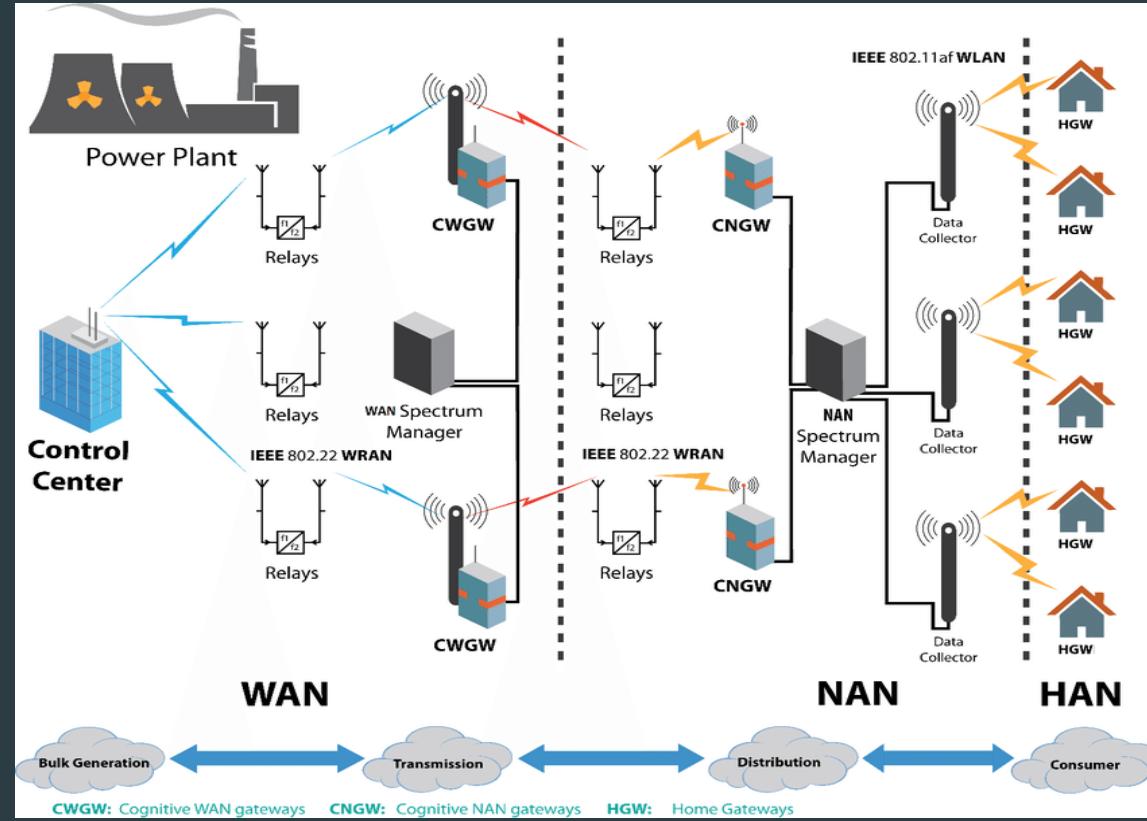


Cyber attacks on smart grid

Overview: network security in SG

- ▶ Enterprise zone
- ▶ Transmission zone
- ▶ Distribution SCADA zone
- ▶ Distribution Non-SCADA zone
- ▶ Interconnected zone



Distribution Non-SCADA network

- ▶ AMI: network between SM and MDMS
 - ▶ NAN
 - ▶ SM
 - ▶ Collector
 - ▶ Head End



Attack a smart meter

- ▶ EPM 6100 by GE:
 - ▶ High class accuracy
 - ▶ Easy to programm and configure
 - ▶ Remote power monitoring with EnerVista



