Enerjide SCADA Sistemlerinin Siber Güvenliği

Barış Sanlı

ISC Turkey 2015

Metodlar

Access (A) refers to how an intruder connects to your network, often enabled by poor basic security practices by employees. The intruder then aims for *persistence (P)* by creating a "foothold" in the network to allow a sustained presence. All of these actions are focused on gaining *control (C)* to achieve the final objective, whether it is to interfere, monitor, steal or alter data, deceive, disable or destroy.

Threat vectors include:	Phases
- **Spear phishing**	A
- **Improperly configured servers or servers with unpatched software vulnerabilities**	A
- **Malicious software**	A, P, C
- **Stolen, legitimate credentials**	A, P, C
- **Destructive/data manipulation attacks**	C
- **Insider threat**	A, P, C
- **Social Engineering**	A
- **Vulnerable networks connected to the target network that enjoy a trust relationship**	A, P
- **USG personnel, at home and at work**	A, P, C

Enerji Sektörü ne kadar kritik

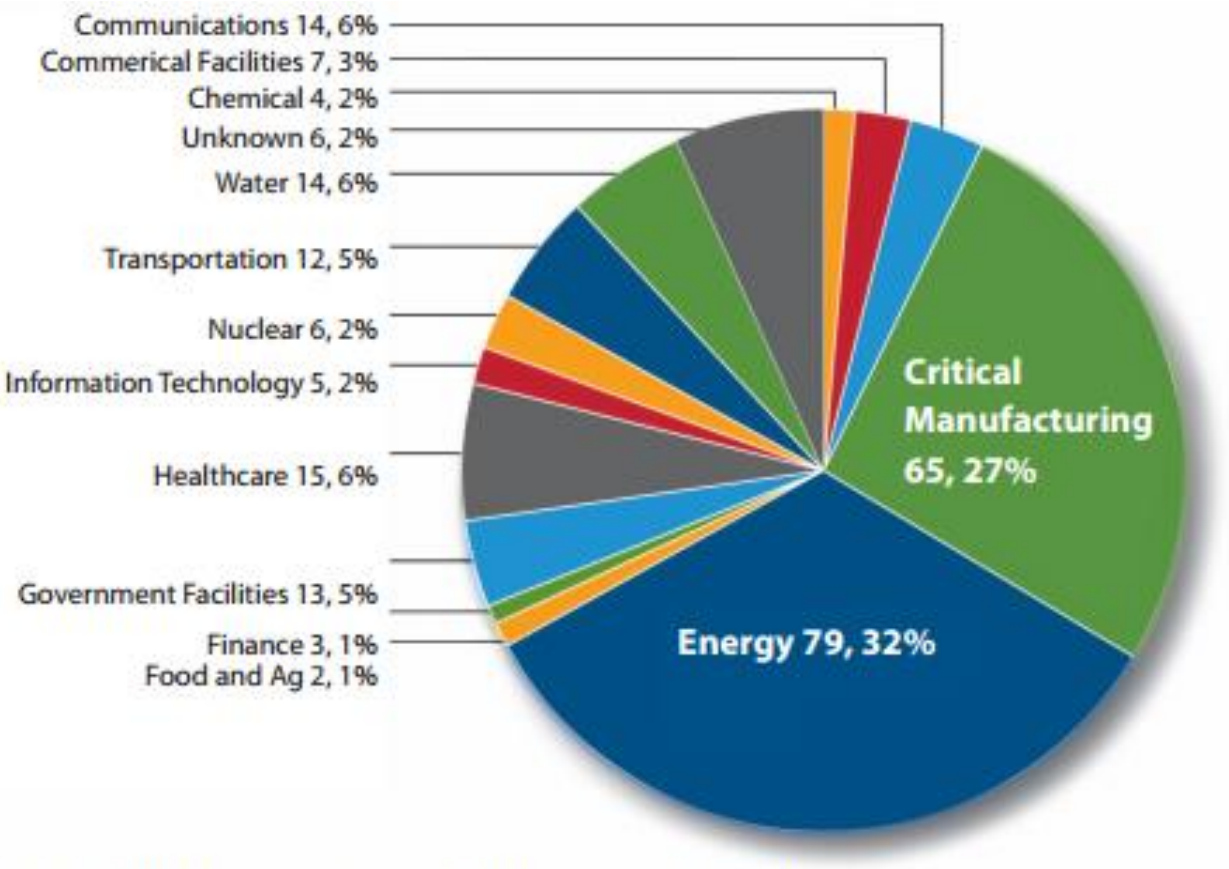
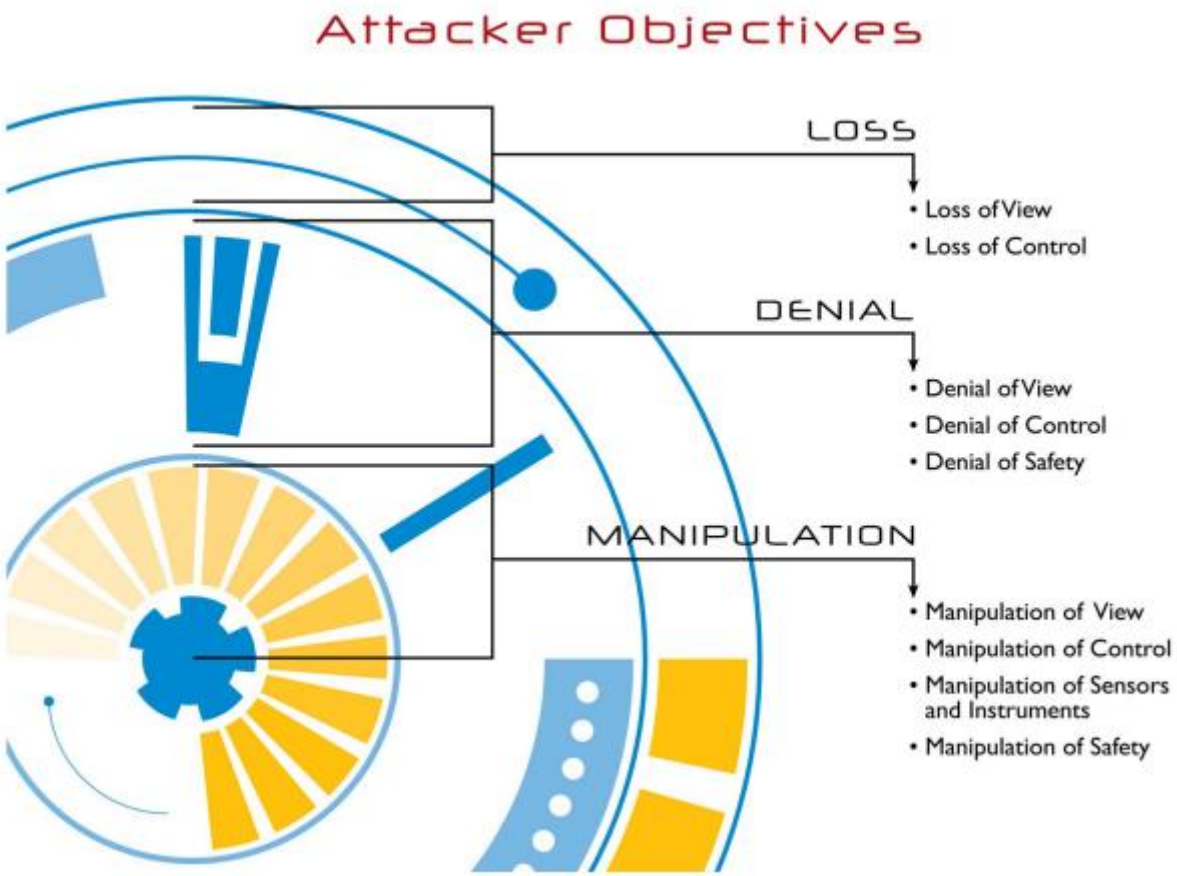


