Assessing a Potential Cyberattack on the Italian Electric System

Authors:

Azahara Lorite-Espejo
Daniela Pestonesi
Clementina Bruno
Luca Guidi

Presented by

Kim Jonatan Wessel Bjørneset

What is the article about?

- **An attack on the electrical system in Italy**
- **Structure of the control system**
- **Attack scenarios**
  - Malware
  - DoS
- **Impact of a potensional attack**
  - Costs, economy

Introduction

- Generation, Transmission, Distribution
- What level of security investment should be considered adequate?
- Who bears the costs?
- The damage, distribution between suppliers and customers

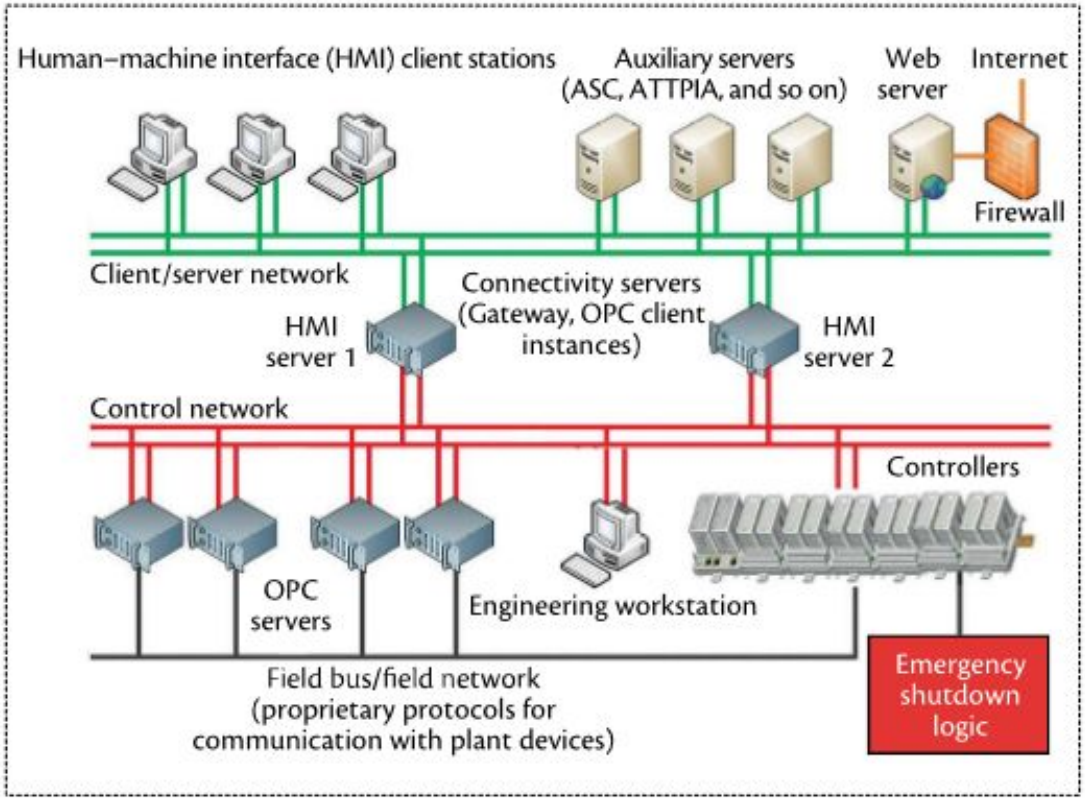
Structure of the Industrial Control System

- **Client/server network**
  - connects HMI client stations of the SCADA and auxilliary servers
- **Control network**
  - connects the controllers, OPC servers and engineering workstations

Implements two protocols:

- IEEE 802.1w Rapid Spanning Tree Protocol
- IEC 62439 Medium Redundancy Protocol

Structure of the Industrial Control System



Attack Scenarios

- **Stuxnet discovered 2010**

- **Malware that exploits vulnerabilities**
  - not only SCADA
  - other systems aswell
- **DoS attack**
  - big delays
  - frozen data and useless info

- **The effects of the scenarios had**
  - both dramatic consequences for network performance
  - different dynamics
  - different durations for recovering
  - situation leading to shutdown
- **Differences for the attacks**
  - Malware took longer to cure than a DoS attack
    - could come from several nodes
  - DoS affected only a few devices
    - easier to isolate from the network
- **Both attacks was considered time consuming**
- **Main consequence is a sudden loss of hundreds of MW**

