Metodologia della Sicurezza Nucleare

Pasquale Avino*, Piero Quercia**, Giuseppe Quartieri***

**DIPIA-ISPESL, Roma*
***INFN-LNF, Frascati, Roma*
****Libera Università L.U.de.S., Lugano*

I metodi e gli strumenti di analisi di sicurezza e del rischio che normalmente vengono impiegati nella progettazione dei sistemi complessi, quali le centrali nucleari, hanno concesso di definire i salti di qualità che si riscontrano nel passaggio dalla terza generazione avanzata alla quarta generazione che dovrebbe includere, entro 30 anni, la sicurezza totale intrinseca delle centrali nucleari

Nuclear Security Methodologies

The methods and instruments for security and risk analysis typically used in the design of complex systems like nuclear power plants allow to define the quality upgrades from the advanced generation III to generation IV reactors. Indeed, in 30 years such upgrades are expected to include the full 100% level of nuclear power plants' intrinsic security

La distribuzione energetica italiana ed europea, partendo dall'obiettivo 20/20/20 (che sintetizza: a) impegno dell'UE per una riduzione delle emissioni di gas serra al minimo del 20% nel 2020 rispetto ai livelli del 1990; b) aumento dell'efficienza energetica allo scopo di ridurre del 20% il consumo rispetto alle proiezioni per l'anno 2020; c) obbligo di impiego di una percentuale del 20% di fonti rinnovabili sul consumo energetico complessivo e di un minimo del 10% di biocarburanti sul consumo complessivo dei carburanti destinati al settore dei trasporti), si è risolto nella proposta di ripartizione di fonti energetiche nel 25% carbone, 25% petrolio (con l'enorme variabilità dei prezzi) e gas, 25% nucleare e 25% fonti integrative (solare, eolico, geotermico ecc.). In questo contesto, è stato varato il piano energia nucleare, dove i principali problemi riguardano:

1. la decisione della localizzazione dei siti, demandata ad un processo di scelta basato sulla mappa di 10 siti prescelti già negli anni '70, supportato da opportune analisi geotecniche (ex art. 25 Legge 99/2009);
2. la sicurezza nucleare, ottimizzata con la scelta della filiera EPR di terza generazione avanzata;
3. la gestione delle scorie radioattive, con accordi internazionali ed europei sotto la vigilanza di enti quali l'International Atomic Energy Agency (IAEA) ecc.

È sufficientemente noto che il passaggio dalla terza generazione avanzata (con i suoi fondamentali improvements progettuali e tecnologici rispetto alla seconda generazione) alla quarta generazione richiederà al minimo trenta anni, con forti implicazioni di ricerca scientifica e tecnologica che avrà come fulcro la ricerca della conoscenza della nuova fisica dei reattori di quarta generazione e delle applicazioni per la realizzazione della sicurezza intrinseca.

Altri rischi residui fondamentali che sono alla base della scelta di investire nel nucleare sono proposti dalla maggiore parte degli analisti, come il fatto che è più pericoloso l'inquinamento da CO_2, con conseguente effetto serra, dello stoccaggio di scorie nucleari in sedi geologiche appropriate, e dopo che le scorie siano state declassate con irraggiamento neutronico. L'analisi parte dal presupposto che il rischio nucleare è preferibile alla certezza della insostenibilità dell'effetto serra. In questa sede non si vuole sindacare sul valore di questa affermazione, ma si vogliono gettare le basi per un discorso più ampio, anche tenendo conto della problematica sopra riportata che non deve essere trascurata. Del resto, a fronte della maggiore pericolosità dell'inquinamento da CO_2, i risultati delle analisi dei rischi nucleari eseguite in tutto il mondo hanno condotto agli stessi risultati condivisi: il rischio da centrale nucleare più importante è lo stoccaggio di scorie nucleari. Questo è il tipo di rischio più individuato dai maggiori istituti e/o istituzioni di ricerca in campo nucleare internazionali, come IAEA, DoE, MoD, MIT, Max Planck Geselleshaft, o italiani, come ENEA, ISPRA, APAT ecc.