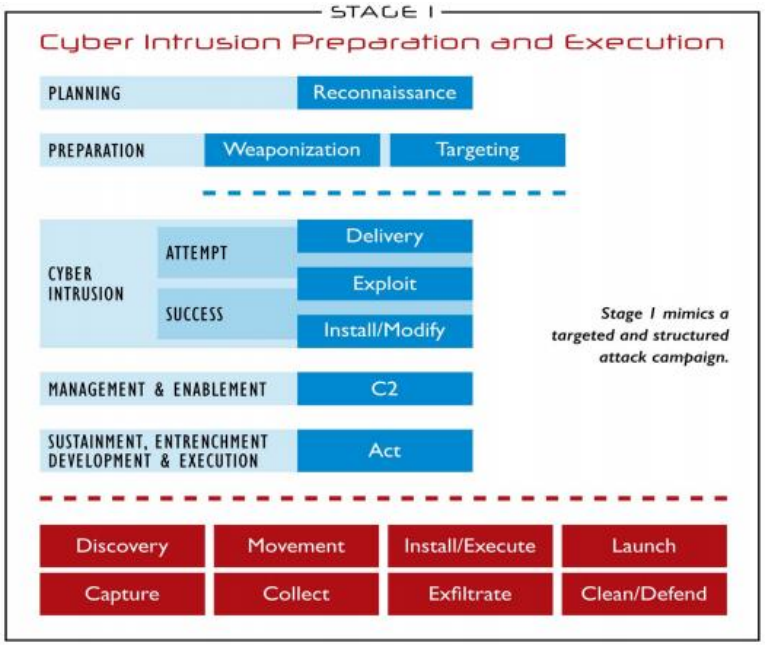
Figure 1. FY 2014 Incidents Reported by sector (245 total).

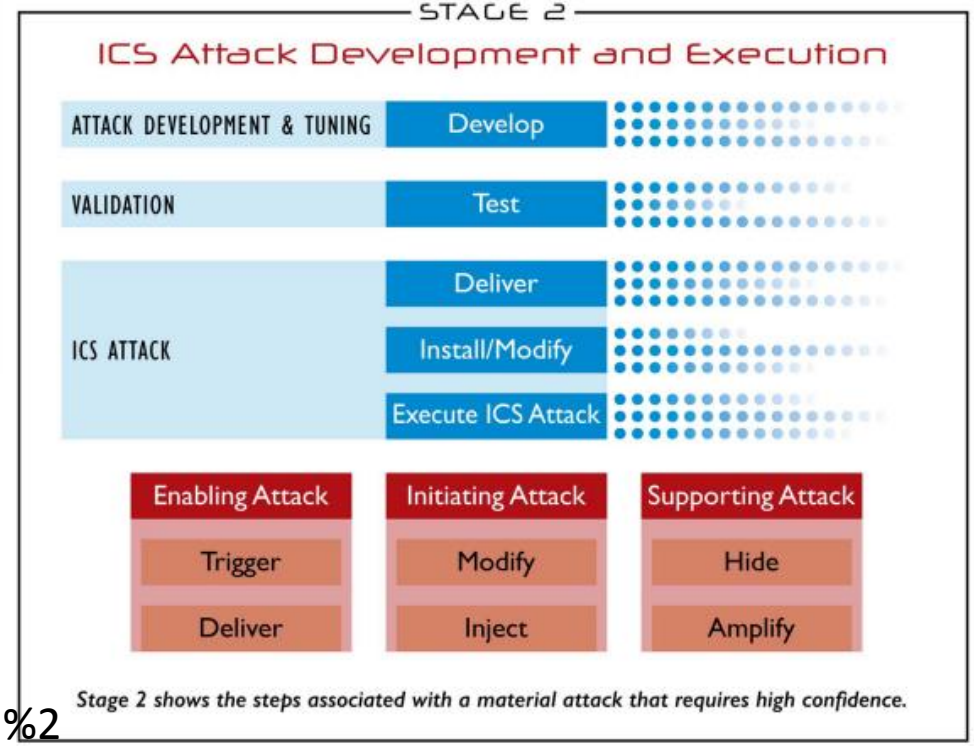
https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