Attack on EPM 6100: Experiment A



385 W load



4.5 Mbps



4 days: final
loss 1.77%



18.6 Million \$
per month



Attack on EPM 6100: Experiment B



400 W load



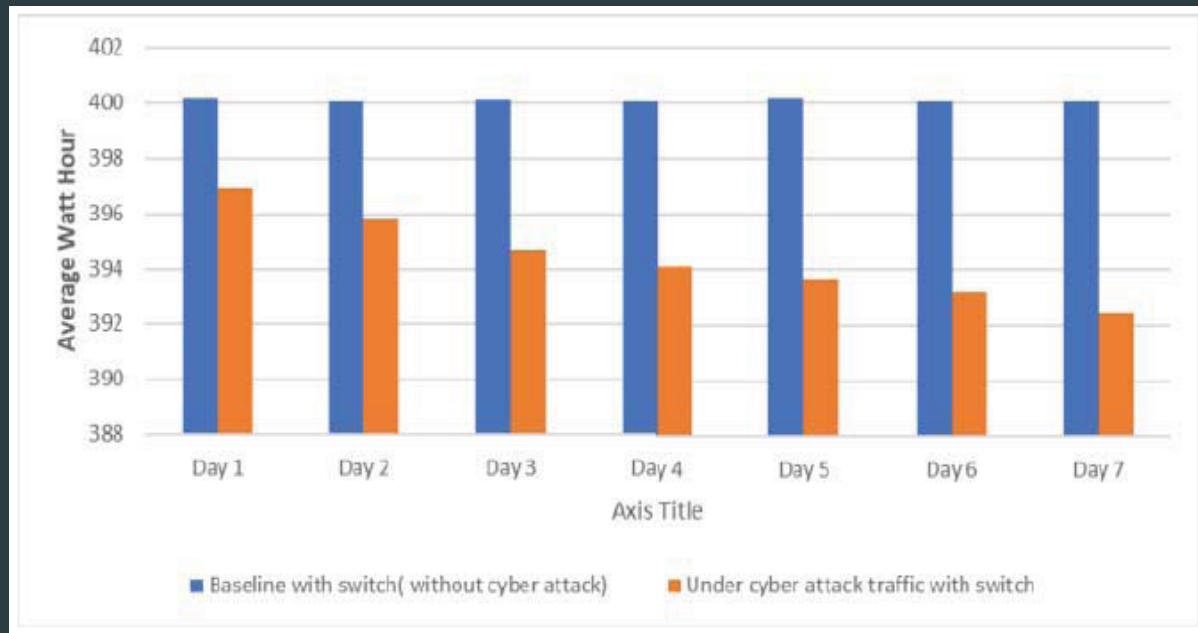
1000 Mbps



7 days: final
loss 1.91%

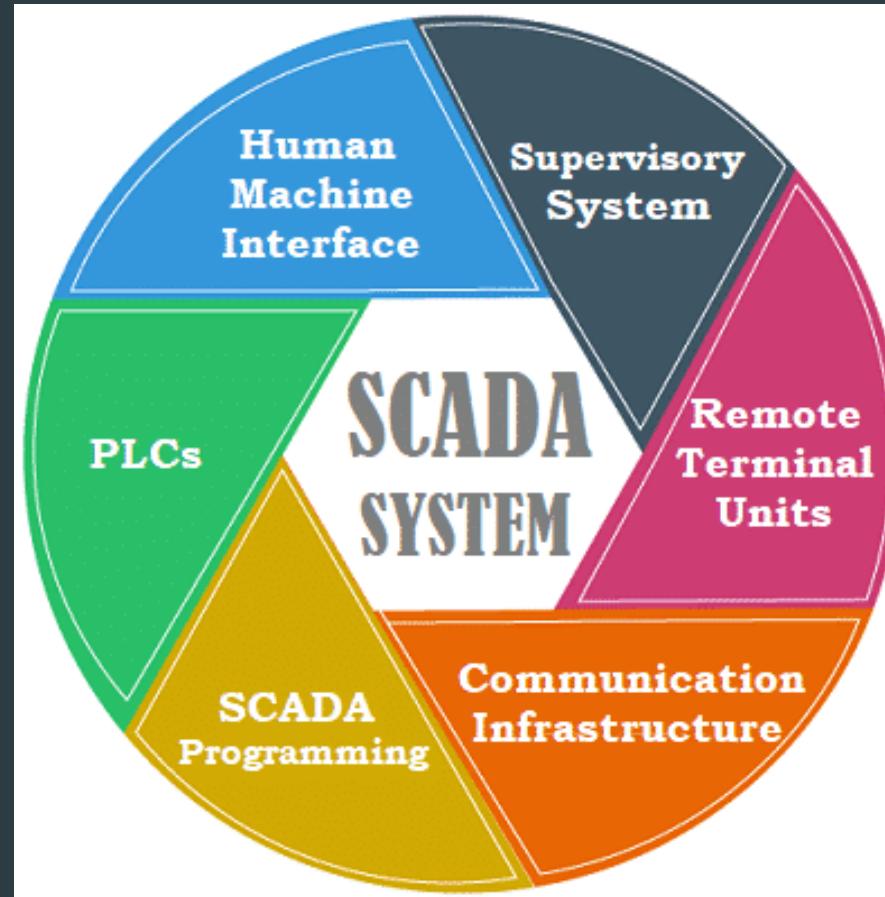


20.9 Million
USD per month



Distribution SCADA zone