Sembra che recentemente la Svezia abbia offerto, o proposto all'Europa, almeno due siti geologici per il deposito di scorie radioattive "dure" (di vita media di migliaia di anni). Questo è in coerenza con il fatto che l'energia elettrica da nucleare è "sistema" (come definito dalla stessa Unione Europea) che può e deve essere gestito in modo comunitario. Inoltre, da più parti si parla di progettare e realizzare nuovi impianti di irraggiamento delle scorie dure con fasci di neutroni per spezzarli e farli diventare elementi a vita media bassa o accettabile (progetto innovativo, per qualche verso similare a quello di Rubbia, in parte realizzato nei pressi di Padova).

In ogni caso la via dell'irraggiamento delle scorie dure con fasci di neutroni deve essere comunque seguita.

Quindi l'impiego dell'energia nucleare è sicuro ed in parte anche rinnovabile in termini artificiali e non naturali. Così il problema di rischio residuo è connesso, solo e soltanto, alla gestione dei rifiuti radioattivi. I ricercatori stanno affrontando questo problema con molti metodi, primo fra tutti quello dell'innesco di reazioni nucleari mediante irraggiamento di neutroni che impongono la scissione delle scorie

radioattive con forte diminuzione della vita media di radioattività. Questo processo può essere ripetuto più volte sino a raggiungere isotopi materiali con vita media e intensità di emissione residua estremamente bassa e completamente accettabile.

L'analisi teorica di sicurezza

I rischi nucleari fondamentali normalmente analizzati sono:

1. la localizzazione della centrale nucleare (rischio geotecnico, geologico, di tipo statico legato all'instabilità del suolo, terremoti, sabotaggi, terrorismo ecc.);
2. la radioattività ambientale esterna alla centrale stessa con conseguente incremento di inquinamento radioattivo ambientale.

Ambedue questi rischi sono stati valutati a fondo dalle agenzie responsabili. Il controllo della radioattività ambientale è stato affidato a diversi specialisti (esperti qualificati), mentre i rischi di localizzazione sono in analisi e sotto controllo. In questa visione panoramica dei rischi residui, si ritiene che la soluzione nucleare sia, nel lungo termine, interessante e concorrente rispetto all'inquinamento da CO_2 e alla conseguente certezza della non sostenibilità dell'effetto serra.
Da diversi anni sono allo studio due proposte per la riduzione del rischio prodotto dalle scorie nucleari:

1. l'impiego del bio-sensore *Ralstonia detusculanense* (RDT®), batterio estremofilo per la rilevazione e cattura di radioattività nelle piscine radioattive annesse ai reattori nucleari;
2. il progetto di "Smaltimento delle scorie radioattive, non riciclabili in reattori di quarta generazione, con la raccolta delle stesse in appositi depositi di navicelle spaziali a bordo di missili lanciati al di là della biosfera nello spazio solare profondo in direzione del Sole". Quest'ultimo progetto consente di soddisfare anche alcuni requisiti economici, quali:
   - un minore impatto sull'ecologia e quindi un beneficio sull'ambiente;
   - la richiesta industriale nel campo dell'aeronautica e aviazione.

L'attuazione di questi programmi di ricerca impone l'applicazione della metodologia (sia classica che avanzata) dell'analisi e previsione della sicurezza e l'esenzione da rischi inaccettabili, supportata dall'analisi dei rischi e del piano di sicurezza di grandi sistemi complessi artefatti, ma anche dalle analisi LLE=RAV di Riduzione della Aspettativa di Vita. Normalmente, l'analisi di sicurezza classica presenta due aspetti fondamentali:

1. l'analisi dei rischi classici del 'sistema impianto nucleare', basata sul *Design Control Document*: ALARA, *Deep Safety*, Semplificazione, *Core Damage Frequency* (CDF), sottosistemi passivi di sicurezza (*safety related*), diversificazione della funzioni di sicurezza ecc.;
2. le analisi di sicurezza degli effetti biologici della radiazione ionizzante.

