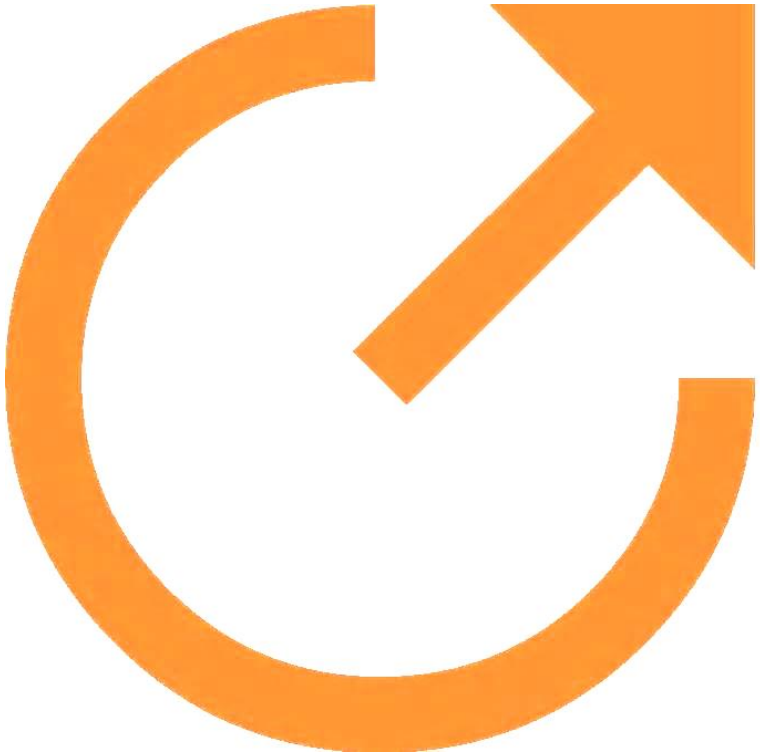
NORMA TECNICA

ENR 11001
NOVEMBRE 2012

Protezione delle Infrastrutture Critiche da Attacchi Terroristici
Requisiti Minimi



G. Lorusso e A. Ferraro – Ente Nazionale di Ricerca per la certificazione e la standardizzazione –
Via F.sco Crispi, 248 - 90139 - Palermo (PA)

ENR
Ente Nazionale di Ricerca per la Certificazione e la Standardizzazione

Indice

Premessa

La presente norma è stata elaborata dall'ENR, nell'ambito del progetto di ricerca denominato "MAS", con la finalità di creare una norma tecnica per la certificazione della sicurezza delle Infrastrutture Critiche (di seguito IC) nei confronti di attacchi terroristici.

Le norme ENR sono revisionate, quando necessario, con la pubblicazione di nuove edizioni o di aggiornamenti.
E' importante pertanto che gli utilizzatori delle stesse si accertino di essere in possesso dell'ultima edizione e degli eventuali aggiornamenti.

La presente norma è stata redatta cercando di tenere in considerazione i punti di vista di tutte le parti interessate per rappresentare il reale stato dell'arte della materia.
Tuttavia chiunque ritenesse, a seguito dell'applicazione della presente norma, di poter fornire suggerimenti per un suo miglioramento o per un suo adeguamento ad uno stato dell'arte in evoluzione è pregato di inviare i propri contributi all'ENR, Ente Nazionale di Ricerca per la certificazione e la standardizzazione - Via Francesco Crispi 248 - 90139 – Palermo - Italia, che li terrà in considerazione per l'eventuale revisione della norma stessa.

INTRODUZIONE

Il proliferare di gruppi politici che adottano metodi violenti, di tipo terroristico, come strumento di lotta e il contemporaneo diffondersi di conoscenze, abilità e opportunità idonee a rendere tali forme di lotta politica particolarmente pericolose e foriere di danni gravissimi alle persone e alle proprietà hanno fatto sorgere la necessità di proteggere detti beni dalle minacce di tipo terroristico.

Tale necessità è acuita dalla dipendenza, per quanto attiene la vita di tutti i giorni di milioni di persone, dal funzionamento di alcune tipologie di infrastrutture critiche, in particolare quelle di trasporto di persone, merci, energia e dati, oltre che dai rischi legati al danneggiamento volontario di impianti caratterizzati da alti rischi di esercizio (petrolchimici, chimici, energetici, nucleari, etc.).