- ▶ Monitoring and Control
- ▶ SCADA is made of:
 - ▶ Sensors and actuators
 - ▶ PLC or microcontrollers
 - ▶ Communication network
 - ▶ Server



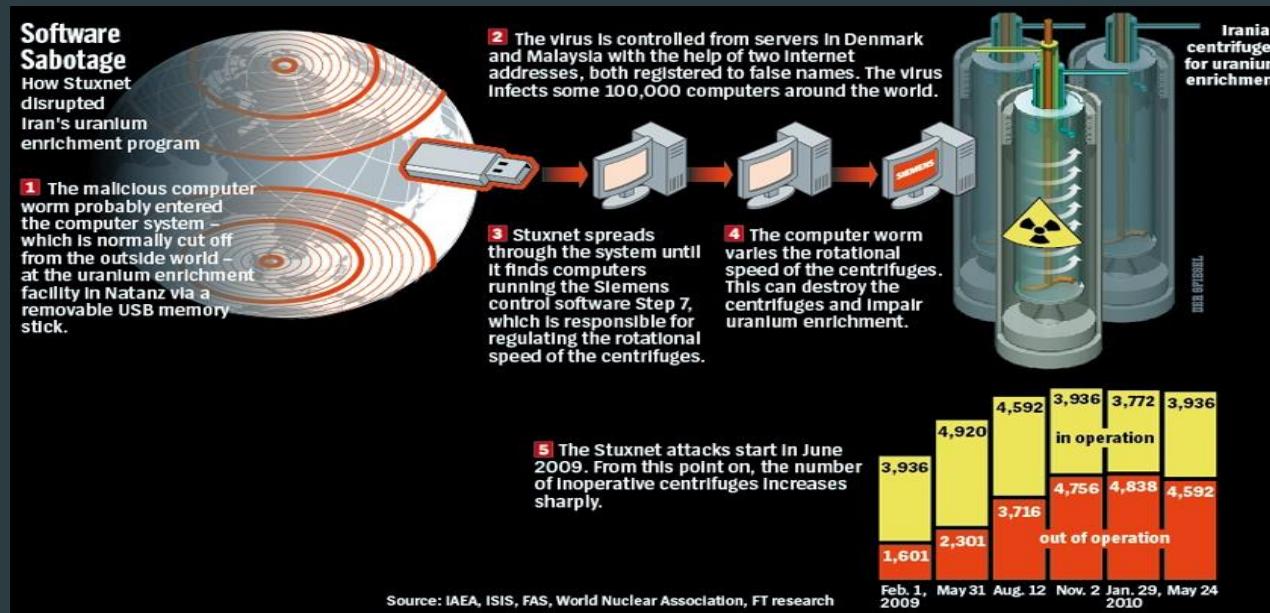
Attack a PLC

- ▶ Siemens S7-300:
 - ▶ 22 different CPU (standard, compact, failsafe, technology)
 - ▶ Different I/O technologies analog and digitals