In particolare, il progetto della sicurezza delle centrali nucleari (ossia di un tipico esempio di sistema complesso) viene eseguito con la metodologia dell'analisi e previsione di sicurezza di grandi sistemi complessi basata sul calcolo della *dependability*, ossia delle interfacce fra affidabilità, disponibilità e mantenibilità del sistema stesso. Le tecniche impiegate (FMEA, FMECA, FTA, CCA, HAZOP ecc.) anche per l'analisi dei rischi (*Tabella 1*) sono ormai standardizzate ed impiegate per ogni tipo di analisi di sicurezza, e quindi anche per l'analisi dei rischi dei reattori nucleari della terza generazione e della prossima quarta generazione, cosiddetta a sicurezza intrinseca.
L'applicazione della moderna teoria dell'organizzazione al sistema di sicurezza delle centrali

Tabella 1 - Ciclo del rischio

1	Identificare gli azzardi
2	Stimare e valutare i rischi
3	Analizzare il controllo e le misure del rischio
4	Prendere le decisioni di controllo (del rischio)
5	Realizzare i controlli (mitigazione ecc.) di rischio
6	Supervisionare, ispezionare e revisionare tutto

Fonte: Institute for Basic Research (IBR), Palm Harbour, Florida, USA

nucleari permette quindi di individuare immediatamente i seguenti fattori organizzativi cardine e non necessariamente esaustivi quali:

- la posizione del responsabile del sotto-sistema di sicurezza delle centrali nucleari nell'organizzazione della sicurezza nucleare in generale;
- la necessità di distribuzione e disseminazione di informazioni concernenti la sicurezza delle centrali nucleari a tutte le parti interessate interne alle aziende di gestione operativa (controllori, operatori ecc.) e a tutte le parti esterne al sistema (clienti e utenti del servizio di utenza di energia elettrica);
- la necessità di impiego di personale competente, consapevole e ben formato (punto delicato e nevralgico al tempo stesso);
- la garanzia e la certificazione di qualità di sicurezza delle singole centrali nucleari;
- la manutenzione per la sicurezza delle centrali nucleari;
- la gestione delle scorie radioattive.

In letteratura, si trovano diversi approcci alla gestione della sicurezza delle centrali nucleari. La *figura 1* riporta il flusso di analisi decisionale dell'analisi di sicurezza di un sistema complesso. Lo sviluppo del flusso di analisi è basilare per l'esecuzione di un piano di sicurezza di un sistema