Saldıranların amaçları



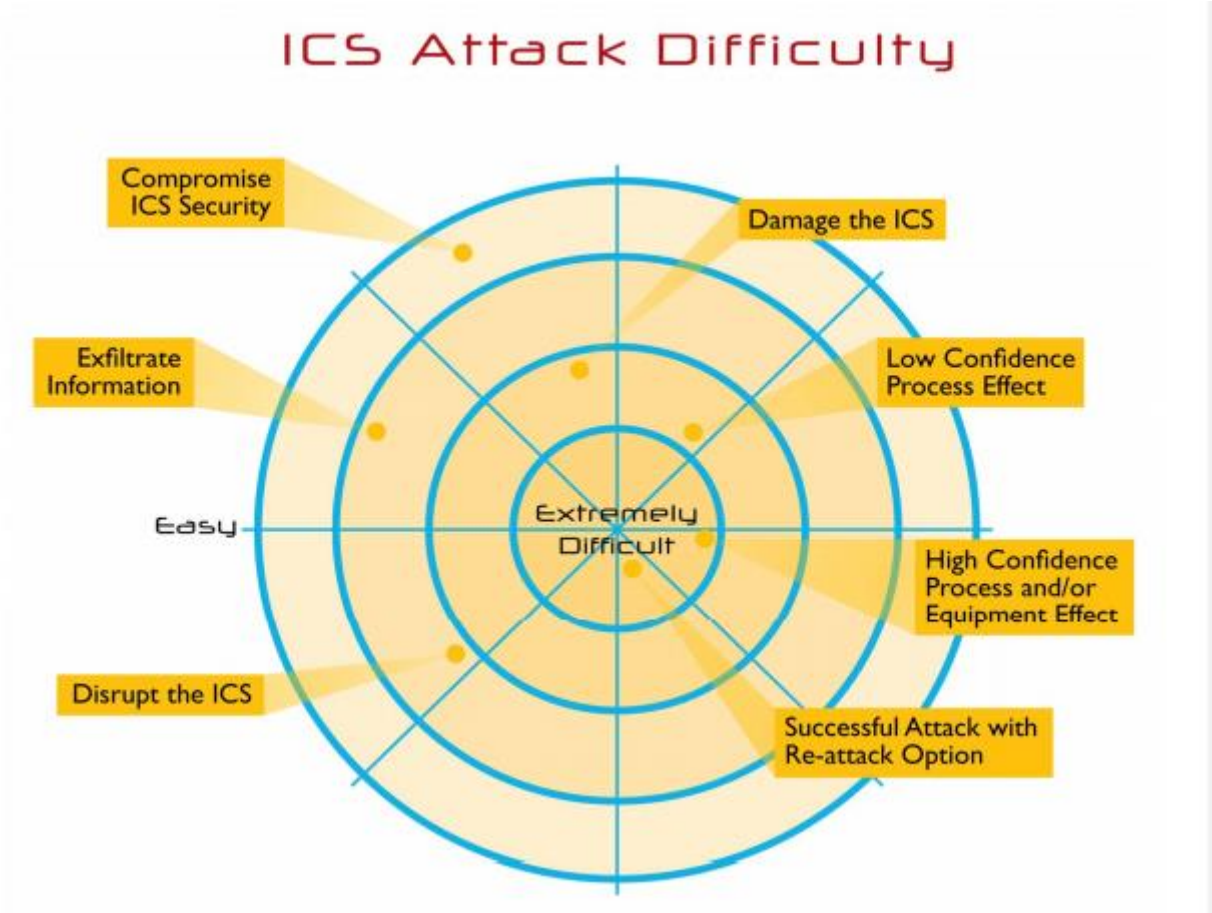
Aşamalar





https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/S2015/D1_1300_SANS%20ICS%20-%20ICS%20Cyber%20Attacks%20Fact%20vs.%20Fiction%20and%20Why%20it%20Matters_Lee_REL_fp.pdf

SCADA Saldırısı ne kadar zor



TÜRKIYE

Wikileaks – Türkiye KEA

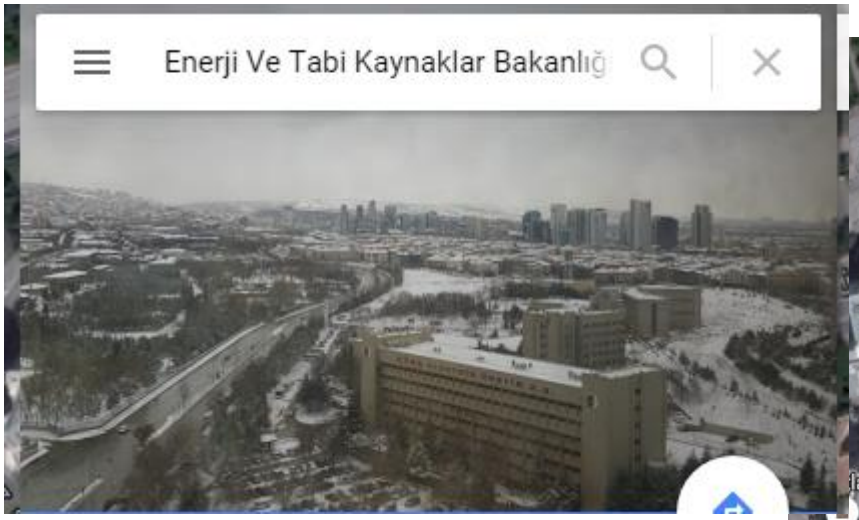
Justification for modifying: The Turkish Straits are among the most hazardous, crowded, difficult to navigate and potentially dangerous natural waterways in the world. Ships carrying 143 million metric tons of petroleum products, including 96 million metric tons of crude oil, transit the straits every year. The closure or disruption of any of these critical infrastructures would impede the flow of significant amounts of crude oil to world markets.

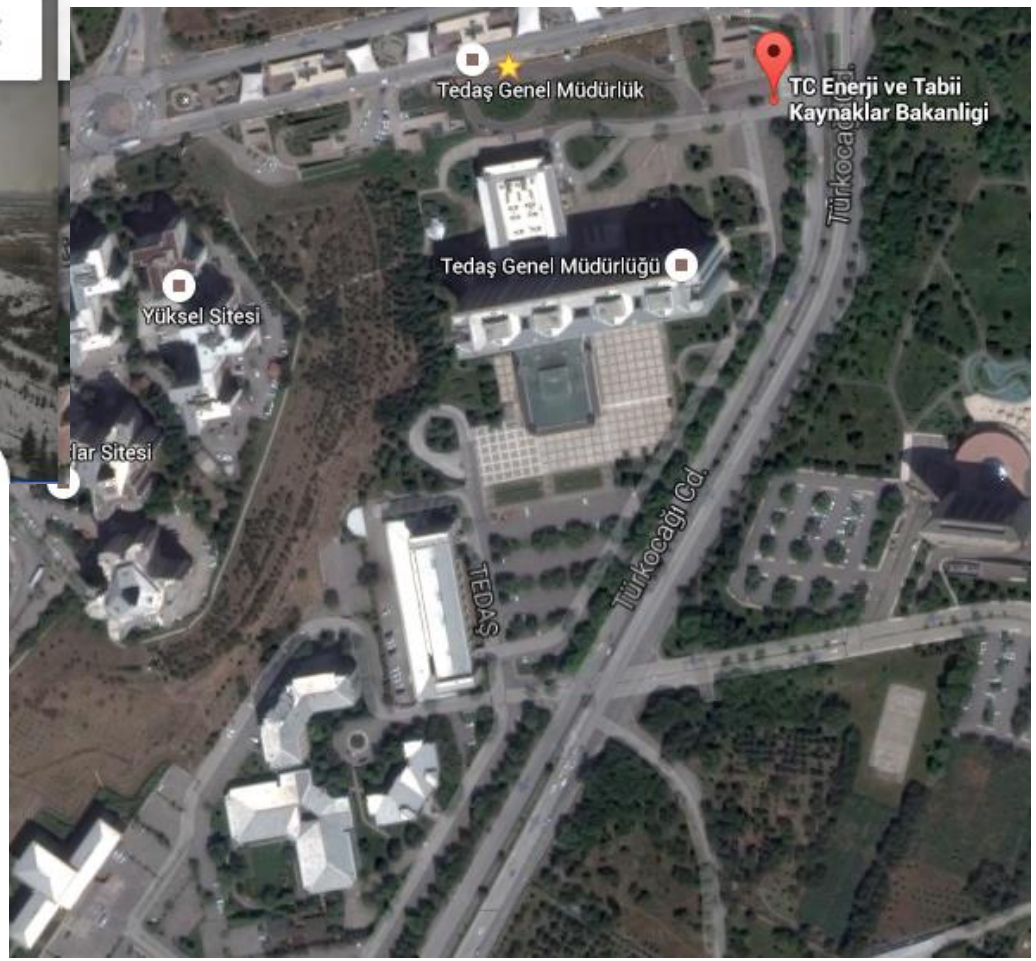
Post believes the Baku-Tbilisi-Ceyhan pipeline and Ceyhan port terminal may be an active target of terrorist groups. In August, 2008, a designated terrorist group, the Kurdish Workers' Party (KGK/PKK), claimed responsibility for an attack on the eastern section of the pipeline that temporarily disrupted its flow. The government, however, asserted the incident was the result of a technical failure.

