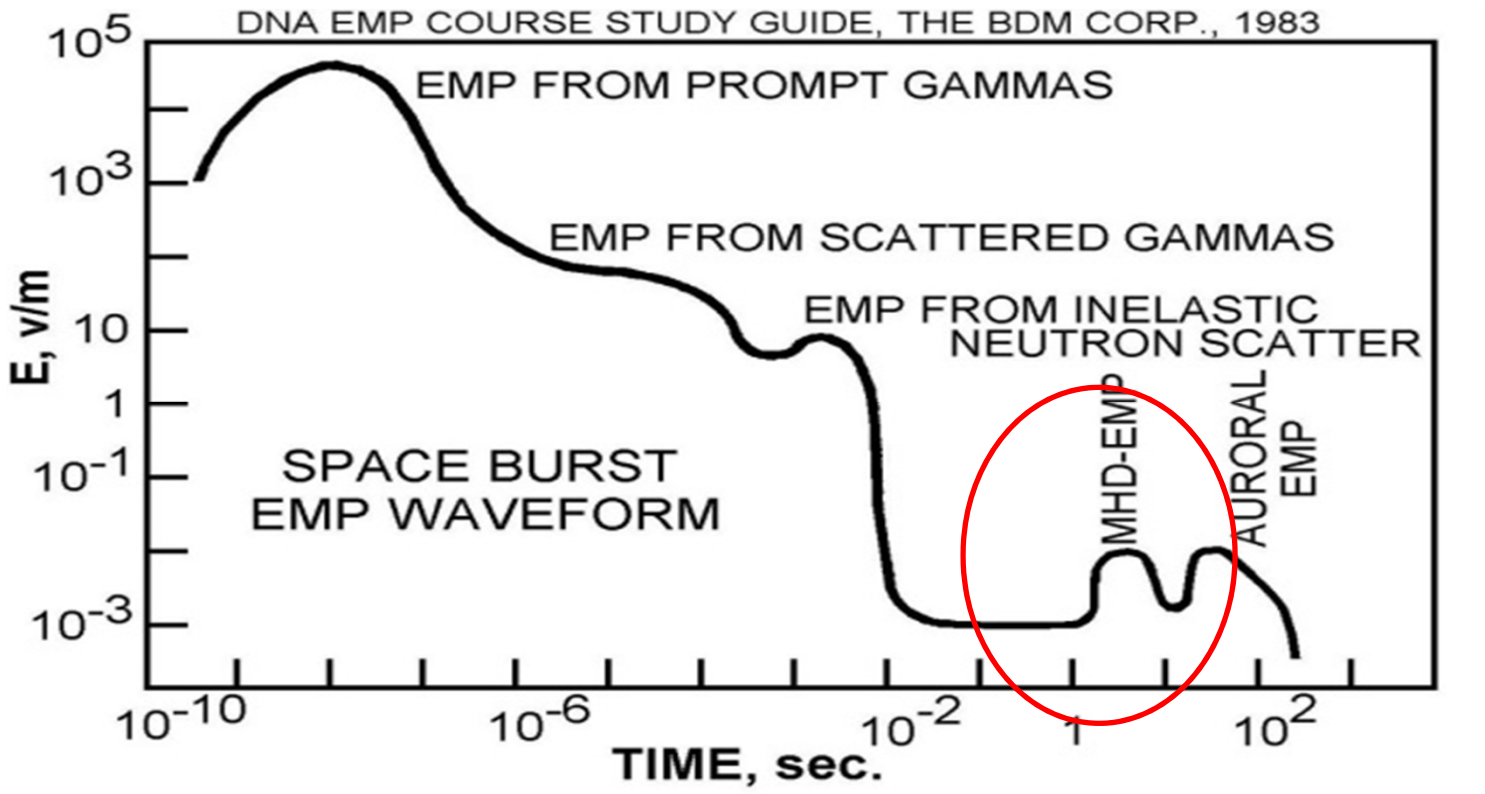
Electromagnetic Pulse (EMP)

Sandia National Laboratories

- The term electromagnetic pulse is a burst of electromagnetic radiation that results from an explosion (especially a nuclear explosion). The resulting electric and magnetic fields may couple with electrical/electronic systems to produce damaging current and voltage surges.

- The effects of EMP on the electrical power system are fundamentally partitioned into its early, middle and late time effects
  - E1, (early) very fast component of nuclear EMP
  - E2, (middle) similar to electromagnetic pulses produced by lightning
  - **E3, (late time)** or Magnetohydrodynamic (MHD) very slow pulse lasting tens to hundreds of seconds (the E3 pulse is similar to the effects of a geomagnetic storm (Although, the MHD-E3 has similar frequency content to a geomagnetic storm, its intensity can be considerably higher.)

EMP Waveform as a Function of Time



Review of Power Grid Vulnerability to Extreme GIC Events from E3 Threats or Severe Geomagnetic Storms

Sandia National Laboratories

- U.S. power grid design trends have greatly increased the vulnerability and potential impact of E3 threats and geomagnetic storms (long east-west transmission lines)
- Ultra High Voltage such as 500kV & 765kV transmission lines are more prone to damage by EMP-H3
- The EMP commission study states that geomagnetically induced current (GIC) risks are potential national security and energy security threats
- Global reach of extreme geomagnetic disturbances raises concerns about the potential for large scale blackouts, permanent damage to transformer assets and extended restoration times

Conclusion

Sandia National Laboratories

- Malicious threats are increasing
- Adversaries are becoming more informed and more capable
- Emerging threats are challenging
  - Physical/cyber
  - System complexity
  - Lifecycle