Agenzia Nazionale per le Nuove Tecnologie,
l'Energia e lo Sviluppo Economico Sostenibile

Ministero dello Sviluppo Economico

RICERCA DI SISTEMA ELETTRICO

Documento CERSE-UNIBO RL 1305/2010

Analisi delle Linee Guida IAEA ed NRC per la revisione dei rapporti di sicurezza

P. Vestrucci, G. Zappellini

Report RdS/2010/132

ANALISI DELLE LINEE GUIDA IAEA ED NRC PER LA REVISIONE DEI RAPPORTI DI SICUREZZA

P. Vestrucci, G. Zappellini

Settembre 2010

Report Ricerca di Sistema Elettrico
Accordo di Programma Ministero dello Sviluppo Economico – ENEA
Area: Produzione e fonti energetiche
Tema: Nuovo Nucleare da Fissione

Responsabile Tema: Stefano Monti, ENEA

CIRTEN

CONSORZIO INTERUNIVERSITARIO

PER LA RICERCA TECNOLOGICA NUCLEARE

UNIVERSITA' DI BOLOGNA

DIPARTIMENTO DI INGEGNERIA ENERGETICA, NUCLEARE E DEL CONTROLLO AMBIENTALE

Analisi delle Linee Guida IAEA ed NRC per l'Analisi dei Rapporti di Sicurezza

CIRTEN-UNIBO RL 1305/2010

AUTORI

P. Vestrucci
G. Zappellini

Bologna, Agosto 2010

Lavoro svolto in esecuzione della linea progettuale LP5 punto A1 - AdP ENEA MSE del 21/06/07
Tema 5.2.5.8 – "Nuovo Nucleare da Fissione".

INDICE

Abstract

Lo studio qui presentato è stato articolato in quattro sezioni.

Una prima sezione introduttiva (Capitolo 2) riassume il quadro generale dei Safety Standards quali strutturati nel Safety Assessment IAEA riferito agli impianti ed alle attività (Facilities and Activities) relativi al settore nucleare. Lo studio segue in particolare la Linea guida "IAEA Safety Standards - Safety Assessment for Facilities and Activities", No. GSR Part. 4 (rif.[1]), ove i Safety Standards vengono indicati e sinteticamente descritti con particolare riferimento ai Safety Fundamentals e Priciples (n° 10), ai Safety Requirements (n° 24) e alle Safety Guides, considerati come riferimento.

La seconda sezione (Capitolo 3) riprende nel dettaglio le linee guida sviluppate da IAEA ed OECD Nuclear Energy volte a fornire una documentazione regolamentare delle modalità di verifica del PSA. Tali studi sono stati articolati in quattro documenti, tre dei quali ripartiscono l'analisi in tre livelli successivi di verifica: IAEA-TECDOC-1135 (livello 1) (rif.[2]) che identifica le sequenze di eventi incidentali che possono portare al danneggiamento del core, senza valutare la capacità di contenimento; IAEA-TECDOC-1229 (livello 2) (rif.[3]) che identifica le cause e i percorsi attraverso i quali può essere perduto il contenimento con un rilascio radioattivo dall'impianto all'ambiente esterno e Safety Series No. 50-P-12 (livello 3) (rif.[5]) che stima le conseguenze sulla salute dell'uomo e sull'ambiente prodotte dal trasporto esterno dei materiali radioattivi.
Il quarto documento Safety Reports Series No. 25 di IAEA, OECD / NEA (rif.[6]) raccoglie l'intera analisi sviluppata dai documenti precedenti in un'unica linea di valutazione, ripartita secondo i tre livelli di cui sopra ma in grado di consentire una maggiore tracciabilità degli elementi analitici considerati. Per tali ragioni il presente studio fa particolare riferimento a questo ultimo elaborato IAEA, considerando il dettaglio delle vaie task e delle valutazioni di verifica introdotte.

La terza sezione (Capitolo 4) ripercorre sinteticamente il tracciato storico delle analisi e delle verifiche sviluppato in sede US-NRC, considerando come documentazione di riferimento il NUREG-1150 (rif.[9]), che riporta e confronta le analisi sviluppate su cinque diversi reattori nucleari. I contenuti di base rispettano i Principles e i Requirements IAEA e seguono le tematiche di analisi e le rispettive modellistiche con medesime tecniche e/o programmi di calcolo simili a quanto riportato nella Linea guida IAEA. Il presente studio si sofferma principalmente a considerare gli aspetti di dettaglio che presentano elementi aggiuntivi o differenziati, utili per una visione complessiva dei metodi di verifica e di analisi dei rapporti di sicurezza.