6. (S) The Government of Turkey does not have a specialized agency responsible for CI/KR security. That task falls to the Turkish military, law enforcement agencies and enterprises' own security guards.

https://wikileaks.org/plusd/cables/09ANKARA406_a.html

ETKB Kampüsü





Snowden Belgeleri

TOP SECRET STRAP1 COMINT

MHS/GCHQ Projects - (TS//SI) Turkey Energy Company Development

• Requirement - The Energy Security Team within GCHQ's OPI-TSI require any indication of where the traffic for the following companies is going and ideas for improving access and collection. They are especially interested in MENR and the balance of power they have established.

• Key organisations: Ministry of Energy and Natural Resources (MENR), Deputy Directorate for Energy, Water and the Environment (MFA), BOTAS (Turkish Energy Company), TPAO (Turkish Petroleum Corporation), Calik Enerji.

• Key personalities: Hilmi Guler (Energy Minister), [redacted]

• GCHQ Customer - OPI-TSI [redacted]
• MHS POC - [redacted]
• Start Date - 29 Oct 08
• Estimated End Date - 2 Mar 09
• Project Status - Assigned

Assigned analysts: [redacted]

• Project Notes
• 29 Oct 08 - Analysts assigned
• 29 Oct 08 - Analysts to target company buildings, identify satellite comms and other technologies being used. Links from comms to be surveyed by NMDC and results in Roadbed analysed.
• 07 Jan 09 - Following attempts to acquire imagery from MHS sources for MENR, BOTAS and TPAO buildings in Ankara, requested TOPI submit a task through JARIC for building rooftop imagery.

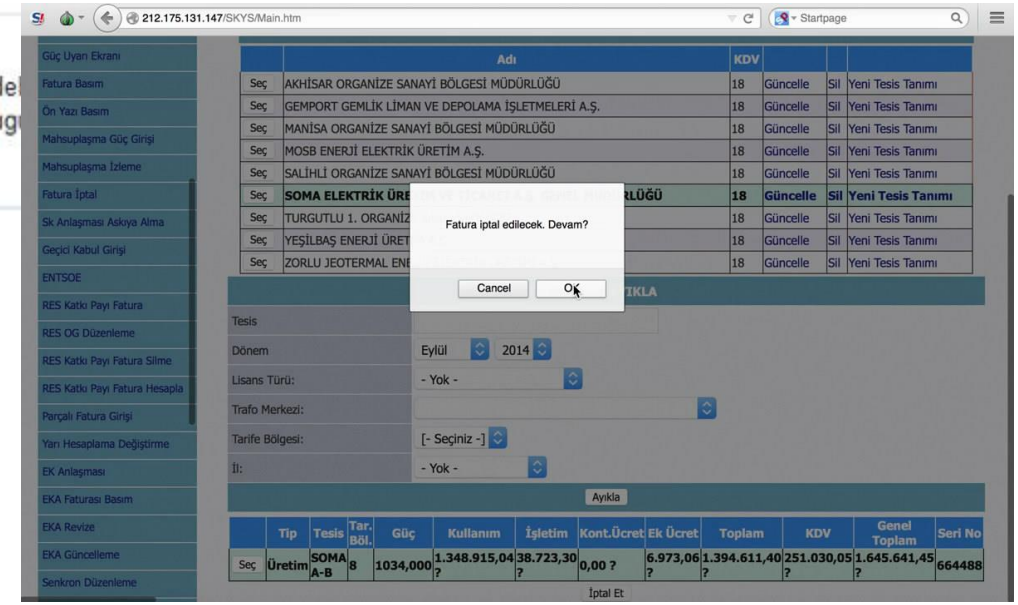
Redhack – TEİAŞ hack (14 Kasım 2014)

Pin it

ck - KizilHack @KizilHackerLAR · 22 dk.
Turkiye'deki tum ELEKTIRIK islerini online olarak yapan, borc mahkeme vb gosteren sistemde 1 haftadir top oynadik pasteht.ml/r4EPV
33 19 ••• Sohbeti göster

RedHack - KizilHack @KizilHackerLAR · 24 dk.
Türkiye Elektrik İletim A.Ş. teias.gov.tr /yedekdavatakib… tarafimizca hacklenmistir
Sifreler: pasteht.ml/r4EPV
Kapanmadan girin BORC silin:)
93 34 •••

RedHack - KizilHack @KizilHackerLAR · 30 dk.
Az sonraki eylemimizi Yirca koylulerine, Valide
hayatta paradan, mevkiden degerli seyler oldug
53 38 •••



BTC Boru hattı (5 Ağustos 2008, Refahiye)

- Alexander Dugin : “BTC Dead”
- “Hackers had shut down alarms, cut off communications and super-pressurized the crude oil in the line, according to four people familiar with the incident who asked not to be identified because details of the investigation are confidential.”
- SANS-ICS

