ABB SpA ABB Power and productivity for a better world™

ADConsulting

Deloitte.

UPO UNIVERSITÀ DEL PIEMONTE ORIENTALE

Enel L'ENERGIA CHE TI ASCOLTA.

JEN

PSE Polskie Sieci Elektroenergetyczne

essence

Consiglio Nazionale delle Ricerche
IRCRES
ISTITUTO di RICERCA sulla CRESCITA ECONOMICA SOSTENIBILE
INSTITUTE of RESEARCH on ECONOMIC SUSTAINABLE GROWTH

Essence - Emerging Security Standards for the EU power Network controls and other Critical Equipment

2012-2014

Elena Ragazzi (elena.ragazzi@ircres.cnr.it)

Alberto Stefanini (Alberto_stefanini@virgilio.it)

Clementina Bruno (clementina.bruno@uniupo.it)

Milano, 28 settembre 2015

Cybersecurity e smart grids (note sul documento 255/2015)

- E' molto importante che il documento 255/2015 si sia focalizzato, seppur brevemente, anche sul tema della cyber-security
- Si tratta infatti di un elemento essenziale da considerare nella progettazione dei sistemi, nonché nei sistemi di regolamentazione che li controllano e/o incentivano.
- E' una tematica di cui si discute da circa 20 anni in relazione alle reti elettriche (ma è di grande attualità anche con riferimento ad altre infrastrutture critiche)
- Il progetto ESSENCE ha approfondito questa tematica per quanto concerne la rete di trasporto ed i maggiori stakeholder nel campo della generazione. L'approccio metodologico utilizzato, tuttavia, sarebbe efficacemente estendibile anche al segmento della distribuzione, e più specificamente, al campo delle smart grid. Le conclusioni emerse dall'attività di ESSENCE possono dare un'idea dell'utilità di un approfondimento nel settore

ESSENCE

→ Il progetto Essence (***E**merging **S**ecurity **S**tandards to the **E**U power **N**etwork controls and other **C**ritical **E**quipment)* propone una valutazione costi-benefici dell'implementazione di standard di sicurezza nel sistema elettrico.

→ L'approccio è decisamente pragmatico in quanto si basa su due ipotetici *case studies:* "caso studio italiano" (generazione) e "caso studio polacco" (trasmissione).

ESSENCE

- L'attività parte da una rassegna dello stato dell'arte nell'ambito degli standard di sicurezza
- Identifica vulnerabilità esistenti nel sistema elettrico
- Propone una stima monetaria:
  a. Dell'impatto di un evento (blackout - 6h) che può essere determinato, al verificarsi di particolari circostanze, dallo sfruttamento di una vulnerabilità attraverso un attacco informatico. Tale grandezza costituisce il beneficio – o risparmio di costo - derivante dall'implementazione degli standard. La stima è declinata su operatori elettrici, famiglie e "non-famiglie" (imprese).
  b. Del costo di implementazione di Standard di sicurezza come contromisure. Sono stati quantificati sia i costi di investimento (investment), che di mantenimento (maintening). Si sono inoltre prese in considerazione due situazioni: costi da sostenere se nessuno standard fosse ancora implementato (no security) oppure costi da sostenere partendo dal livello di sicurezza corrente, per incrementarlo (delta).

ESSENCE – sintesi risultati

(dati in milioni di €)

ITALIAN CASE STUDY

BENEFIT		COST	Delta	No protection
Electricity operators	2	Investment	20-40	28-53
Non households	35-46	Maintaining	3.5-6	6.5-12.9
Households	36-64			
TOTAL	73-112			

POLISH CASE STUDY

BENEFIT		COST	Delta	No protection
Electricity operators	0.7	Investment	7.5	26
Non households	25-35	Maintaining	2.5	5
Households	30-61			
TOTAL	55.7-96.7			

ESSENCE - conclusioni

- Esistono importanti vulnerabilità all'interno dei sistemi di controllo degli impianti di produzione e di trasmissione dell'elettricità. I *case-studies* sviluppati in Essence mostrano che, in circostanze particolari, queste vulnerabilità possono essere sfruttate per indurre black-out di lunga durata che coinvolgono ampie porzioni di territorio.

- L'adozione delle contromisure necessarie a mitigare tali vulnerabilità, implica un investimento notevole per l'impresa, peraltro difficile da preventivare, il cui costo deve essere calcolato basandosi sul reale stato delle infrastrutture in esame.

- Il beneficio economico connesso alla protezione del sistema dal rischio di black-out è molto grande e decisamente superiore all'investimento per l'adesione a uno standard di protezione. Tale beneficio ricade però prevalentemente sulla collettività e avvantaggia solo in minima parte l'impresa. Questo costituisce un forte disincentivo all'investimento, evidenziando la necessità di interventi regolatori.

…cybersecurity e smart grids

Nonostante l'attività di Essence sia focalizzata sui segmenti di generazione e trasmissione, i risultati mostrano alcuni punti che si rivelano calzanti e che meritano approfondimento anche rispetto al comparto della distribuzione.

- La presenza di vulnerabilità andrebbe valutata anche nell'ambito della distribuzione, dove rischia di essere accentuata con il passaggio al modello delle smart-grid, per via della estrema interconnessione delle reti
- Gli incentivi di mercato sono spesso insufficienti a garantire investimenti efficienti e un livello di protezione opportuno
- Progettare un adeguato sistema di contromisure mentre viene creato il sistema smart è con tutta probabilità più efficace e anche meno costoso rispetto ad intervenire ex post.
- L'importanza di un'efficace attività di regolazione è evidente anche rispetto al tema della sicurezza, che va attentamente considerato nel momento in cui si approcci una prima regolamentazione delle smart grid.

All reports and other relevant references can be found at:

http://essence.ceris.cnr.it/

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs