

Exceptional service in the national interest



energy.sandia.gov



An Overview of Threats to the Power Grid

Juan Torres

Deputy Program Area Director

Renewable Systems and Energy Infrastructure



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

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

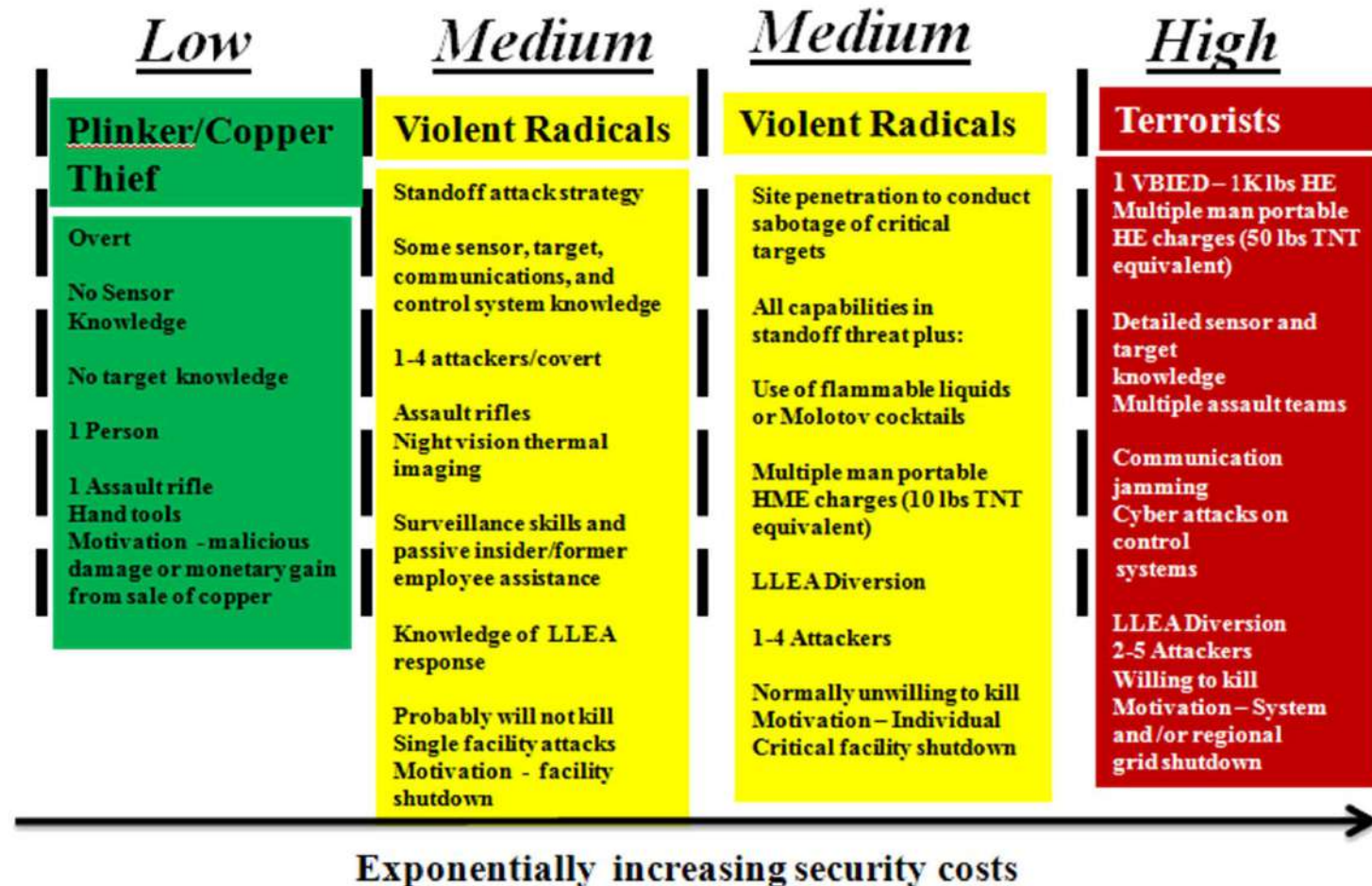
Outline

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

Example: Malicious Threat Capability Matrix

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	KNOWLEDGE		ACCESS
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



Outline

- 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

“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

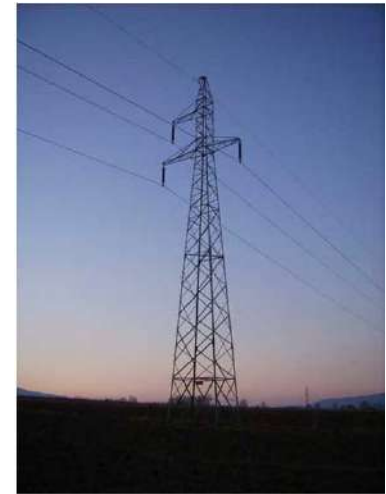
June 17, 2014

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

Arkansas Transmission Line Attack

“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

- 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.