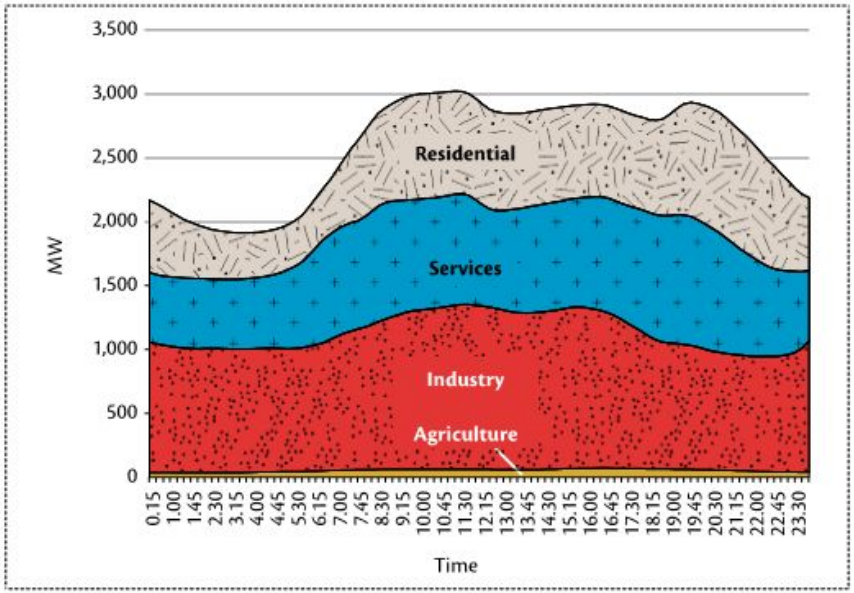
- **Events added for for a realistic scenario**
  - informatics attack on highest generation power plant
  - outages of other plants due to frequency
  - maintainance on the connection to the NTG
  - isolated but supplyed because of the local subgrid
- **Causes a total blackout of the area**

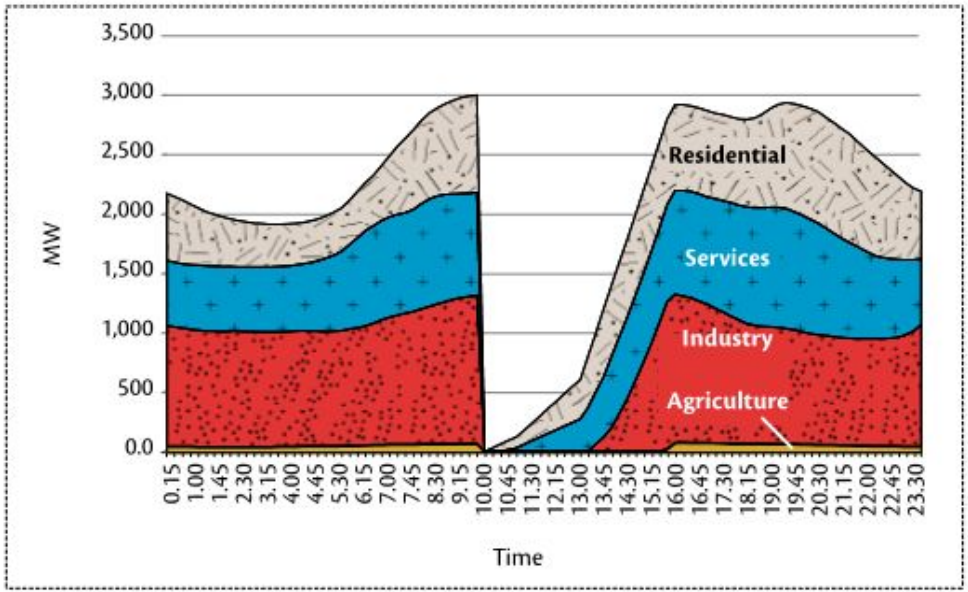
- **1-3 hours for renewable sources**
- **6 hours for a full recovery**

- power plant A—thermoelectric with 1,280 MW of gross power,
- power plant B—thermoelectric with 774 MW of gross power,
- power plant C—thermoelectric with 1,340 MW of gross power,
- power plant D—hydroelectric with 500 MW of gross power,
- power plant E—gas turbine with 180 MW of gross power,
- power plant F—thermoelectric with 470 MW of gross power, and
- photovoltaic and wind-distributed generators with 2,500 MW of total gross power.