http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

31 Mart Kesintisi – Atış Serbest

OPINION

Iran Flexes Its Power by Transporting Turkey to the Stone Age

By Micah Halpern • 04/22/15 10:31am

COMMENT

http://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/

31 Mart Kesintisi – ENTSO-E Raporu

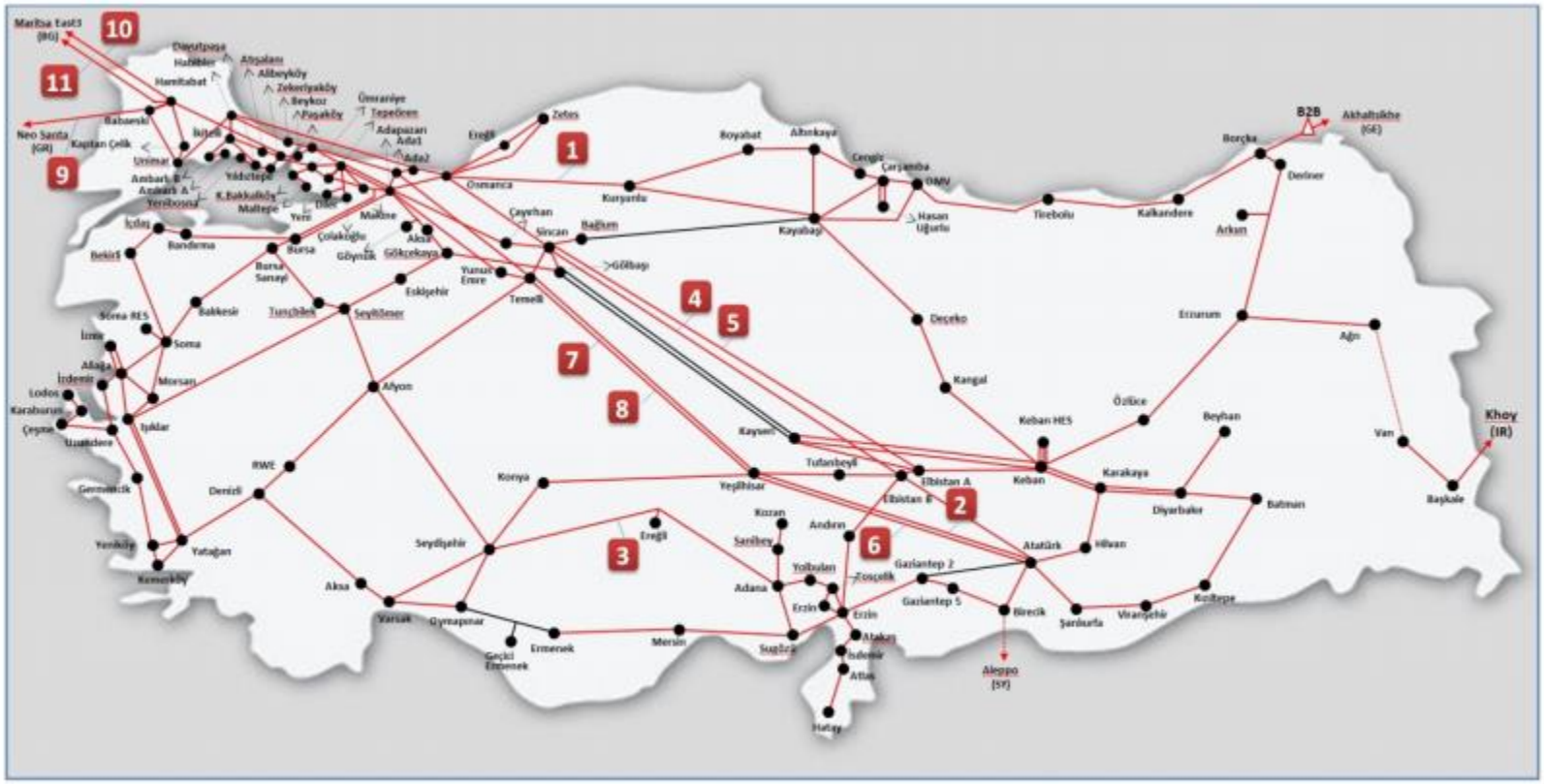


Figure 1: Turkish transmission system map with sequence of events

Entso-E Raporu

2. Prior to the blackout there was no adequate awareness about the importance of the series capacitors for angular stability of the system operation condition.
3. Although the Turkish 400 kV grid is equipped with a protection system that is in line with international standards, the effect of the distance relay settings on the line that tripped first was not correctly evaluated.

Critical Factors

In addition to the main causes described above, the following two factors contributed in a negative way to the event evolution.

1. Reliable on-line automatic contingency analysis and off-line angular stability analysis were not yet available in the National Control Centre (NCC).
2. Not enough attention was paid in the NCC with respect to the angular stress in East-West direction throughout the Turkish grid.

Türkiye'yi hedef alan - Dragonfly

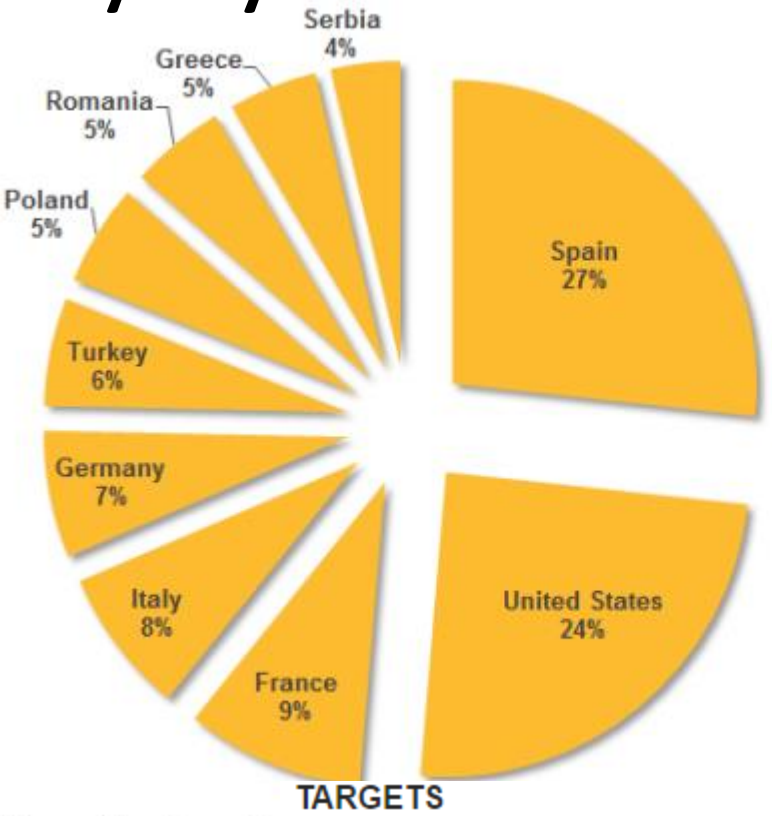


Figure. *Top 10 countries by activ*

- Aviation Industry – US and Canada (Pre 2013)
- Defence Industry – US and Canada (Pre 2013)
- Energy Industry – US and Europe (Spain, France, Italy, Germany, Turkey, Poland)
  - Energy Grid Operators
  - Major Electricity Generation Firms
  - Petroleum Pipeline Operators
  - Energy Industry, Industrial Control System (ISC) Equipment Manufacturers

Almanya’da Çelik Fabrikası Saldırısı

- In one case they noted that a malicious actor had infiltrated a steel facility. The adversary used a spear phishing email to gain access to the corporate network and then moved into the plant network. According to the report, the adversary showed knowledge in ICS and was able to cause multiple components of the system to fail. This specifically impacted critical process components to become unregulated, which resulted in massive physical damage.