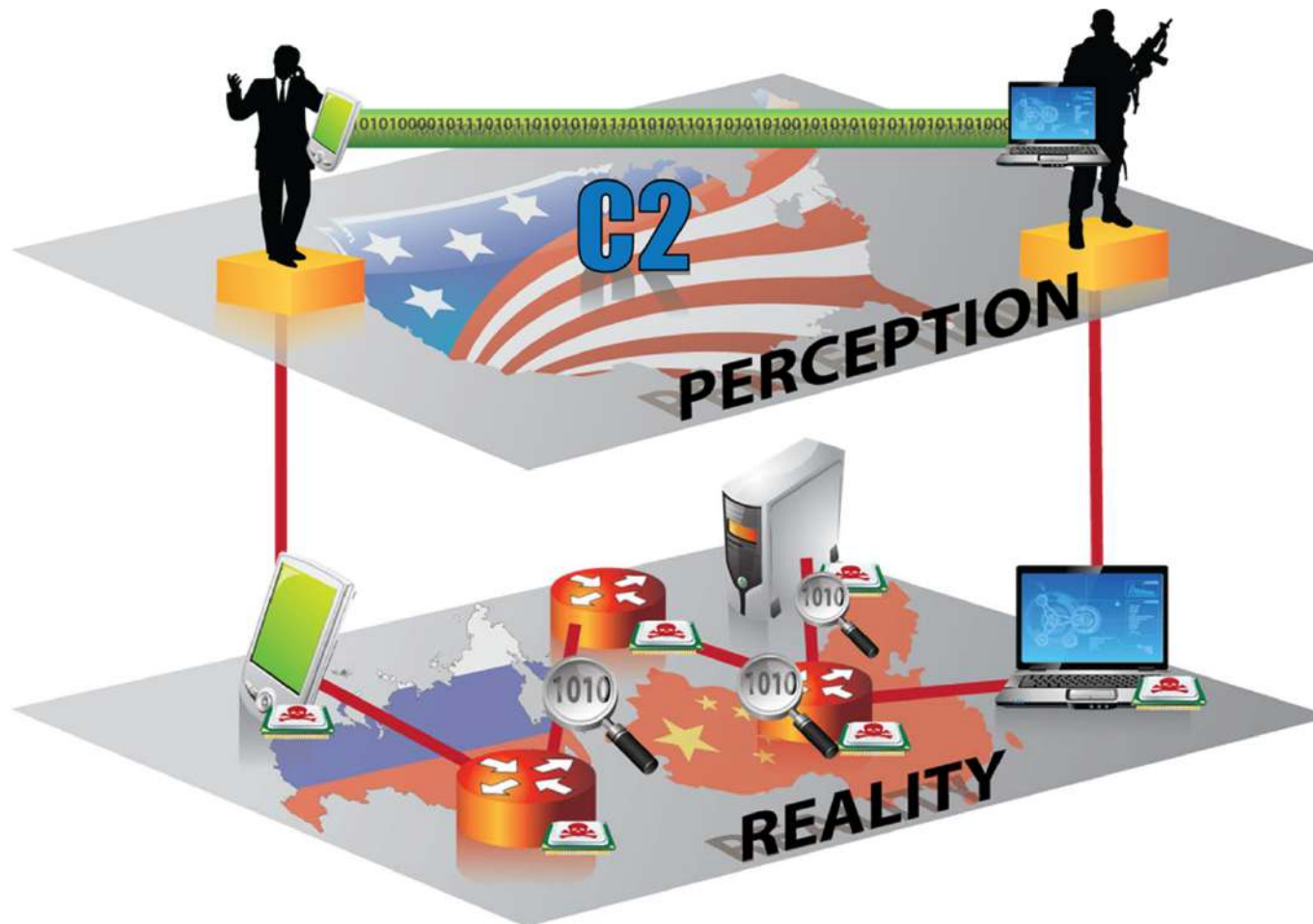
Outline

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

Supply Chain in a Globalized Economy

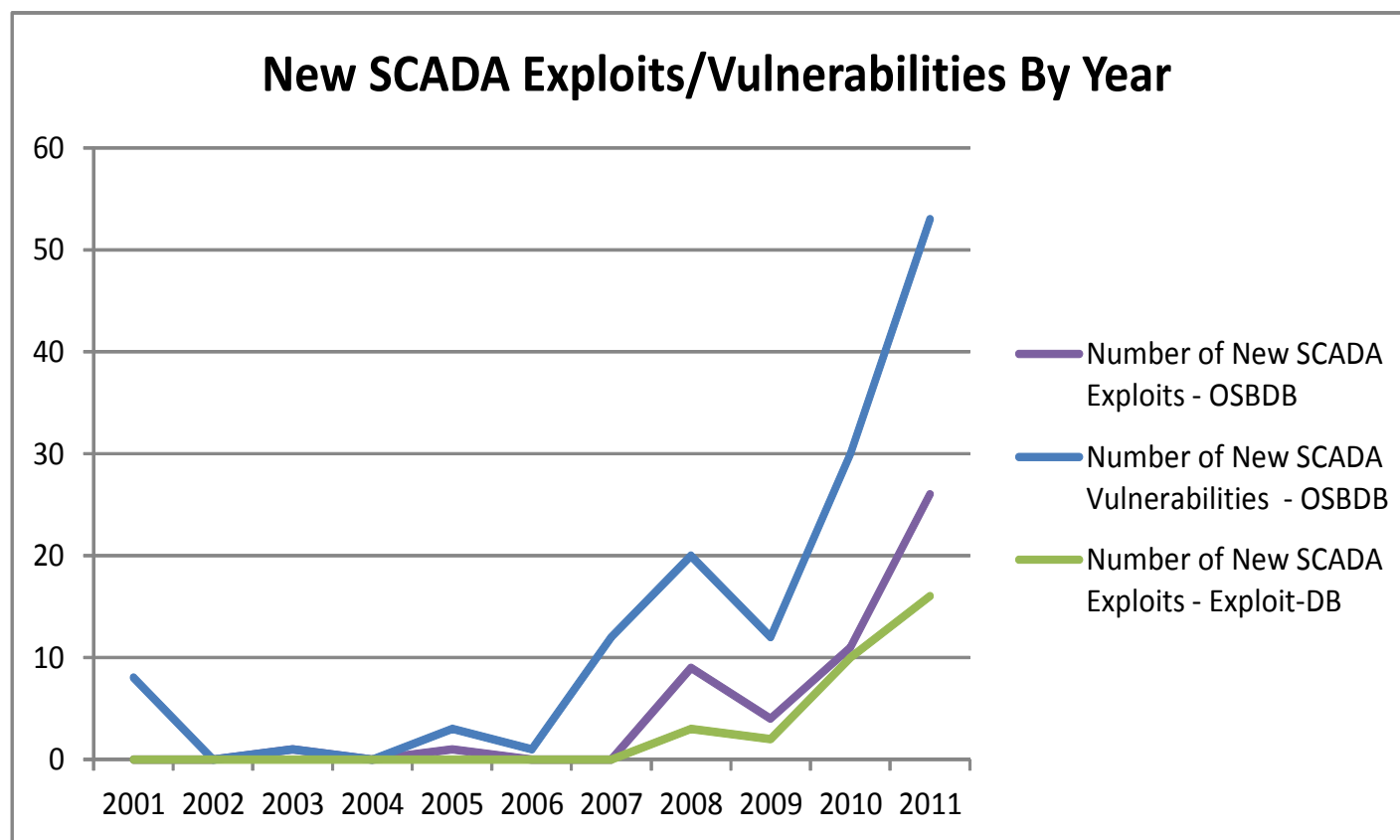


© 2014 Pearson Education, Inc. or its affiliate(s). All rights reserved.



Indications of SCADA Vulnerability

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



Indications of Vulnerability (example)



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.

SHODAN

IBM-HTTP-Server country:CN

Search

Register | Login

Error: 'country' filter ignored. Please login to use the 'country' filtering option.