La quarta sezione (Capitolo 5) contiene spunti che, riprendendo elementi particolari dalle strutture e dai metodi presentati nelle tre sezioni precedenti, possano fornire utili riferimenti per la definizione di una Linea Guida Nazionale.

1 DOCUMENTI DI RIFERIMENTO E ACRONIMI

1.1 Documenti di riferimento

Rif.	Documento
[1]	IAEA Safety Standards - Safety Assessment for Facilities and Activities - No. GSR Part. 4 (Vienna 2009)
[2]	IAEA-TECDOC-1135, Regulatory review of probabilistic safety assessment (PSA) – Level 1 (February 2000)
[3]	IAEA-TECDOC-1229, Regulatory review of probabilistic safety assessment (PSA) – Level 2 (July 2001)
[4]	INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), Safety Series No. 50-P-8, IAEA,Vienna (1995).
[5]	INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), Safety Series No. 50-P-12, IAEA,Vienna (1996).
[6]	Safety Reports Series No. 25 – Review of Probabilistic Safety Assessment by Regulatory Bodies, Vienna (2001)
[7]	PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants (NUREG/CR-2300)
[8]	U.S Nuclear Regulatory Commission “Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants”, WASH-1400 (NUREG-75/014)”
[9]	U.S Nuclear Regulatory Commission (NRC), “Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants” , NUREG-1150
[10]	HANNAMAN, G.W., SPURGIN, A.J., Systematic Human Action Reliability Procedure (SHARP), Rep. EPRI-NP-3583, Electric Power Research Institute, Palo Alto, Ca (1984)

Rif.	Documento
[11]	SWAIN, A.D., GUTTMAN, H.E., Handbook of Human Reliability Analysis with Emphasis on Nuclear power plant Applications, Rep. NUREG/CR-1278, United States Nuclear regulatory Commission, Washington, DC (1983)
[12]	HEALTH AND SAFETY EXECUTIVE (HSE), The Use of Computers in Safety-critical Applications, Final report of a Study Group on the Safety of Operational Computer Systems, HSE Books, London (1998)
[13]	WENRA, Harmonization of Reactor Safety in WENRA Countries, Genuary 2006

1.2 Acronimi

BWR **B**oiling **W**ater **R**eactor

CDF **C**ore **D**amage **F**requency

CET **C**ontainment **E**vent **T**rees

ECCS **E**ngineering **C**ore **C**ooling **S**ystem

FCI **F**uel **C**oolant **I**onteraction

FMEA **F**ailure **M**ode and **E**ffects **A**nalysis

FSP **F**undamentals **S**afety **P**rinciples

HEP **H**uman **E**rror **P**robability

HR **H**uman **R**eliability

HRA **H**uman **R**eliability **A**ssessment

HAZOP **HAZ**ard and **OP**erability Analysis

IAEA **I**nternational **A**tomic **E**nergy **A**gency

LOCA **L**oss **O**f **C**oolant **A**ccident

LPIS	**L**ow **P**ressure **I**njection **S**ystem
NUSSC	**N**uclear **S**afety **S**tandards **C**ommittee
OECD	**O**rganization for **E**conomic **C**o-operation and **D**evelopment
POS	**P**lant **O**perating **S**tate
PDS	**P**lant **D**amage **S**tates
PRA	**P**robabilistic **R**isk **A**ssessment
PSA	**P**robabilistic **S**afety **A**ssessment
PWR	**P**ressurized **W**ater **R**eactor
QA	**Q**uality **A**ssurance
RASSC	Radiation Safety Standards Committee
RCS	**R**eactor **C**oolant **S**ystem
Req	**R**equirement
SA	**S**afety **A**ssessment
SGTR	**S**team **G**enerator **T**ube **R**upture
SHARP	**S**ystematic **H**uman **A**ction **R**eliability **P**rocedure
TRANSSC	**TRAN**sport **S**afety Standards **C**ommittee
WASSC	**WA**ste **S**afety Standards **C**ommittee
WENRA	**W**estern **E**uropean **N**uclear **R**egulators'**A**ssociation

2 INTRODUZIONE

Nell'impostazione della normativa IAEA, l'approccio alla sicurezza degli impianti e delle attività attinenti il settore con produzione ed uso di radionuclidi, è concepito come una struttura organica identificata con il termine Safety Assessment (di seguito SA) ed organizzata su vari livelli con elementi fondamentali noti come Safety Standards. La normativa è seguita con continui aggiornamenti da quattro comitati in particolare: NUSSC, RASSC, WASSC e TRANSSC.