Lo scopo di questa norma è di ampliare i requisiti minimi prescritti dal Decreto Legislativo 11 Aprile 2011, n° 61 "Attuazione della d irettiva 2008/114/CE – recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione" entrando nel dettaglio dei requisiti tecnici minimi richiesti agli impianti industriali per assolvere lo scopo di aumentare la propria resistenza agli attacchi terroristici.

1. SCOPO E CAMPO DI APPLICAZIONE

La presente norma definisce i principi e specifica i requisiti che un'organizzazione di gestione di una Infrastruttura Critica deve considerare per raggiungere la certificazione della propria infrastruttura in linea con gli attuali requisiti richiesti dalla presente norma.
La tipologia dei requisiti di sistema oggetto della presente norma sono solo quelli ritenuti dall'ENR come fondamentali per un moderno standard di certificazione e non altrimenti specificati. Non si esclude peraltro la possibilità che i requisiti di seguito riportati possano essere integrati da altre di enti statuali, intergovernativi, internazionali o non-governativi che, così facendo, intendano mettere in evidenza particolari caratteristiche di sistemi, tecnologie o tecniche ritenute utili o anche solo maggiormente idonee ad affrontare meglio tutte o talune specifiche minacce.

2. TERMINI E DEFINIZIONI

a) **infrastruttura**: un elemento, un sistema o parte di questo, che contribuisce al mantenimento delle funzioni della società, della salute, della sicurezza e del benessere economico e sociale della popolazione;
b) **infrastruttura critica (IC)**: infrastruttura, ubicata in uno Stato membro dell'Unione europea, che e' essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in quello Stato, a causa dell'impossibilita' di mantenere tali funzioni;
c) **settore**: campo di attività omogenee, per materia, nel quale operano le infrastrutture, che può essere ulteriormente diviso in sottosettori;
d) **intersettoriale**: che riguarda due o più settori o sotto-settori;
e) **infrastruttura critica europea (ICE)**: infrastruttura critica ubicata negli Stati membri dell'UE il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri. La rilevanza di tale impatto e' valutata in termini intersettoriali. Sono compresi gli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture;
f) **effetti negativi esterni**: effetti negativi dovuti alla perdita di funzionalità di un'infrastruttura e di erogazione del relativo bene o servizio;
g) **effetti negativi intrinseci**: effetti negativi che, l'eventuale danneggiamento o distruzione di un'infrastruttura, produce nei confronti dell'infrastruttura stessa e dell'ambiente circostante;
h) **criterio di valutazione settoriale**: percentuale dei fruitori del bene o servizio che l'infrastruttura eroga, rispetto alla popolazione nazionale o di altro Stato membro oppure a quella di una parte di territorio dell'Unione europea;
i) **criteri di valutazione intersettoriale**: elementi per la valutazione degli effetti negativi esterni e degli effetti negativi intrinseci sul mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione;
j) **proprietario dell'infrastruttura**: soggetto pubblico o privato che ha la proprietà di un'infrastruttura;
k) **operatore dell'infrastruttura**: soggetto pubblico o privato responsabile del funzionamento di una infrastruttura;
l) **informazioni sensibili relative alle IC**: dati e notizie, relative alle IC, che, se divulgati, potrebbero essere usati per pianificare ed eseguire azioni volte al danneggiamento o alla distruzione di tali infrastrutture;
m) **analisi dei rischi**: valutazione della vulnerabilità di una ICE rispetto alle diverse possibili minacce e prevedibili conseguenze del danneggiamento o distruzione della stessa, in termini di effetti negativi esterni e intrinseci;
n) **protezione**: attività per assicurar funzionalità, continuità ed integrità di una ICE o ridurne, comunque, le possibilità di danneggiamento o distruzione;
o) **Piano di Sicurezza dell'Operatore (PSO)**: Piano dettagliato, predisposto secondo metodologie standardizzate, volto ad individuare le vulnerabilità dell'Infrastruttura Critica e a definirne le modalità di protezione;
p) **Organizzazione per la sicurezza dell'infrastruttura**: struttura aziendale con il compito di mantenere l'esercizio in sicurezza dell'Infrastruttura Critica e gestire la prima risposta in caso di attentati;
q) **funzionario alla sicurezza**: responsabile della struttura di cui al punto p;
r) **unzionario di collegamento in materia di sicurezza**: funzionario incaricato dal gestore della Infrastruttura Critica a mantenere i contatti con la Prefettura competente per territorio. Coincide col funzionario di cui al punto q.