Results 1 - 10 of about 32350 for IBM-HTTP-Server country:CN

IP Address	Country	Count
210.177.232.222	United States	14,453
213.215.202.146	China	2,269
140.212.202.247	Japan	1,658
67.221.179.215	Canada	1,202
61.237.224.170	Korea, Republic of	1,212

» Top countries matching your search

210.177.232.222
Added on 28.07.2011
Central District
HTTP/1.0 200 OK
Date: Thu, 28 Jul 2011 14:25:09 GMT
Server: IBM_HTTP_SERVER/1.3.28.1-PK55141 Apache/1.3.28 (Unix)
Last-Modified: Mon, 20 Jul 2009 09:55:25 GMT
Accept-Ranges: bytes
Content-Length: 140
Content-Type: text/html

213.215.202.146
Added on 28.07.2011
Milan
HTTP/1.0 200 OK
Date: Thu, 28 Jul 2011 13:42:28 GMT
Server: IBM_HTTP_Server
Last-Modified: Wed, 03 Mar 2008 10:03:43 GMT
ETag: "5f73-e6f-e3a01f87"
Accept-Ranges: bytes
Content-Length: 3183
Content-Type: text/html

140.212.202.247
Added on 28.07.2011
Chicago
catalog.panasonic.com
HTTP/1.0 200 OK
Date: Thu, 28 Jul 2011 13:15:54 GMT
Server: IBM_HTTP_Server
Last-Modified: Thu, 11 Nov 2010 21:07:41 GMT
ETag: "20b6-166-5d474140"
Accept-Ranges: bytes
Content-Length: 338
Content-Type: text/html

67.221.179.215
Added on 28.07.2011
New York
67.221.179.215.static.nyinternet.net
HTTP/1.0 200 OK
Date: Thu, 28 Jul 2011 13:10:35 GMT
Server: IBM_HTTP_Server
Last-Modified: Fri, 27 May 2011 20:34:00 GMT
ETag: "c6eb8-e6-d81e1e00"
Accept-Ranges: bytes
Content-Length: 230
Vary: Accept-Encoding
Content-Type: text/html

61.237.224.170
Added on 28.07.2011
Beijing
HTTP/1.0 200 OK
Date: Thu, 28 Jul 2011 12:55:36 GMT
Server: IBM_HTTP_Server
Set-Cookie: JSESSIONID=000031bdxqbt9237UCy3PrkSeE:155kr84gn; Path=/
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Cache-Control: no-cache="set-cookie, set-cookie2"
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Content-Language: zh-CN

Sponsored by
EXPOSED THE TOP 10K WEBSITES
POWERED BY
SHODAN (IN)SECURITY
SHODAN RESEARCH

Cyber Tool Development (Product Example)



The screenshot shows the GLEG website interface. At the top left is the GLEG logo, which consists of a stylized orange and black bug-like icon next to the text 'GLEG'. To the right of the logo are links for 'contact us' and 'support', followed by a search bar with a 'search' button. Below the logo is a navigation menu with links for 'Home', 'Products', 'Services', 'Partners', and 'About'. The main banner features the text 'When security is not an option' and 'The eldest among Canvas addon pack developers', with a 'READ MORE' button. To the right of the banner is an image of a software box and a CD-ROM, both labeled 'GLEG' and 'agora'. Below the banner are two columns of product information. The left column is titled 'NEW: SCADA+ Pack' and lists features: 'An effort towards 100% public SCADA vulns coverage', '0 Days for SCADA!', 'Focused on Industrial software & hardware environment', and 'Weak points analyses', with a 'READ MORE' button. The right column is titled 'Agora Pack' and lists features: 'Fresh & unpatched stuff each month', 'Mainstream WEB related software covered', 'Modules to defeat the defense, hack the database', and 'New attack techniques', with a 'READ MORE' button. At the bottom of the page is a footer with the copyright notice '© 2004-2011 GLEG Ltd All rights reserved' and a 'sitemap' link.