Gli Standards sono definiti in ottemperanza allo statuto IAEA che autorizza l'Agenzia a stabilire ed adottare, in collaborazione con i competenti organi delle Nazioni Unite, i riferimenti di sicurezza per la protezione della salute, la minimizzazione dei danni alla vita delle popolazioni, nonché alle proprietà e all'ambiente. Il riferimento normativo, adottato in questa sede per riassumere gli elementi e le strutture analitiche ritenute di maggiore importanza, è il rapporto "IAEA Safety Standards - Safety Assessment for Facilities and Activities", No. GSR Part. 4 (rif.[1]).

Il Safety Assessment struttura gli Standards per principi fondamentali (Fundamentals Safety Principles) e per requisiti di sicurezza (Safety Requirements) che devono essere rispettati (*must be met*) per assicurare una adeguata protezione alle popolazioni e all'ambiente.

I Fundamentals Safety Principles sono di tipo generale, e –mantenendo la termologia inglese- sono i seguenti:

Principle 1:	Responsibility for safety;
Principle 2:	Role of government;
Principle 3:	Leadership and management for safety;
Principle 4:	Justification of facilities and activities;
Principle 5:	Optimization of the protection;
Principle 6:	Limitation of the risks to individuals;
Principle 7:	Protection of population (present and future generations);
Principle 8:	Protection of accidents;
Principle 9:	Emergency prevention and response;
Principle 10:	Protective actions to reduce existing or unregulated radiation risks.

Un ulteriore schema di Safety Fundamentals, riferito alle tipologie di impianto ed attività cui essi sono rivolti ed alle aree delle tematiche generali su cui sono focalizzati, è riportato nel seguito (schema IAEA Safety Standards - protecting people and the environment).