3. DESCRIZIONE DELLA MINACCIA

I rischi correlati agli atti di terrorismo portati contro le infrastrutture critiche dipendono dalla probabilità che essi avvengano posti in atto, dalla tolleranza ai danni degli obiettivi e dalle misure di protezione adottate.

La protezione dai rischi derivanti da azioni di terrorismo si può suddividere in tre fasi, ovvero:
1. Previsione;

2. Prevenzione;
3. Protezione.

La **previsione** è relativa all'individuazione dei bersagli e alle modalità di attacco, ed è responsabilità prevalente delle Forze dell'Ordine e dei Servizi di Sicurezza.

La **prevenzione**, espressa analogamente alla normativa di safety, prevede attività volte a individuare e riconoscere l'attacco mentre esso viene portato o nei momenti immediatamente precedenti e le misure tecniche, costruttive o organizzative messe in atto per minimizzare l'effetto degli attacchi portati a termine contro le infrastrutture critiche.

La **protezione**, nuovamente espressa in analogia alla normativa di safety, concerne la minimizzazione delle conseguenze dell'attacco, quando quest'ultimo ormai è stato messo in esecuzione.

3.1 PREVISIONE DELLA MINACCIA

Gli atti di terrorismo sono portati normalmente da piccoli gruppi di militanti politici, molto motivati e le cui logiche sono prevalentemente autoreferenziali, che individuano i possibili bersagli delle proprie azioni sulla base, fondamentalmente, di considerazioni sulle conseguenze del gesto in se, con riguardo alla propria causa e all'esposizione mediatica.

Le infrastrutture bersaglio, quindi, sono caratterizzate dall'avere grande visibilità (mediatica, ma non esclusivamente, anche impianti particolarmente grandi o classificabili come pericolosi) e da bassa o nulla protezione.

Poiché la scoperta delle intenzioni di questi gruppi è un compito complesso, che ricade nell'esclusiva responsabilità delle forze dell'ordine, il Gestore dell'Infrastruttura Critica nominerà un funzionario responsabile per mantenere il collegamento con i funzionari incaricati della Prefettura competente e del Dipartimento della Protezione Civile al fine di prevedere le probabilità che attacchi possano essere portati contro di essa.

3.2 PREVEVENZIONE DELLA MINACCIA

La **prevenzione**, espressa analogamente alla normativa di safety, prevede attività volte a individuare e riconoscere l'attacco mentre esso è portato o nei momenti immediatamente precedenti e le misure tecniche, costruttive o organizzative messe in atto per minimizzare l'effetto degli attacchi portati a termine contro le infrastrutture critiche.

Poiché ogni ECI è contraddistinta dai propri rischi peculiari, un'analisi dei rischi dovrà essere portata a termine da personale qualificato, allo scopo di individuare le criticità e redarre il piano di sicurezza dell'infrastruttura.

La suddetta analisi dei rischi dovrà considerare, come minimo, i seguenti tipi di attacco:

1. Attacco con camion bomba contenente 4.500 kg di TNT equivalente;
2. Attacco di sabotatori armati di razzi (gittata 100 m);
3. Attacco di barchino contenenti 900 kg di TNT equivalente con velocità di 30 nodi, se applicabile;
4. Attacco di sabotatori con razzi su barchino con velocità di 30 nodi, se applicabile;
5. Attacco di sommozzatori con due cariche esplosive da 1,5 kg di TNT equivalente, se applicabile;
6. Attacco con picchiata di Jet a Medio raggio (Boeing 737/ Airbus 320 o equivalente) con l'85% di carburante;
7. Attacco con picchiata di velivolo da aviazione generale (Cessna 172 o equivalente) con l'85% di carburante.

3.3 PROTEZIONE DALLA MINACCIA

La **protezione**, nuovamente espressa in analogia alla normativa di safety, concerne la minimizzazione delle conseguenze dell'attacco, quando quest'ultimo ormai è stato messo in esecuzione.

Per ogni minaccia individuata, dovrà essere preparata una procedura di reazione, assegnata alla responsabilità e supervisione di un'unità organizzativa dedicata, che ne verificherà l'efficacia attraverso esercitazioni periodiche, ne analizzerà i risultati e ne valuterà eventuali modifiche.