GLEG

contact us | support

Home Products Services Partners About

When security is not an option
The eldest among Canvas addon pack developers

READ MORE

NEW: SCADA+ Pack

- > An effort towards 100% public SCADA vulns coverage
- > **0 Days for SCADA!**
- > Focused on Industrial software & hardware environment
- > Weak points analyses

READ MORE

Agora Pack

- > Fresh & unpatched stuff each month
- > Mainstream WEB related software covered
- > Modules to defeat the defense, hack the database
- > New attack techniques

READ MORE

© 2004-2011 GLEG Ltd All rights reserved

→ [sitemap](#)

Cyber Tool Development

(Product example)



— 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 successful 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 powerful features [more](#)

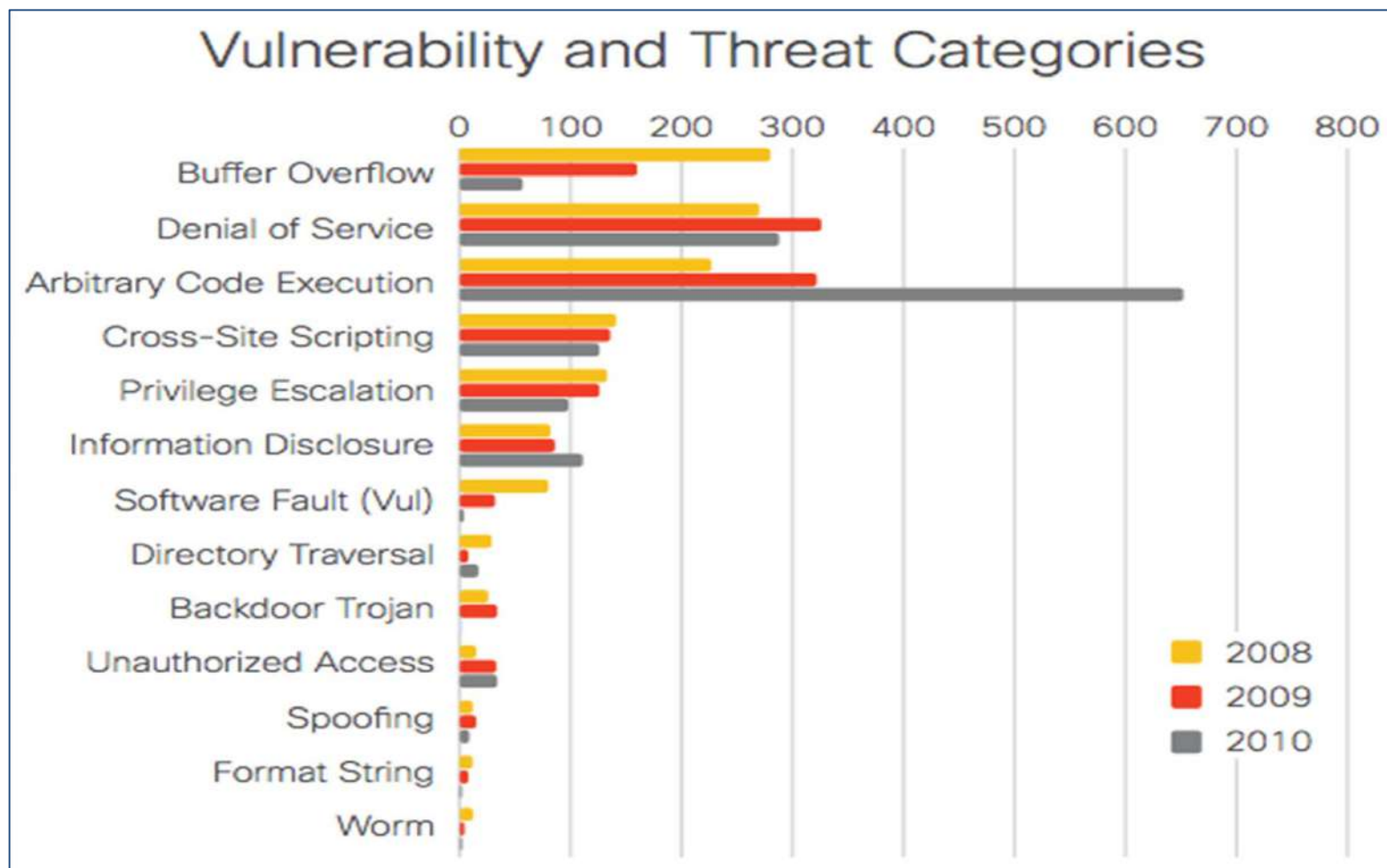
Some SCADA+ demos could be found [here on our pentesting.ru site](#):

List of featured modules available instantly via [Step Ahead](#) :

For how to buy information - [refer here](#)