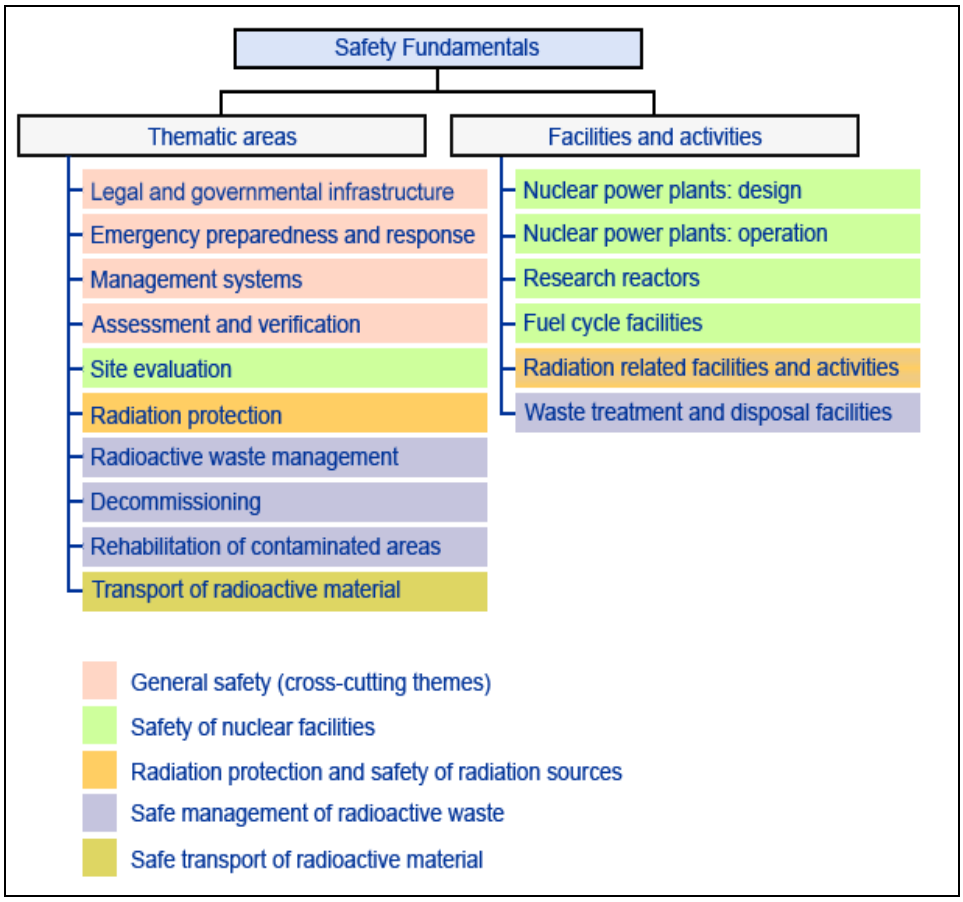

Figura 1 - Schema dei Safety Fundamentals (IAEA Safety Standards - protecting people and the environment)

I Safety Fundamentals contengono gli obiettivi fondamentali di sicurezza e i relativi principi di protezione. Essi, inoltre, costituiscono la base per l'impostazione dei Safety Requirements.

I Safety Requirements sono sviluppati nel dettaglio analitico e nel concreto delle raccomandazioni gestionali, tecniche ed operative. Tali requisiti devono essere soddisfatti per assicurare una adeguata protezione alla popolazione e all'ambiente nel breve e nel lungo termine. Essi sono riportati in 24 voci che vengono qui riprese dalla versione originale e brevemente descritte

Req. 1: Graded approach

Per determinare lo scopo ed il livello di dettaglio con cui è sviluppato il SA, può essere utilizzato un approccio graduato. Il requisito suggerisce che le risorse messe a disposizione per la sicurezza, gli obiettivi e la severità dei regolamenti da applicazione devono essere commisurate con la gravità dei possibili rischi e con la capacità del loro controllo.

Req. 2: Scope of the safety assessment

Il SA deve essere sviluppato per tutte le applicazioni, impianti ed attività che possono causare rischio da radiazione.

Req. 3: Responsibility for the safety assessment

La responsabilità della realizzazione del SA è attribuita alla persona legalmente responsabile, cioè alla persona o all'organizzazione responsabile dell'impianto o dell'attività. In altri termini, non è delegabile agli specialisti o tecnici che partecipino alla realizzazione materiale dello stesso.

Req. 4: Purpose of the safety assessment

Gli scopi primari del SA consistono nel determinare il raggiungimento di un adeguato livello di sicurezza per un impianto (o una attività) e nel verificare se gli obiettivi base e i criteri di sicurezza stabiliti dal progettista, dalle organizzazioni operative e dall'Agenzia, in accordo con i requisiti per la protezione e la sicurezza stabiliti in "International Basic Safety Standards", sono stati soddisfatti interamente. Il SA deve essere avviato almeno nella fase di progetto di un nuovo impianto o attività, comunque il più presto possibile nel caso di un impianto esistente.

Il requisito richiede ovviamente che sia verificato che tutte le safety features (prestazioni attinenti la sicurezza) siano operative.

La frequenza con la quale il SA deve essere aggiornato è in relazione al rischio di radiazione associato all'impianto o alla attività; in ogni caso, il SA va eseguito per tutte le varianti eventualmente inserite nel tempo nell'impianto.

Req. 5: Preparation for the safety assessment

Il primo passo nel portare avanti il SA è assicurarsi che tutte le risorse necessarie, le informazioni, i dati, gli strumenti analitici e i modelli di sicurezza siano identificati e disponibili.

Req. 6: Assessment of the possible radiation risks

Devono essere identificati e presi in esame tutti i possibili rischi da radiazione associati all'impianto o alle attività.

Req. 7: Assessment of safety function

Devono essere identificate e prese in esame tutte le safety functions associate all'impianto o alle attività.

Le safety functions sono funzioni che devono essere necessariamente realizzate per l'impianto e per le attività al fine di prevenire o mitigare le conseguenze radiologiche delle normali condizioni operative degli anticipated transient e delle condizioni incidentali. Queste funzioni includono il controllo della radioattività, la rimozione del calore di materiali radioattivi, il confinamento dello schermaggio dei materiali radioattivi nei termini e secondo la natura dell'impianto o dell'attività.