4. REQUISITI MINIMI

La protezione di una ECI impone l'applicazione di numerosi requisiti, suddivisi fra quelli richiesti a tutto il sistema e quelli richiesti ai singoli componenti.

4.1 REQUISITI DI SISTEMA

Il Gestore della ECI da certificare dovrà predisporre un Piano di Sicurezza dell'Operatore (PSO), composto dai seguenti documenti:

1. Uno studio d'impianto, per individuare le parti o gli elementi dello stesso maggiormente soggette a rischi di attacco terroristico, con particolare riferimento alle sezioni dell'ECI caratterizzate dal maggior contenuto energetico, dal maggior affollamento e/o dalla maggior presenza di sostanze pericolose.
2. Un'analisi dei rischi al fine di individuare individualmente e univocamente le vulnerabilità, ipotizzando l'attacco contro ognuna delle parti maggiormente a rischio di cui al punto precedente con le metodologie indicate al paragrafo 3.2. Sulla base della stima dell'equivalente in TNT del singolo caso (somma del metodo di attacco più il rischio presente), si valuterà l'impatto dell'attacco

stesso. Nell'eventualità della presenza di sostanze pericolose, si stimeranno, sulla base delle condizioni meteorologiche e ambientali prevalenti, l'ampiezza delle aree soggette a contaminazione;

3. Uno studio per l'individuazione, la selezione e la prioritarizzazione delle contromisure, di tipo fisico, di sorveglianza e delle procedure di blocco impianto, messa in sicurezza e pronto intervento, distinguendo fra misure permanenti e misure graduali, da adottare all'occorrenza.
4. Predisporre un'organizzazione per la sicurezza dell'infrastruttura, responsabile della sorveglianza nei confronti delle minacce e della reazione alle stesse qualora avvengano il cui responsabile sarà anche il funzionario incaricato quale punto di contatto con la Prefettura e la Protezione Civile.

4.2 REQUISITI DEI PRODOTTI E DEI SOTTOSISTEMI IMPIEGATI

Tutti i componenti hardware e software impiegati nel sistema di sicurezza della ECI dovranno:

1. essere selezionati in base alle risultanze dell'analisi dei rischi di cui al paragrafo 4.1;
2. avere prestazioni tali da garantire la scoperta della minaccia nelle condizioni ambientali d'impiego (rumore, traffico, meteo, etc.);
3. essere idonei all'impiego nelle condizioni ambientali previste (ambiente marino, climi rigidi, caldi, etc.);
4. essere dotati di doppia alimentazione (normale e di emergenza);
5. disporre di linee di trasmissione dati schermate e non disperdenti i segnali nell'ambiente esterno;
6. essere certificati secondo standard CE, UNI, RINA o equivalenti;
7. essere corredati di tutta la documentazione tecnica di uso e manutenzione, con particolare riguardo alle specifiche dei pezzi di rispetto, alle interfacce hardware e software e alle procedure di manutenzione.

4.3 VERIFICHE, PROVE E COLLAUDI

Il sistema di sicurezza, progettato sulla scorta degli studi di cui al paragrafo 4.1, sarà sottoposto a collaudo, attraverso l'esecuzione simulata di eventi terroristici, in tutti i suoi aspetti, ovvero rilevazione, reazione, contenimento con l'obbiettivo di porre l'ECI nello stato di minore vulnerabilità nel tempo disponibile dalla rilevazione della minaccia al raggiungimento da parte dell'incursione del proprio obbiettivo.
La simulazione dell'attacco con velivolo di linea a medio raggio, per evidenti difficoltà organizzative, sarà ritenuta soddisfacentemente verificata qualora portata a termine con il velivolo da aviazione generale.