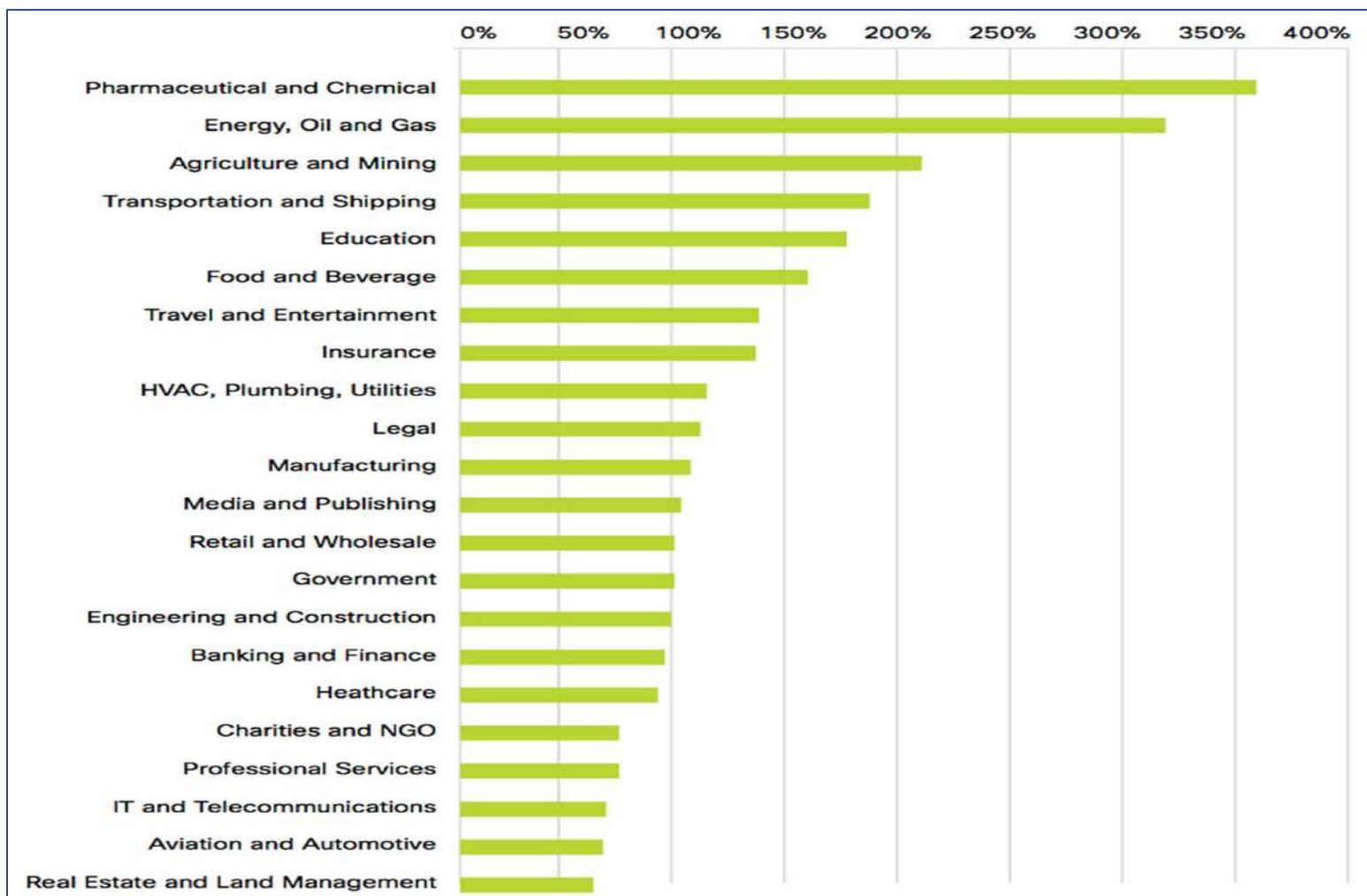
Cyber Tool Development

Adversaries are becoming more capable



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

Indications of Adversary Interest



ScanSafe, Annual global Threat Report 2010

Outline

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

Accidents and Inadvertent Errors



- ▶ 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