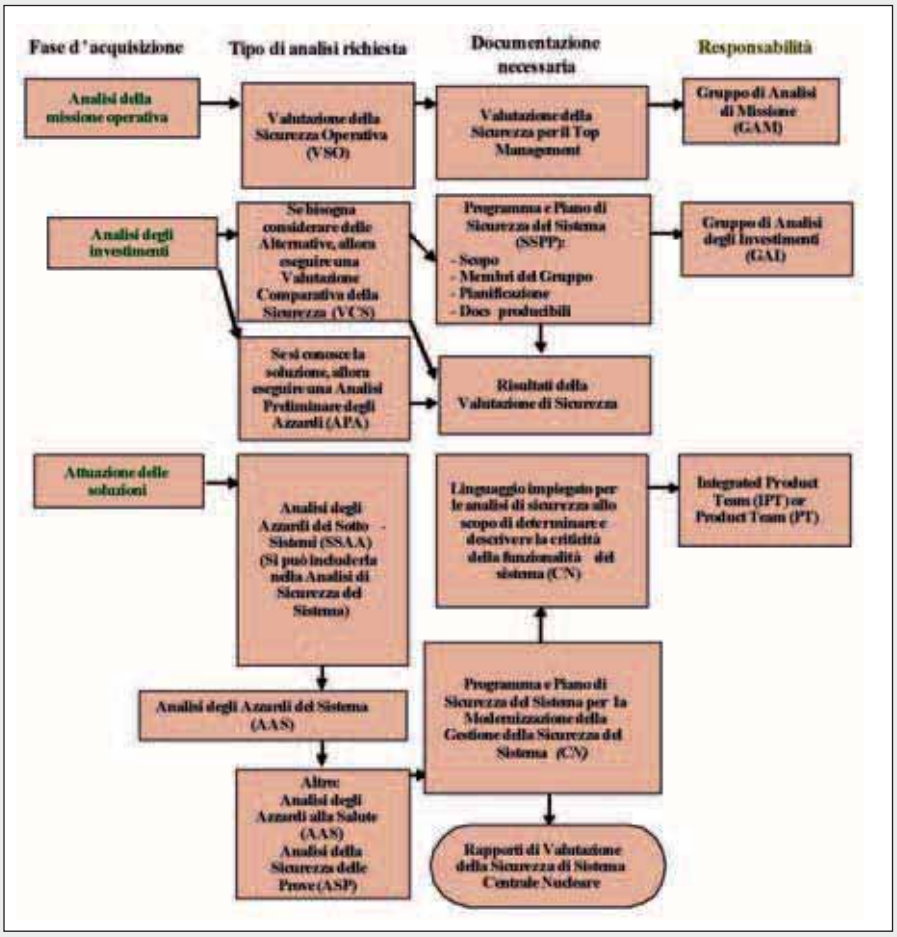

Figura 1
Flusso del processo decisionale dell'analisi di sicurezza del sistema
Fonte: Institute for Basic Research (IBR), Palm Harbour, Florida, USA

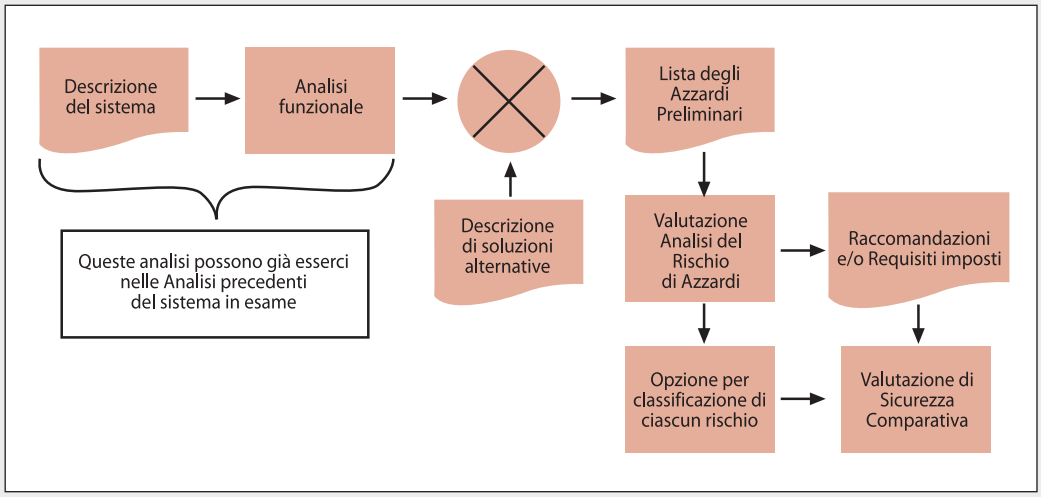

Figura 2
Analisi di sicurezza comparativa
Fonte: Institute for Basic Research (IBR), Palm Harbour, Florida, USA

complesso come quello di una centrale nucleare. Effettivamente, le differenze organizzative sono molto poche, ad esempio fra l'approccio americano e quello europeo. Negli Stati Uniti si usa applicare un approccio di gestione a gruppo degli aspetti di sicurezza delle centrali nucleari. L'analisi tenta di presentare una classificazione più completa anche se non proprio esaustiva dell'approccio generale come è descritto nella *figura 2* sull'analisi comparativa di varie alternative.
In questa parte dell'analisi si tratterà soprattutto di questi tre aspetti della sicurezza della centrale nucleare, con particolare riguardo ai casi di rottura di sottosistemi, apparati e/o dispositivi che conducono la centrale nucleare in condizioni tali da far verificare uno stato di guasto.
Recentemente, nel panorama della sicurezza delle centrali nucleari, alcune industrie multinazionali hanno coniato una nuova dizione per indicare l'approccio sistemico, ossia "Strategia Globale per la Sicurezza delle Centrali Nucleari" (*Global Safety Strategy*). Aldilà dell'autore della dizione, quello che interessa è vedere se funziona e, in ogni caso, riportarne il significato ed eventualmente condividerne i metodi, la tecnologia e la metodologia investigativa.

