



## Defending the European Energy Infrastructures

DEFENDER affronta le nuove sfide associate alla protezione proattiva e al rapido ripristino, dopo un attacco, dell'infrastruttura di rete di trasmissione e distribuzione elettrica, che è al centro di qualsiasi infrastruttura energetica critica (CEI), al fine di mitigare incidenti, attacchi fisici o informatici e, soprattutto, attacchi combinati di tipo cyber-fisico.

### SFIDE STRATEGICHE

DEFENDER protegge la legacy della CEI e progetta una nuova generazione di infrastruttura energetica critica europea più resiliente, in grado di ripararsi autonomamente e capace di:

- sopravvivere a incidenti e inconvenienti su larga scala di tipo cyber-fisico, sociale o di tipo combinato;
- garantire la continuità delle operazioni e contemporaneamente minimizzare gli effetti a catena nell'infrastruttura, nell'ambiente, per i cittadini vicini e per gli utenti finali dell'energia.

### VISION

DEFENDER adatta, integra, migliora, implementa e valida un gran numero di tecnologie diverse e progetti operativi, al fine di sviluppare un nuovo approccio per salvaguardare l'infrastruttura energetica critica europea esistente e futura dalle minacce cyber-fisico-sociali, grazie a:

- nuovi concetti protettivi per la valutazione del ciclo di vita, capacità di recupero e auto-guarigione grazie alla "security by design";
- ispezione avanzata delle intrusioni e sistemi di mitigazione degli incidenti;
- una cultura della sicurezza, in cui lo scambio di informazioni attendibili tra dipendenti qualificati e volontari completerà il ciclo di protezione, preservando la privacy dei cittadini coinvolti.

### PILOTI

I risultati di DEFENDER saranno validati grazie ad un simulatore capace di riprodurre in laboratorio l'attuale stato dell'arte dell'infrastruttura energetica critica (RWTH, Germania) e a 4 studi reali (Francia, Italia e Slovenia) per valutare, validare e dimostrare come e in che misura la soluzione di DEFENDER consenta un efficace approccio olistico alla sicurezza cyber-fisica nelle principali installazioni la cui CEI è costituita da impianti di generazione, rete di trasmissione, rete elettrica di distribuzione e prosumer industriale.

### APPROCCIO

Per realizzare la sua visione, DEFENDER implementa quattro strategie:

- Valutazione del rischio. Fornire agli stakeholder CEI una comprensione approfondita del loro attuale grado di sicurezza e consentire loro di valutare continuamente le minacce e le vulnerabilità in evoluzione, i rischi e le potenziali contromisure.
- Misure protettive. Saranno sviluppate nuove misure protettive (proattive) per ridurre i rischi del sistema (comprese vulnerabilità e minacce emergenti).
- Gestione degli incidenti. Quando le misure di protezione non vengono applicate o non riescono a prevenire l'incidente, le contromisure riducono al minimo l'impatto.
- Costruire una cultura della sicurezza. Analisi post-incidente e analisi forense consentono agli stakeholder CEI di imparare dall'incidente.

#### Project Coordinator:

Dr. **Massimo Bertoncini** - Engineering

#### More information at:

[www.defender-project.eu](http://www.defender-project.eu)

#### Contact:

[info@defender-project.eu](mailto:info@defender-project.eu)





## Defending the European Energy Infrastructures

### DEFENDER Workshop

La protezione dei dati personali nelle infrastrutture critiche  
*Esperienze dal progetto Europeo di Ricerca e Innovazione DEFENDER*

Roma, martedì 20 novembre 2018

Ore 9:30-17:00

E-Lex Studio Legale

Via dei Barbieri, 6

Roma - Italia

### Programma

Ore 9:30-9:40 : Benvenuto

*Avv. Adriana Peduto - E-Lex Studio Legale*

Ore 09:40-10:00 : Presentazione del progetto DEFENDER

*Ing. Giampaolo Fiorentino - Engineering Ingegneria Informatica*

Ore 10:00-10:30 : Analisi di un caso di studio di DEFENDER

*Ing. Marco Paulucci - ASM Terni*

Ore 10:30-11:00 : Il ruolo del fattore umano nella costruzione di una cultura della sicurezza

*D.ssa Isabella Corradini – Themis Research Centre*

Ore 11:00-11:30 : Coffee break

Ore 11:30-12:00 : Protezione delle infrastrutture critiche e conformità al GDPR: il principio dell'Accountability e la gestione dei rischi

*Dott. Luigi Carrozzi – Garante per la protezione dei dati personali*

Ore 12:00-12:25 : 5G Essence - Soluzioni innovative basate su 5G e MEC per sviluppare servizi "Mission-Critical"

*D.ssa Maria Rita Spada – Wind Tre*

Ore 12:25-12:50 : Success – Securing Critical Energy Infrastructures  
*Ing. Gianluca Lipari – RWTH (Aachen Germania)*

Ore 12: 50-13:15 : NRG5 - Il 5G al servizio delle infrastrutture energetiche: il caso NRG-5  
*Ing. Filippo Rebecchi – Thales (Francia)*

Ore 13:15-13:45 : Nuove tecnologie in uso alla Polizia di Stato  
*Dott. Alessandro Carini - Polizia di Stato*

Ore 13:45-15:00 : Light Lunch

Ore 15:00-16:30 : Tavola rotonda – Infrastrutture critiche e privacy: rimedi legali e soluzioni tecnologiche

*Avv. Federica Resta - Garante per la protezione dei dati personali*

*Avv. Francesco Pergolini – Vodafone*

*Ing. Dorotea Alessandra De Marco - Garante per la protezione dei dati personali*

*Dott. Raffaella D'Alessandro – IBM*

*Dott. Fabio Lazzini - SOGEI*

*Moderatore Prof. Avv. Giovanni Maria Riccio - E-Lex Studio Legale*

**Conclusioni:** On. Angelo Tofalo, Sottosegretario di Stato alla Difesa

email [posta@e-lex.it](mailto:posta@e-lex.it) tel. 06 8775 0524