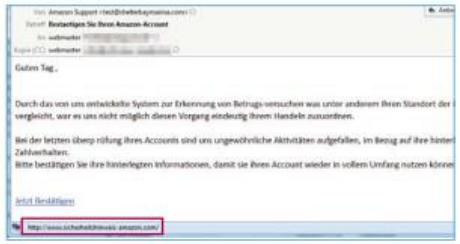
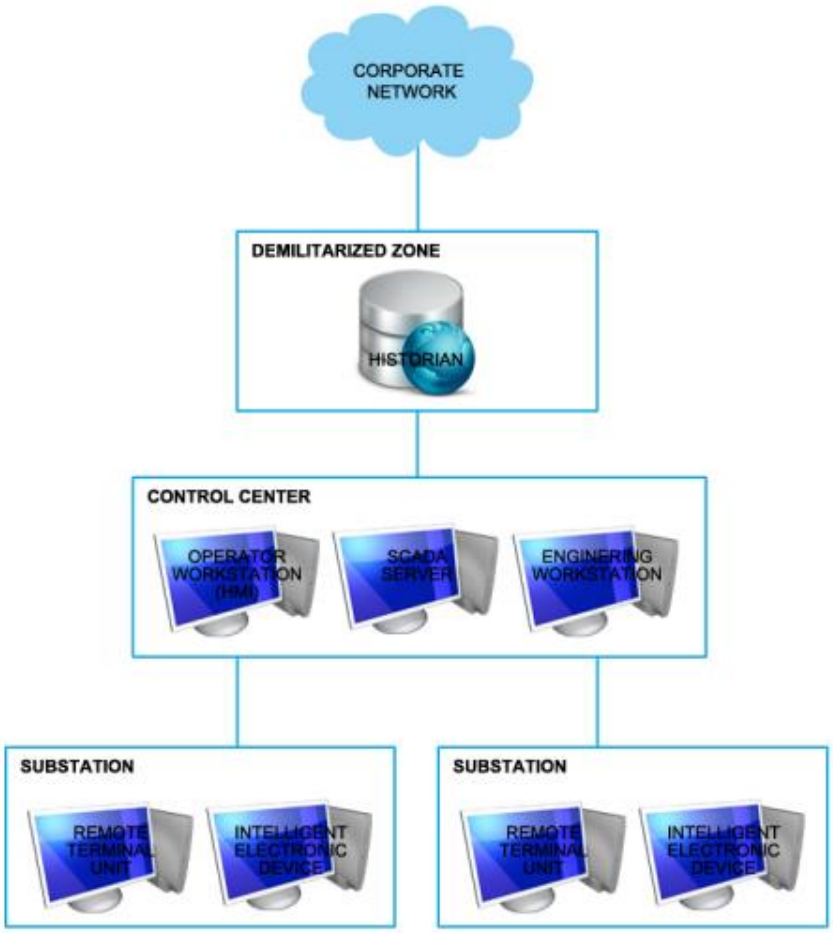


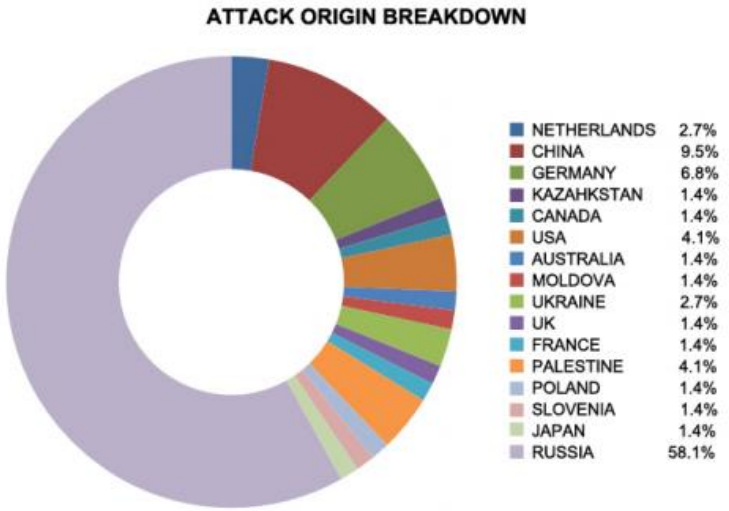
Abbildung 5: Beispiel einer Phishing-Mail – erkennbar an der gefälschten Absenderadresse

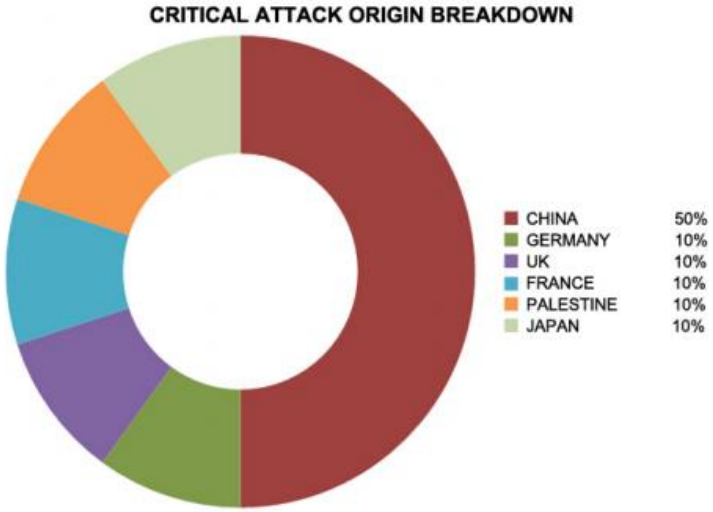
Abbildung 6: Beispiel einer Phishing-Webseite – erkennbar an der gefälschten URL

https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

2013 ICS Baltuzağı deneyi







https://media.blackhat.com/us-13/US-13-Wilhoit-The-SCADA-That-Didnt-Cry-Wolf-Whos-Really-Attacking-Your-ICS-Devices-Slides.pdf

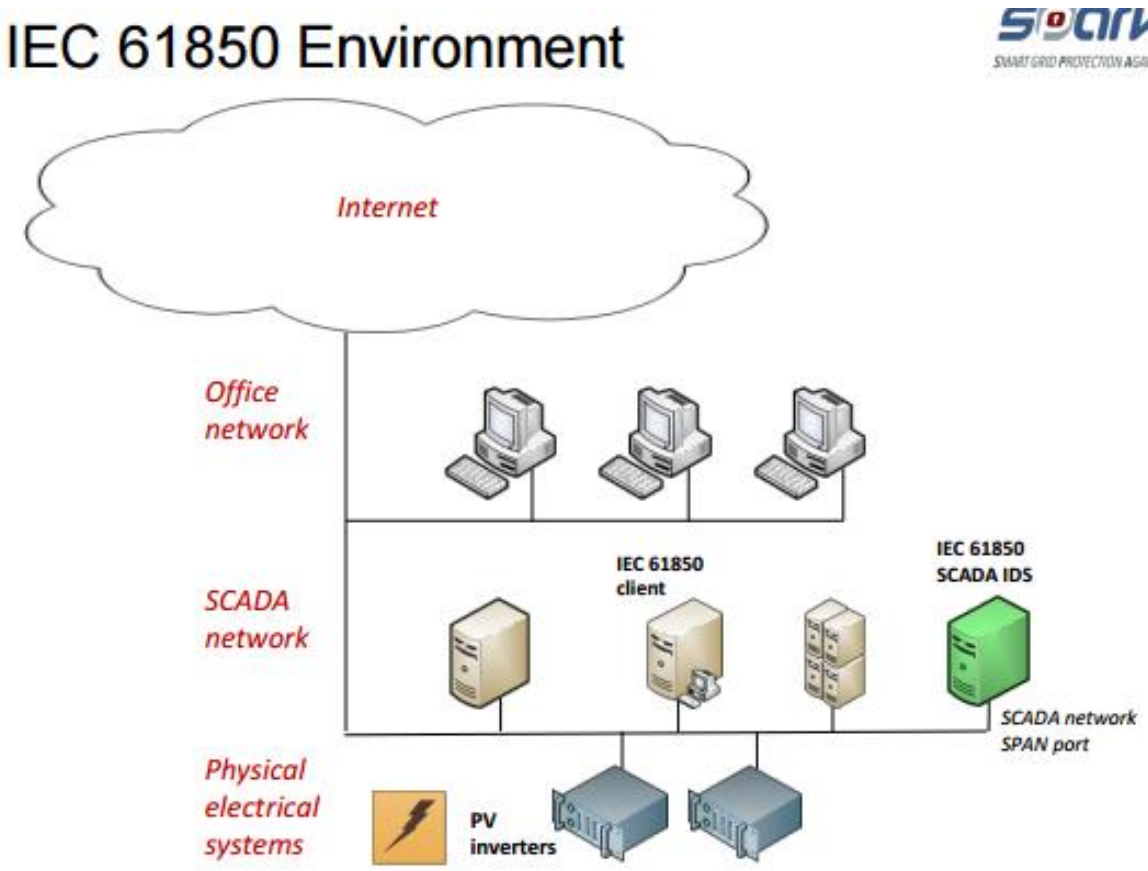
SCADA sistemleri

- Sistemlerde siber güvenlik düşük
- Sistem mesajları şifresiz
- Şifreleme, kullanıcı doğrulama düşük
- Eski protokoller