L'analisi dei rischi

Per procedere ad una sintetica esposizione dell'analisi e della gestione del rischio nella gestione della sicurezza di una centrale nucleare, si riportano brevemente le definizioni fondamentali di difetto, guasto, stato e modo di guasto e i diagrammi di base delle loro relazioni. In particolare, per interpretare questi fenomeni che controllano, regolano e soprassiedono alla sicurezza delle centrali nucleari e la condizionano pesantemente, bisogna procedere nella direzione indicata dalla moderna scienza della gestione manageriale dei grandi sistemi complessi di cui il sistema nucleare, ma anche aerospaziale, aeronautico e di aviazione sono casi eclatanti. Alcuni malfunzionamenti producono difetti e, a loro volta, alcuni di essi possono diventare dei guasti che propagandosi ad albero lungo il sistema possono raggiungere componenti, apparati e/o sottosistemi il cui guasto produce una situazione critica e/o catastrofica del sistema nucleare globale.
A seguito dell'analisi si produce un *safety case*, ossia un 'caso di sicurezza', ossia un corpo documentato di evidenze sostanziate che permette di

fornire argomenti convincenti e validi per dimostrare che il sistema in esame è adeguatamente sicuro per una data applicazione in un dato ambiente. La costruzione di un *safety case* (*figura 3*) è un compito difficile e complicato che consente di finalizzare la risoluzione di un problema di sicurezza basandosi su metodologie e teorie scientifiche, quali le buone pratiche di processi produttivi (SGQA, standard di progetto ecc.).

L'analisi dipende dai concetti e delle definizioni dei malfunzionamenti, dei difetti e dei relativi guasti. Ad esempio la *figura 4* serve a spiegare, in modo pratico e pittorico, la differenza fra errore umano e guasto di sistema provenienti da un ambiente software. Un *fault*, ossia uno stato di guasto, è generato da un errore umano nella produzione del software; un *fault* si può manifestare in un guasto.

A seconda della definizione impiegata si sviluppano diagrammi di flusso e di relazioni che possono variare di volta in volta. Tuttavia, l'analisi finale conduce sempre allo stesso risultato.

In generale, si sviluppano le relative procedure di analisi secondo la seguente linea guida:

- prima di tutto si chiarisce il concetto di 'rischio', gli sviluppi delle 'regolamentazioni', la terminologia dei rischi ed i processi di azzardo, e quindi le varie gestioni dei rischi;
- si passa poi alla descrizione di sistema e all'applicazione di una o di varie tecniche di 'analisi di affidabilità' (es. *Cause-Consequence Diagram*

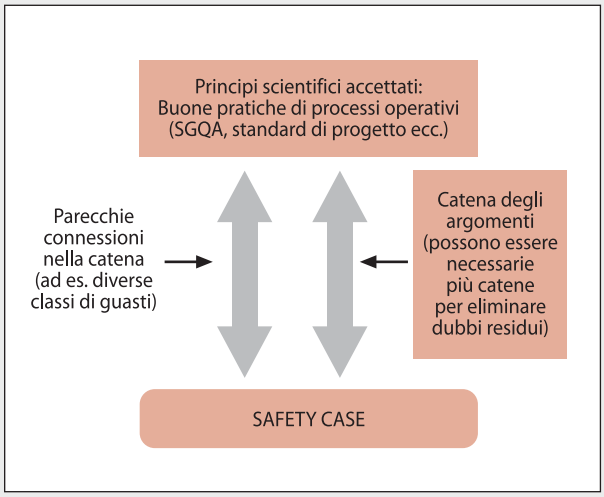

Figura 3
Argomenti per un safety case
Fonte: Institute for Basic Research (IBR), Palm Harbour, Florida, USA

