



Consiglio Nazionale delle Ricerche



ISTITUTO di RICERCA sulla CRESCITA ECONOMICA SOSTENIBILE
RESEARCH INSTITUTE on SUSTAINABLE ECONOMIC GROWTH

Via Real Collegio, 30 – 10024 Moncalieri (TO) – Italia – Tel. 011-6824.911 – Fax 011-6824.966
C.F. 80054330586 – P.I. 02118311006 – segreteria@ircres.cnr.it – www.ircres.cnr.it

CNR-Ircres

NOTE sul doc. di consultazione 255/2015

A cura di E. Ragazzi (elena.ragazzi@ircres.cnr.it) e A. Stefanini (Alberto_stefanini@virgilio.it)

Nell'insieme si tratta di un documento abbastanza equilibrato, ed è importante che nel discorso complessivo abbia trovato posto anche il tema della cyber-sicurezza. Questo non è infatti un tema aggiuntivo, da trattare in modo separato, ma un elemento essenziale da considerare fin dall'inizio nella progettazione dei sistemi, nonché nei sistemi di regolamentazione che li controllano e/o incentivano.

Di seguito riportiamo una lista di osservazioni puntuali, che si concentrano sulla parte del documento dedicato alla sicurezza cibernetica (punti 5.19-5.26).

1. Forse si può obiettare che il punto sotto sembra sottovalutare in qualche modo il problema della sicurezza cibernetica. Questa non è una tematica che 'sta emergendo', se ne parla ormai da almeno 20 anni in relazione alla rete elettrica¹. Inoltre è un problema diffuso, i sistemi cibernetici sono sotto attacco continuo e le misure di sicurezza relative sono necessarie per garantire la resilienza delle smart grid e quella complessiva del sistema elettrico.
2. La formulazione del punto 5.21 in merito rafforza questa impressione. Si cita il doc. del governo americano sulla protezione del cyber space e la costituzione del Dip. per la Homeland security. Ma ci sono notizie più recenti e concrete che si riferiscono al problema, ad esempio si può citare l'attacco informatico russo all'Estonia (maggio 2007, cfr http://www.corriere.it/Primo_Piano/Esteri/2007/05_Maggio/18/mosca.shtml?refresh_ce-cp) che ha bloccato per giorni quel paese, oppure l'attacco ai sistemi cibernetici dell'Iran tramite la diffusione di un virus (Giugno 2010 - <https://en.wikipedia.org/wiki/Stuxnet>). Questa 'prassi' è ormai un fattore diffuso nelle relazioni internazionali, le potenze (maggiori e minori) ne fanno uso costante. Si può presumere che stati canaglie e terroristi se ne occupino con solerzia.
3. Al punto 5.25 si nota che 'il monitoraggio delle attività delle imprese regolate ... potrebbe essere utile a promuovere le migliori pratiche'. ESSENCE ha promosso questa prassi per quanto concerne la rete di trasporto ed i maggiori stakeholder nel campo della generazione. Si può dire che siamo interessati a estendere questa consultazione agli attori

¹ Ricordo di essere stato invitato ad un workshop USA sul tema con partecipazione EU ancora sotto la presidenza Clinton, credo nel 1998.

nel campo delle smart grid, anche per capire se questa problematica può essere un ulteriore fattore limitante alla loro diffusione.

In generale, l'esperienza di Essence si è concentrata sui settori della trasmissione e della generazione, ma ha comunque portato a conclusioni che possono essere particolarmente illuminanti anche per il settore della distribuzione. Vale la pena richiamarli qui in breve, come spunto di discussione al documento esaminato:

- Esistono importanti vulnerabilità all'interno dei sistemi di controllo degli impianti di produzione e di trasmissione dell'elettricità. Come chiaramente dichiarato anche nel documento in esame, nell'ambito della distribuzione questa vulnerabilità non può che essere amplificata, per via dell'estrema interconnessione delle reti, e verrebbe ulteriormente moltiplicata con il passaggio al modello delle smart grid. Il progetto Essence ha mostrato con i suoi casi di studio che questo tipo di 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, così come descritte in numerosi standard e linee guida, implica un investimento notevole per l'impresa, investimento che è difficile preventivare (per esempio con l'adozione di parametri standard per stimare un costo in funzione di determinate variabili), ma che deve essere calcolato basandosi sul reale stato delle infrastrutture in esame. In tal senso, il campo delle smart grid, dove presumibilmente si darebbe luogo a nuovi investimenti, potrebbe risultare a volte facilitato, in quanto invece la messa in sicurezza e l'adeguamento ai requisiti previsti dagli standard di sistemi preesistenti può essere molto costosa e difficoltosa, soprattutto nel caso di architetture derivanti da stratificazioni successive e in quello di sistemi che non possono mai essere messi in stand-by.
- Il beneficio economico connesso alla protezione del sistema dal rischio di black-out è molto grande e decisamente superiore al seppur ingente 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, soprattutto in assenza di una chiara regolamentazione.

I risultati dettagliati a cui tali spunti fanno riferimento, così come la loro discussione sono presenti sul documento: Ragazzi E., García Gutiérrez F., (2014) **Trial evaluation: conclusive lessons from Essence case studies** Rapporto Tecnico Ceris N.57. http://essence.ceris.cnr.it/images/documenti/RT_57.pdf. Tutti i rapporti e il materiale informativo del progetto sono disponibili sul sito: <http://essence.ceris.cnr.it/>

In conclusione vale la pena ribadire che:

- Gli incentivi di mercato sono sicuramente insufficienti a garantire investimenti efficienti (5.24) e un livello di protezione opportuno
- Progettare un adeguato sistema di contromisure mentre viene creato il sistema smart è sicuramente più efficace e anche meno costoso rispetto ad intervenire ex post.

Occorre dunque perseverare nello sforzo di regolamentare anche il tema della sicurezza nel momento in cui si approci una prima regolamentazione delle smart grid.