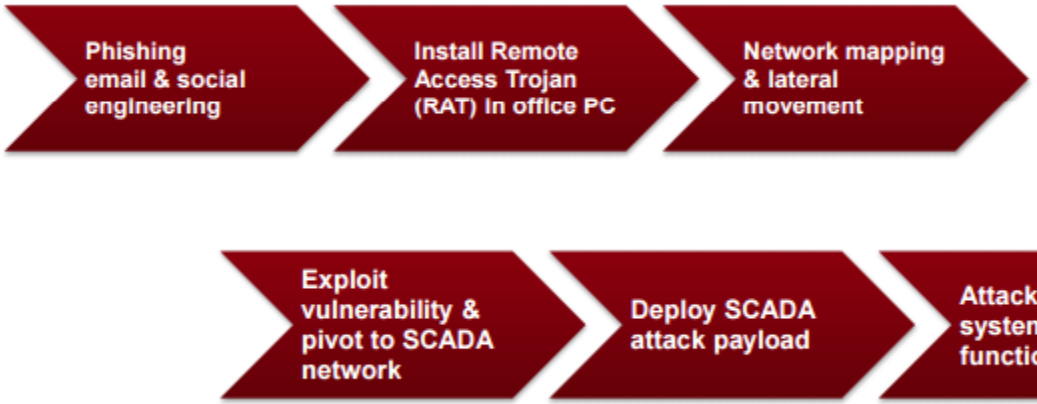
- Akıllı Şebeke sistemleri - > Siber-fiziksel sistemler

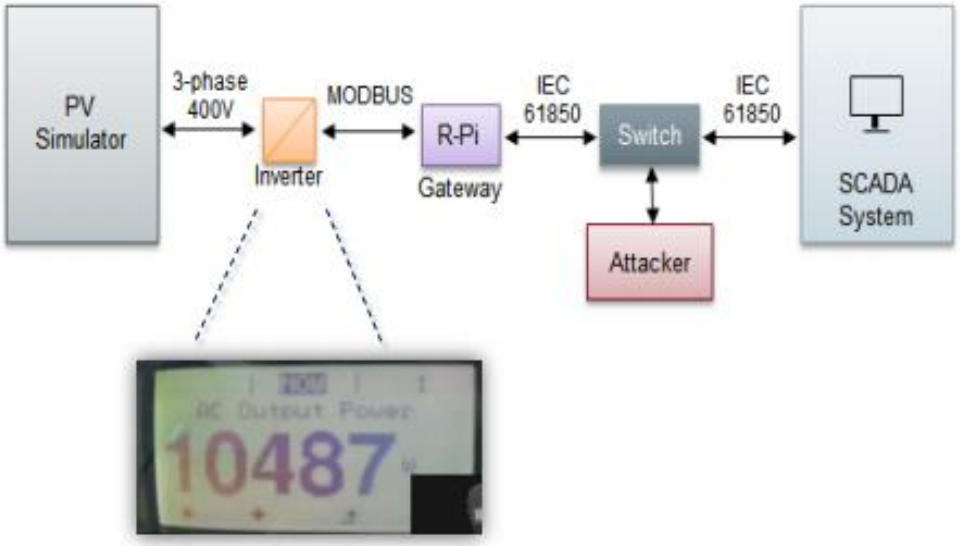
https://project-sparks.eu/wp-content/uploads/2015/02/04-mclaughlin-scada-ids-sparks.pdf