Impacts of Attack

Hourly profile in absence of an attack, and in case of an attack





- **Evaluation of the Economic Impact**
  - Productive sector
  - Electricity industry

- **Productive sector**
  - Refers to related work
  - Value Added (VA)
  - Electricity Consumption (EC)
  - Value of Lost Load (VoLL)
  - Gives a good guess of potentionally loss
  - About 35 million euros

$$VoLL_i = \frac{VA_i}{EC_i},$$

- **Electricity industry**

  - Value of unsupplied energy
  - VA lost for generators
  - 2 million euros

average market price: €107.486/MWh;
undelivered energy: 11,542 MWh;
lost revenues for generators: €107.486 × 11,542 = €1,240,602.

$1{,}240{,}602 - (11{,}542 \times 52.83) = €630{,}838.$

This value, adjusted for inflation for the first quarter of 2014, is

VA lost for generators = €636,169.

Conclusion

- **Outage of one part leads to a widespread shutdown**
- **Security investment should therefore be considered**
- **Productive sector suffered much more than the electricity industry**

Evaluation of the article and key findings

- Refers often to other work
  - Shows that they have a lot of work to refer to
  - Knowledge could also be outdated

- Many long sentences with much information ex. ->

> This work provides quantitative empirical support and reports results from the Essence project (*Emerging Security Standards to the EU Power Network Controls and Other Critical Equipment*; http://essence.ceris.cnr.it), founded by the European Commission through the Prevention, Preparedness and Consequence Management of Terrorism and Other Security-Related Risks (CIPS) program, with focus on the monetary impact that a potential cyberattack could have on the electric industry and other productive sectors.) Previous ver-

- Details
  - Goes very deep in details some places
  - Not so deep other places, ex. Stuxnet example

- Attack scenarios
  - Missing details
  - How did they measure the different durations on recovery time?

- Impact of the attack
  - Ignores other costs and other consequences

- Almost 60% “other costs”
- What are the other costs?
- Ignores other costs
  - Mentioned in the text

Table 3. Evaluation of damage from blackout. (Source: Elaboration from Essence Project.)

Sector	Non supplied energy (MWh)	Value of the lost load (VoLL) (per kWh)	Loss of value added (VA) (× 1,000)	Energy dependence (share)	Corrected VoLL (per kWh)	Corrected loss of VA (× 1,000)
Agricultural	382.77	€6.73	€2,575.09	0.40	€2.69	€1,030.04
Industrial						
Food products, beverages, and tobacco	389.86	€3.02	€1,177.40	0.90	€2.72	€1,059.66
Textiles, textile products, and leather products	14.38	€10.25	€147.47	0.90	€9.23	€132.72
Coke, refined petroleum products, and nuclear fuel (chemical and pharmaceutical)	3,248.13	€0.35	€1,124.18	0.90	€0.31	€1,011.76
Mechanical equipment, electric and optical equipment, and transport equipment	544.34	€2.89	€1,573.69	0.90	€2.60	€1,416.32
Gas	21.64	€17.90	€387.43	0.90	€16.11	€348.69
Water	718.89	€1.61	€1,157.41	0.90	€1.45	€1,041.67
Construction	68.35	€59.99	€4,100.49	0.40	€24.00	€1,640.20
Other	910.71	€1.96	€1,788.61	0.90	€1.77	€1,609.75
Services						
Commercial	787.90	€5.35	€4,213.76	0.80	€4.28	€3,371.00
Hotels and restaurants	377.22	€3.33	€1,256.27	0.80	€2.66	€1,005.01
Financial intermediation	53.74	€26.03	€1,398.84	0.80	€20.82	€1,119.07
Other	1,667.00	€14.89	€24,827.31	0.80	€11.91	€19,861.84
Total damage			**€45,727.95**			**€34,647.74**

- Compared this study to other similiar studies
  - About the same result in percentage

- Other consequences
  - Psychological damage
  - Health and lives more important

- Views of the authors only