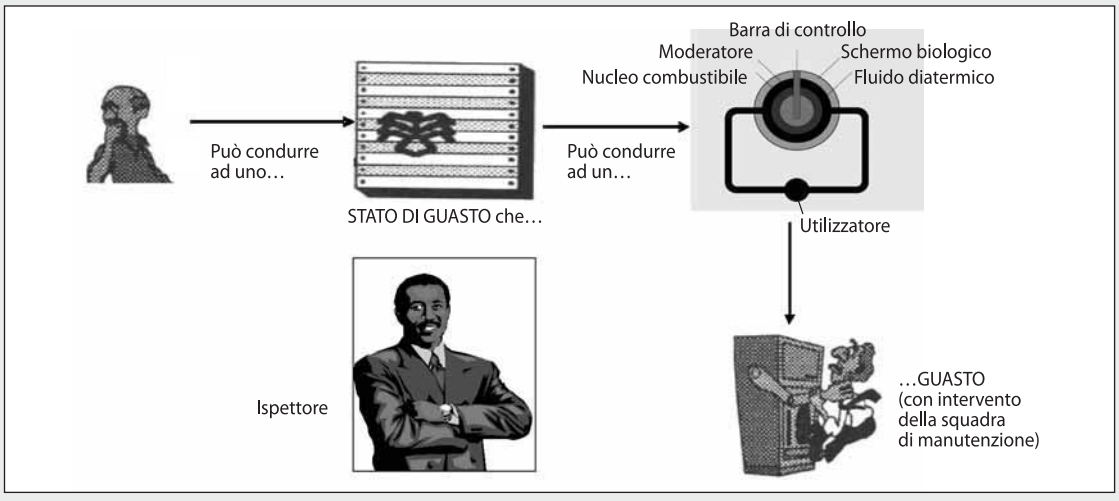

Figura 4
Relazione fra errore umano, stato di guasto e guasto
Fonte: Institute for Basic Research (IBR), Palm Harbour, Florida, USA

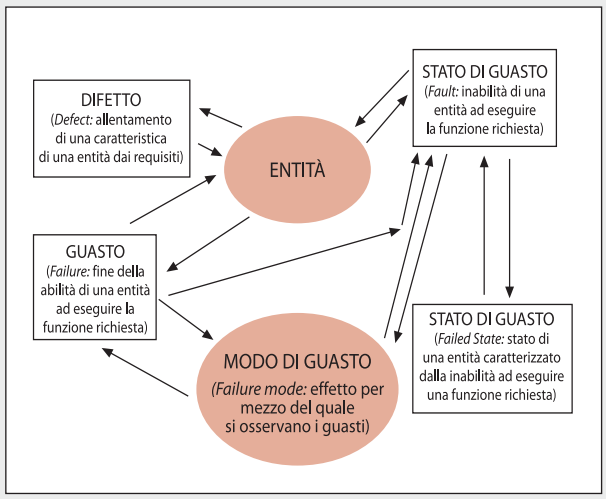

Figura 5
Relazione fra errore umano, stato di guasto e guasto
Fonte: Institute for Basic Research (IBR), Palm Harbour, Florida, USA

Method (CCDM), *Consequence Tree Method* (CQTM), *Cause Tree Method* (CTM), *Decision Table Method* (DTM), *Failure Mode and Effect Analysis* (FMEA), *Gathered Fault Combination Method* (GFCM)) per poi poter condurre 'analisi di sicurezza' (es. *Failure Mode Effect and Criticality Analysis* (FMECA), *Preliminary Hazard Analysis* (PHA), *Preliminary Hazard and Risk Analysis* (PHRA), *Probabilistic Risk Assessment* (PRA), *Probabilistic Safety Assessment* (PSA), *Success Diagram Method* (SDM), *State Space Method (SSM), Truth Table Method* (TTM)) e quindi finalmente passare alla 'analisi degli azzardi di processo' (AAPr=PrHA) sfruttando, tra l'altro, anche il metodo *Hazard and Operability Analysis* (HAZOP) (*figure 2, 5, 6*);

- quindi si passa alla convalida di procedure e risultati di PHA (AAP) e alla gestione delle modifiche (GM=MOC);
- è necessario elaborare metodi di stima degli ordini di grandezza del tempo necessario all'esecuzione di una AAPr (PrHA);
- si esegue l'analisi di gestione degli azzardi rispetto alle condizioni della struttura della centrale nucleare;
- le suddette analisi (AAPr ecc.) devono essere elaborate rispettando i protocolli e i regolamenti applicabili e le linee guida di salvaguardia per la sicurezza delle centrali nucleari;
- l'elaborazione quindi passa all'analisi dei fattori umani e alle sollecitazioni ambientali che possono aumentare la possibilità e il rischio di errore. Quando sono chiaramente noti questi fattori (specifiche tecniche dei fattori umani ed ergonometrici, specifica tecnica ambientale ecc.) si inizia l'analisi per la mitigazione e la minimizzazione dei potenziali errori umani ed ambientali;
- analisi degli azzardi comuni;
- esecuzione della gestione e giustificazione delle raccomandazioni che provengono dall'elaborazione dei risultati di AAPr (PrHA).