Akıllı Şebeke Sistemi

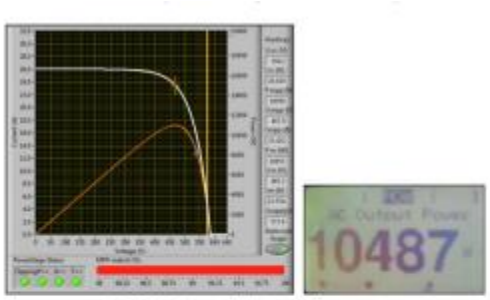


Hedeftaki Inverter

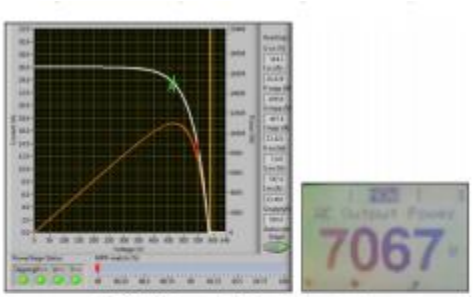




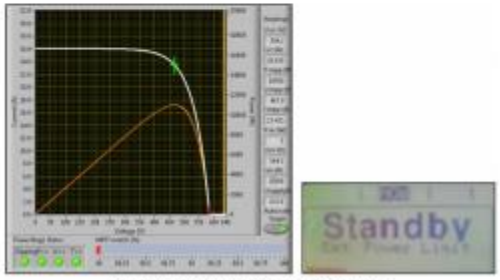
PV Panel Değer düşümü



(a) 100% of power limitation by the operator



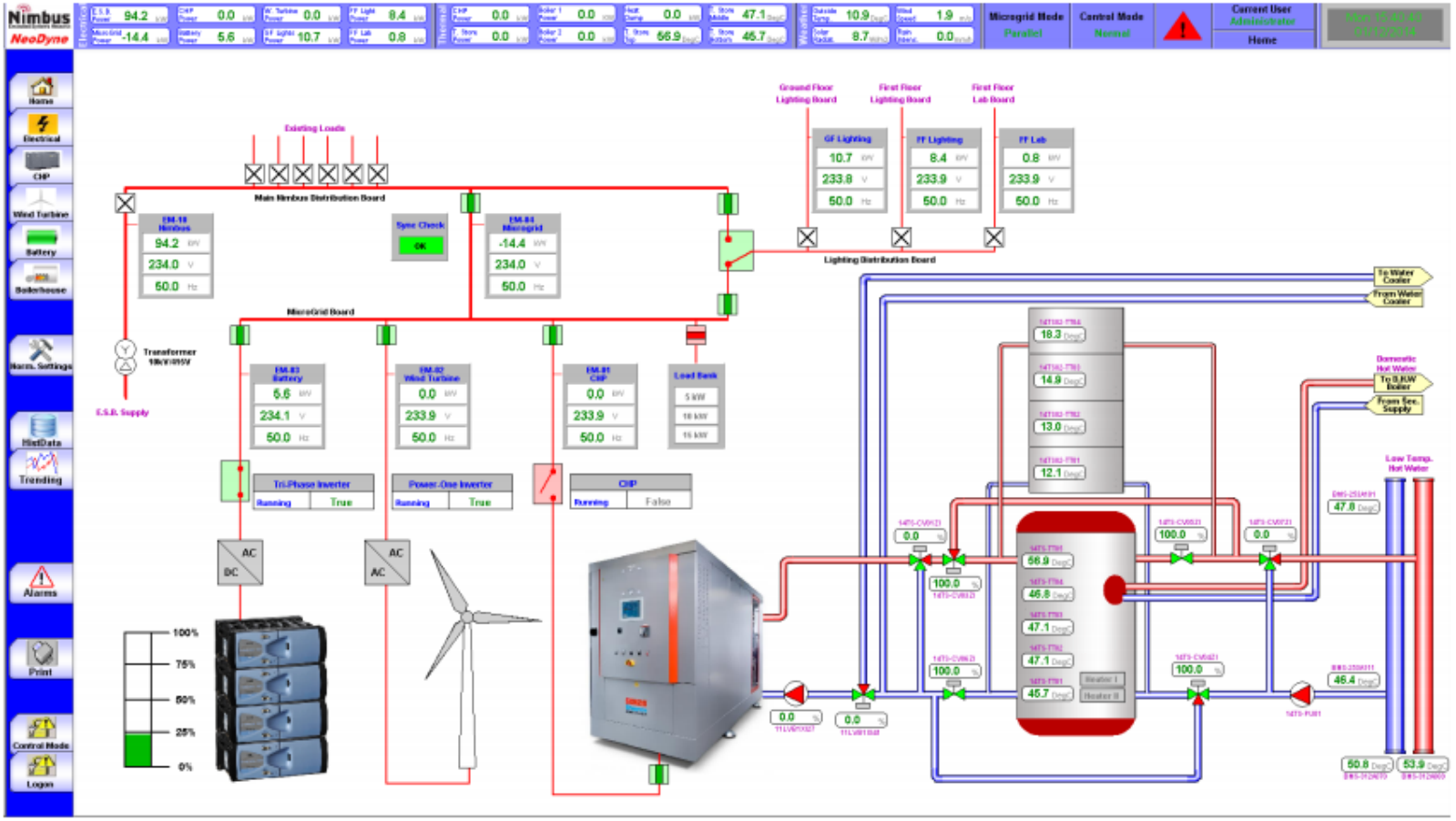
(b) 60% of power limitation by the operator



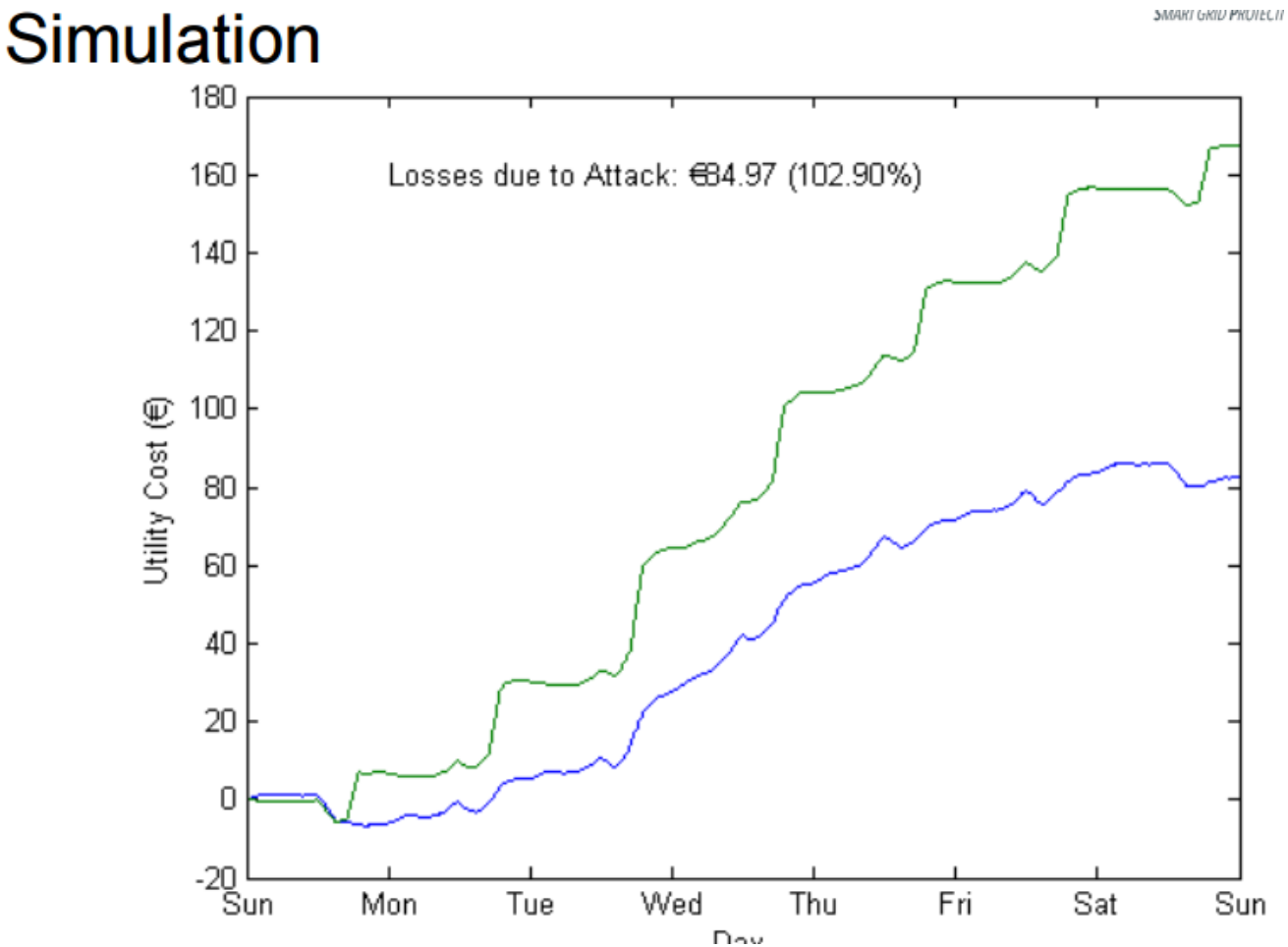
(c) 10% of power limitation by the operator

https://www.eclipse.org/4diac/uws/2015/UW_06_Strasser.pdf

Microgrid saldırısı



Simulasyon



https://project-sparks.eu/wp-content/uploads/2015/02/09-chabukswar-modelling-impact-sparks.pdf

Gelecek - Tartışma

- Daha fazla boru hattı
- Daha fazla elektrik santrali
- Daha dağınık bir üretim
- IoT
- Akıllı Tüketim/Şebeke

Teşekkürler

- Google «Barış Sanlı»