Stuxnet attack

- ▶ Advanced Persistent Threat Attack
- ▶ Made by US and Israeli Government to attack Iran
- ▶ Works on 2 update: learn and control
- ▶ 3 infections: Windows, s7otbxdx.dll, Siemens S7-300



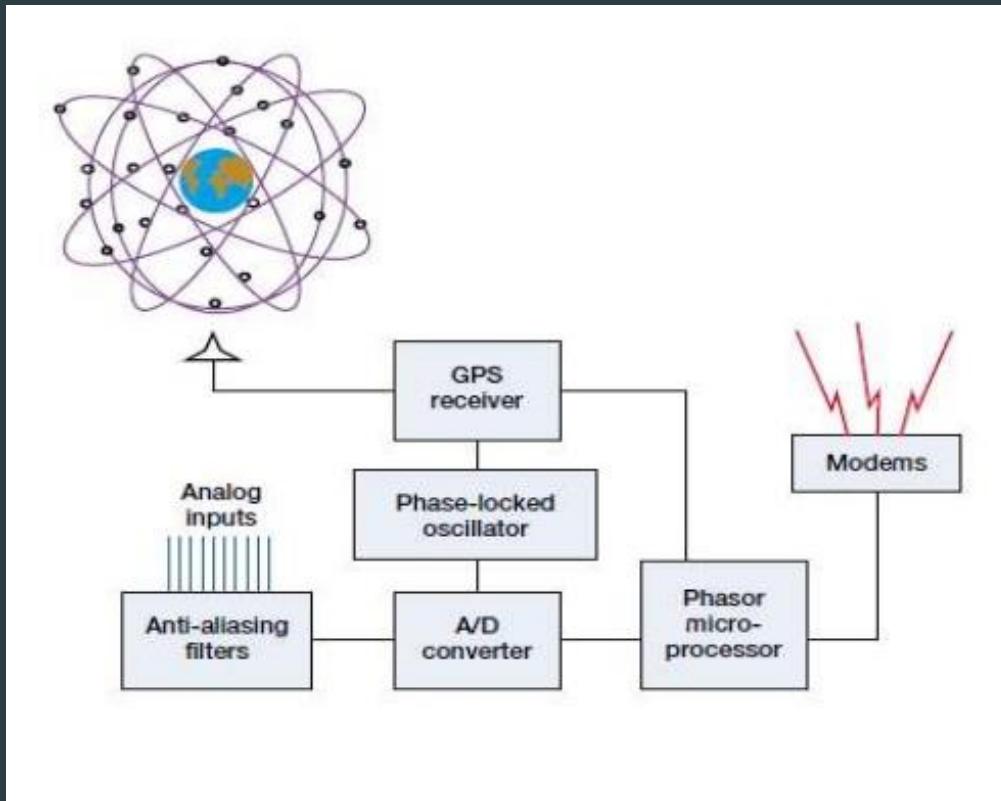
Stuxnet variances

- ▶ 09/2011 Duqu: steal information to attack the industry (key logger)
- ▶ 05/2012 Flame: cyber espionage on Middle Eastern countries
- ▶ 08/2012 Shamoon: attack energy and oil sector of Middle East countries
- ▶ 12/2017 Triton: not even known

 2010 STUXNET Worm Targeting SCADA and Modifying PLCs	 2011 NIGHT DRAGON Large-Scale Advanced Persistent Threat Targeting Global Energy
 2012 SHAMOON Virus Targeting Energy Sector Largest Wipe Attack	 2010 OPERATION AURORA APT Cyber Attack on 20+ High Tech, Security & Defense Cos.
 2012 FLAME Virus for Targeted Cyber Espionage in Middle East	 2013 RED OCTOBER Cyber-Espionage Malware Targeting Govt & Research Organizations
 2011 DUQU Worm Targeting ICS Information Gathering and Stealing	 2012 GAUSS Information Stealer Malware
 2014 HEARTBLEED Security Bug and Vulnerability Exploited by Attackers	 2014 HAVEX Industrial Control System Remote Access Trojan & Information Stealer