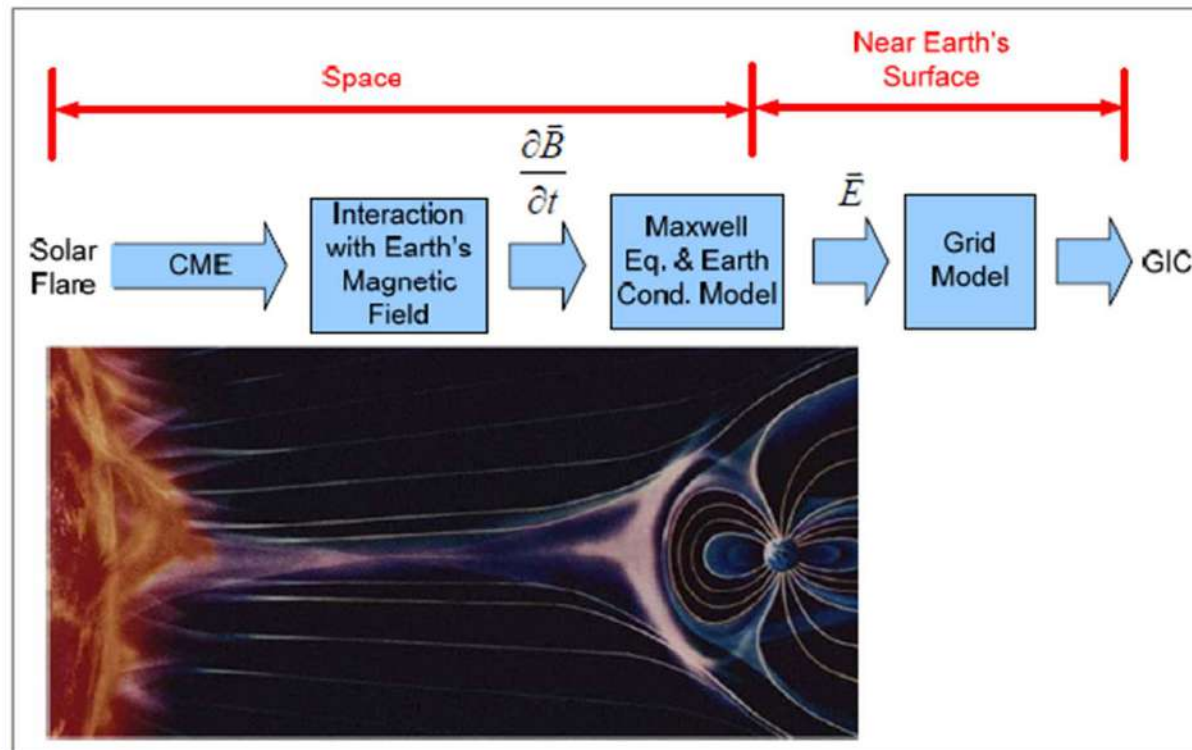


Outline

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

Risks to the Grid from Geomagnetic Disturbance

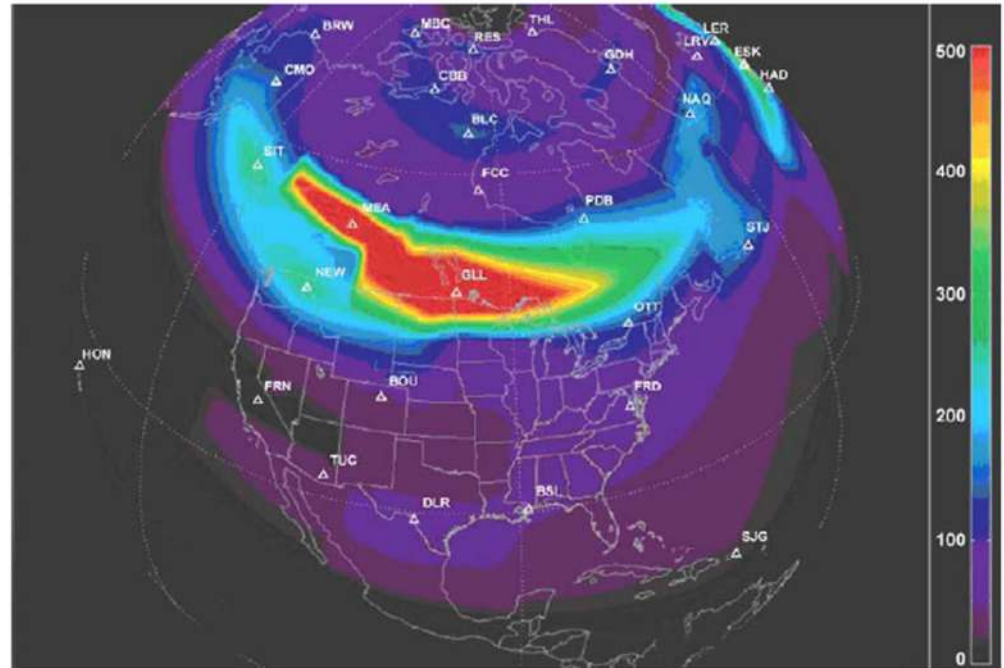
- Damage to bulk power system assets, typically associated with transformers
- Loss of reactive power support, which could lead to voltage instability and power system collapse.