5. GESTIONE DELLA DOCUMENTAZIONE

Tutti i documenti tecnici, gli studi, le analisi, le procedure, le registrazioni degli accessi alle aree sensibili della ECI, l'esito delle esercitazioni e delle attivazioni, sia dovute a cause inesistenti che reali ma non tali da mettere a repentaglio la sicurezza della ECI devono essere esaminate, classificate per segretezza secondo la normativa vigente, raccolte e archiviate in maniera riservata, aggiornata, revisionata, datata, leggibile e facilmente disponibile a chi potrebbe aver bisogno di consultarle.
L'UO responsabile della sicurezza dell'ECI comunica alle competenti autorità la liste delle persone a cui è necessaria concedere il "nulla Osta Sicurezza" per avere l'accesso alle informazioni classificate con classifica superiore a "riservato", per gli adempimenti di competenza.
In generale, la documentazione utile ai fini della sicurezza dovrà essere conservata per i seguenti periodi, fatte salve disposizioni diverse e più restrittive:

1. **fino alla dismissione dell'impianto**: disegni e informazioni progettuali dell'ECI e del sistema di sicurezza, PSO e documenti correlati, fra cui analisi dei rischi, analisi delle contromisure, procedure, nonché le relative modifiche/aggiornamenti, tutte le informazioni relative ad attivazioni reali pregresse del sistema e, in generale, tutte le informazioni su interventi caratterizzati da permanenza dell'effetto.
2. **5 anni:** Manutenzioni straordinarie, ivi comprese i dati dei ricambi utilizzati, rapporti delle esercitazioni di ECI e delle attivazioni non reali (falsi positivi) e, in generale, tutti quegli interventi caratterizzati da lunghi intervalli fra le loro ripetizioni non superiori comunque a 2,5 anni;
3. **2 anni:** manutenzioni ordinarie, ivi comprese i dati dei ricambi utilizzati, gli audit interni del sistema, i rapporti delle esercitazioni di reparto della ECI e, in generale, tutti quegli interventi caratterizzati da intervalli intermedi fra le loro ripetizioni non superiori comunque ad 1 anno.
4. **2 mesi:** registrazione degli accessi alle aree sensibili della ECI, registrazione dei sistemi di sorveglianza nei momenti in cui non siano state rilevate attività anormali, piccola manutenzione e in generale tutte le informazioni su attività a carattere quotidiano.

Le suddette registrazioni potranno essere mantenute in formato analogico o digitale. In entrambi i casi dovrà essere assicurata la conservazione degli archivi in una posizione sicura e poco esposta ai rischi connessi con la ECI e accessibile, in emergenza, anche remotamente tramite accesso sicuro e protetto agli enti e persone autorizzati.

6. FORMAZIONE ADDESTRAMENTO

Il responsabile della UO responsabile della sicurezza dell'ECI dovrà essere selezionato, assunto e qualificato

secondo gli standard approvati dalle Autorità competenti, agirà come punto di contatto con le Autorià competenti per territorio e sarà responsabile del buon funzionamento del servizio di allerta e delle procedure di emergenza in caso di attentato, avere una formazione tecnica di base e formazione specialistica aggiuntiva sulla ECI specifica e sulle tecniche di protezione da attacchi terroristici.
Gli addetti assegnati alla UO responsabile della sicurezza dell'ECI dovranno essere qualificati secondo gli standard approvati dalle Autorità competenti per territorio e a avere una formazione di base sulla ECI specifica e sulle tecniche di protezione da attacchi terroristici.
I dipendenti dell'Ente gestore la ECI dovranno ricevere un addestramento per fronteggiare le emergenze come previsto dalle procedure in vigore che dovrà essere verificato e riesaminato periodicamente.

7. VERIFICHE ISPETTIVE INTERNE

Il gestore della ECI dovrà, con frequenza minima annuale, effettuare una verifica ispettiva interna volta a verificare il soddisfacimento di tutti i requisiti della presente norma.
Le registrazioni di tali audit devono essere adeguatamente conservate per almeno 2 anni.

8. GESTIONE DELLE NON CONFORMITÀ, AZIONI CORRETTIVE, PREVENTIVE E DI MIGLIORAMENTO CONTINUO

L'organizzazione deve stabilire, attuare e mantenere attiva una procedura per trattare eventuali non conformità reali o potenziali e per intraprendere azioni correttive e azioni preventive. La procedura deve definire i requisiti per:

1. identificare e correggere le non conformità;
2. gestire eventuali falsi positivi o falsi negativi;
3. esaminare l'esito delle esercitazioni per determinare la necessità di modifiche alle procedure e/o all'addestramento degli addetti;
4. esaminare le non conformità, determinare la/e causa/e e intraprenderne azioni al fine di impedirne il ripetersi;
5. riesaminare l'efficacia delle azioni correttive e delle azioni preventive intraprese;
6. Rivedere periodicamente, con cadenza almeno annuale, in maniera critica il sistema per individuare possibili miglioramenti che possono essere perseguiti.