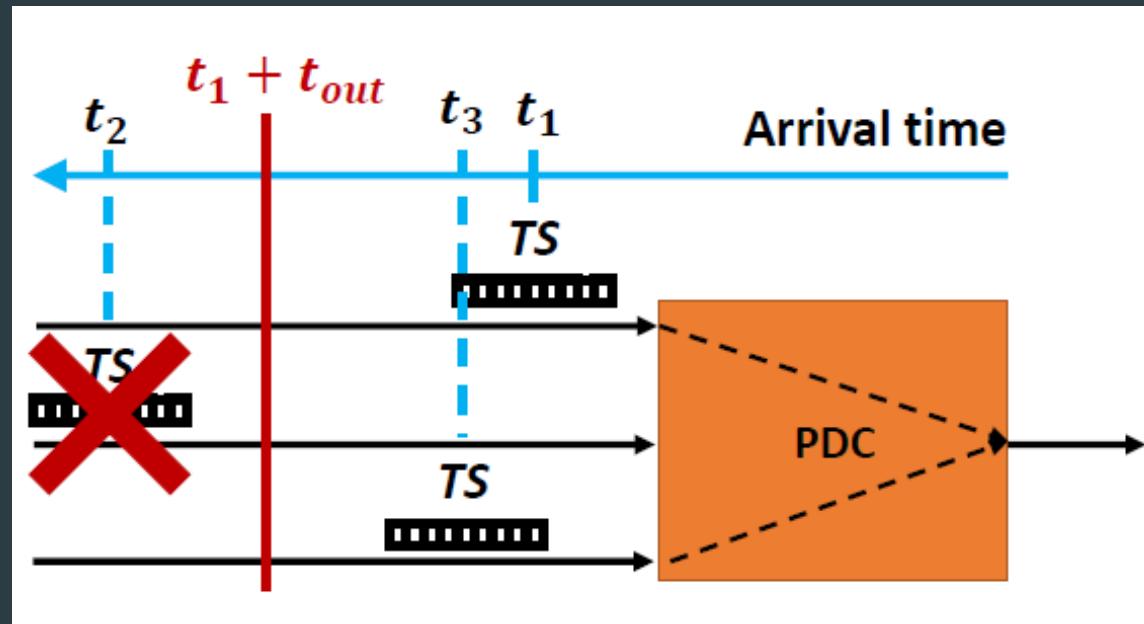
Transmission network

- ▶ PMU:
 - ▶ Replace SCADA measurements
 - ▶ Phasor measurement
 - ▶ Time Synchronized



Attack a PMU

- ▶ Jammer GPS
- ▶ Act as a PMU
- ▶ Delay: hop, modify timestamp
- ▶ Steal data from PDC storage



Storage electrical system

- ▶ The importance on smart grid:
 - ▶ Demand and response
 - ▶ Renewable sources
 - ▶ Store for blackout



Attack a storage system

- ▶ Electrical damage on a single cell to break the accumulator
- ▶ Change environmental temperature: break charge-discharge cycle



How to know if the grid is under attack?

- ▶ State estimation or STAMP



- ▶ Traffic matrix

	Server 1	Server2
Router 1	X1 Mbps	X2 Mbps
Router 2	X3 Mbps	X4 Mbps

- ▶ FMEA: Risk Assessment

f(Threat, Vulnerability)	Level of Risk < Threshold risk
-----------------------------	-----------------------------------



How to protect the grid?

- ▶ Firewall (DMZ)
- ▶ Encryption
- ▶ Logical isolation
- ▶ DBMS protection
- ▶ Constantly update software
- ▶ Biometric authentication
- ▶ Hierarchical authority