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



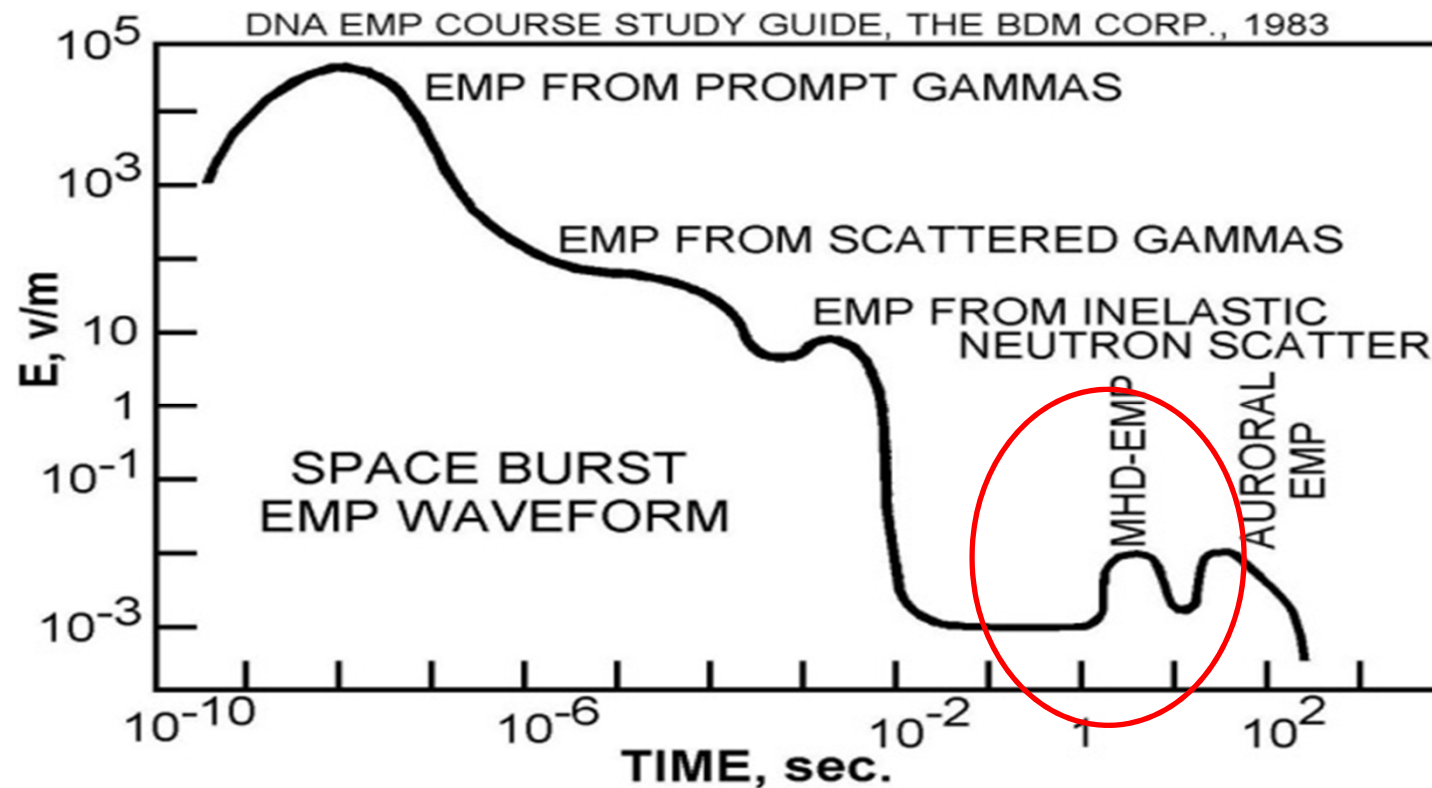
Geomagnetic intensity–March 1989 storm

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

Electromagnetic Pulse (EMP)

- 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

- 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

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