I risultati di queste analisi devono essere quindi integrati fra di loro e con altre analisi ed altri metodi di natura anche più generale, al fine di ottenere ed applicare la strategia globale su accennata.

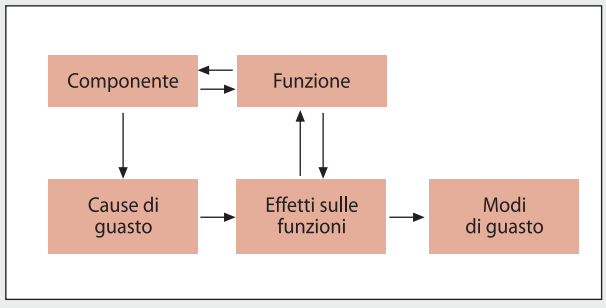

Figura 6
Schema di relazione fra componente, funzione e modi di guasto
Fonte: Institute for Basic Research (IBR), Palm Harbour, Florida, USA

Le regole fondamentali: aspetti operativi

L'approccio operativo per sistemi include tre aspetti fondamentali:

1. la sicurezza intrinseca delle centrali nucleari (ad es. gli apparati essenziali per la sicurezza operativa, i livelli di sicurezza intrinseci di progettazione meccanica, il livello di sopravvi-

venza all'impatto, i margini di sicurezza del progetto idrodinamico e del nocciolo ecc.). I fattori intrinseci includono la progettazione, lo sviluppo, la produzione e la qualificazione (prove funzionali, prove di volo, prove ambientali ecc.);

2. gli aspetti di controllo operativo esterni e correlati allo spazio esterno alla centrale nucleare tramite sistemi di comunicazione quali, ad esempio il Global Position System (GPS), l'EGPWS, per aspetti migliorati di allarme nelle vicinanze alla centrale nucleare, e il TCAS, per il controllo dell'approccio e della discesa di elicotteri di sicurezza;
3. la security di impianto, cioè la gestione manageriale dell'impianto e di tutti gli annessi e connessi, quali la gestione ed attuazione della manutenzione e della dependability in generale per l'efficienza di una centrale nucleare.

Conclusioni

In questa relazione sono riportati alcuni concetti fondamentali della teoria della sicurezza di sistemi complessi, ed in particolare di sistemi nucleari per la generazione di energia elettrica. Uno sguardo più attento, sebbene in forma sintetica, è stato dedicato alla metodologia dell'analisi dei rischi, dopo avere messo in evidenza la necessità di una riduzione dell'inquinamento da CO_2, e dunque l'esigenza di non affidare la produzione di energia elettrica solo a fonti di tipo fossile, affrontando, tra le nuove tecnologie alternative, un nuovo progetto nucleare.
In generale, i metodi teorici e le tecniche presentati hanno concesso di definire i salti di qualità che si riscontrano nel passaggio dalla terza generazione avanzata di centrali nucleari alla quarta generazione, che dovrebbe includere, entro 30 anni, la sicurezza totale intrinseca dell'intero sistema.

riflettore su

Bibliografia

- I. Bazovsky, Reliability, Theory and Practice, Prentice Hall, Englewood Cliffs, N.J. 1961.
- R.P. De Havilland, Introduction to the Theory of Reliability, General Electric Report 57 D 423, 1957, SAEP 343D.
- S. Garribba, S. Vacca, Il Controllo Sociale dell'energia nucleare in Italia, Franco Angeli Ed. 1978.
- M. Cumo, Impianti nucleari, UTET 1986.
- C. Dellarciprete, Criteri, studi e indagini per la localizzazione degli impianti nucleari, Elettronica, aprile 1982.
- G. Quartieri, On the component 'imp' in the system, Safety Analysis XXIX, Convegno Internazionale delle Comunicazioni 1981, Genova.
- H.W. Lewis, Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission, U.S.N.R.C. National Technical Information Service 1975.
- H.W. Lewis, La sicurezza dei reattori a fissione, Le Scienze, maggio 1980.
- US Nuclear Regulatory Commission, Safety Goal for Nuclear power plants: a proposed policy, 1983 NUREG, 0880, Rw. 1.
- A. Villemeur, Reliability, Availability, Maintainability and Safety Assessment, John Wiley & Sons, Chichester.