Req. 8: Assessment of site characteristics

E' necessario analizzare le caratteristiche del sito in relazione alla sicurezza dell'impianto o dell'attività. Tale approccio deve considerare almeno le seguenti condizioni:

a. le caratteristiche fisiche, chimiche e radiologiche che possono influire sulla dispersione del materiale radioattivo nelle varie situazioni di impianto;

b. l'identificazione degli eventi esterni di origine umana o naturale che hanno la potenzialità di influire sulle prestazioni dell'impianto e delle attività (come condizioni meteo estreme, terremoti, alluvioni, oppure impatti con aerei o mezzi di trasporto o con attività industriali);

c. la distribuzione della popolazione intorno al sito e le sue caratteristiche in relazione alla politica del Paese e dei Paesi vicini, in rapporto allo sviluppo di un eventuale piano di emergenza.

Req. 9: Assessment of provisions for radiation protection

Deve essere verificato e valutato in sede di SA se sono state predisposte adeguate misure di protezione della popolazione e dell'ambiente rispetto le radiazioni nucleari.

Req. 10: Assessment for engineering aspects

Deve essere verificato e valutato in sede di SA se un impianto o una attività utilizza, con la massima estensione possibile, strutture, sistemi e componenti con caratteristiche adeguate e provate.

Req. 11: Assessment of human factors

In SA sono affrontate le interazioni umane con l'impianto o con le attività. In tale contesto occorre determinare se le procedure e le misure di sicurezza

adottate per le normali attività operative garantiscono un adeguato livello di sicurezza. E' inoltre necessario valutare se le competenze del personale e i programmi di addestramento sono adeguati per mantenere il livello di sicurezza richiesto.

Req. 12: Assessment of safety over the lifetime of a facility or activity

Il SA deve coprire tutte le fasi della vita di un impianto o di una attività in cui sia possibile il rischio da radiazione. Il SA include pertanto attività che sono svolte su un lungo periodo di tempo che comprende il decommissioning, lo smantellamento di un impianto, il deposito a lungo termine delle scorie radioattive e le attività da svolgere nella fase di post chiusura di una giacenza di rifiuti radioattivi.

Req. 13: Assessment of defence in depth

L'approccio alla "difesa in profondità" (defence in depth) richiede la verifica dell'adeguatezza dei provvedimenti adottati per ciascun "livello di difesa" in modo da permettere al responsabile legale dell'impianto di poter:

a. *fronteggiare le deviazioni dalle condizioni operative normali o, per quanto riguarda le giacenze, intervenire sulle evoluzioni a lungo termine di tali giacenze radioattive;*

b. *effettuare il controllo degli eventi incidentali entro i limiti stabiliti dal progetto;*

c. *specificare le misure per mitigare le conseguenze degli incidenti che superano tali limiti;*

d. *mitigare i rischi di radiazione associati ai possibili rilasci di materiale radioattivo.*

Nel SA devono essere identificati tutti i necessari livelli di protezione, incluse le barriere fisiche di confinamento del materiale radioattivo nelle sue specifiche localizzazioni. Devono essere altresì identificati i controlli amministrativi di supporto per raggiungere la difesa in profondità. Ciò include l'identificazione:

- *delle safety functions che devono essere interamente soddisfatte;*
- *delle domande rivolte alle safety functions;*
- *di eventi (mechanism) che fanno insorgere queste domande e le necessarie e conseguenti risposte ad essi;*
- *di provvedimenti da prendere per prevenire l'insorgere di tali eventi;*
- *di provvedimenti presi per identificare o monitorare i deterioramenti causati da tali eventi;*
- *di provvedimenti per mitigare le conseguenze prodotte dal fallimento delle safety functions.*

Il SA deve determinare se la difesa in profondità è stata adeguatamente impostata.

Req. 14: Scope of the safety analysis

Nell'analisi di sicurezza deve essere verificata la prestazione di un impianto o di una attività in ogni sua fase operativa e, se necessario, post operativa.

Deve essere determinato in sede di SA se l'impianto o l'attività è in accordo con i rilevanti "safety requirements" e "regulatory requirements".

Req. 15: Deterministic and probabilistic approaches

Una safety analysis deve essere condotta mediante i due tipi di approccio: deterministico e probabilistico.

Gli approcci deterministici e probabilistici sono considerati complementari e pertanto possono essere utilizzati insieme per permettere un processo decisionale organico e completo.

Gli obiettivi dell'approccio deterministico sono di specificare ed applicare un set di regole conservative, in fase di progetto ed in fase operativa, al fine di determinare un elevato grado di confidenza soprattutto nella valutazione delle conseguenze di impatto (esempio: valutazione della capacità di contenimento).

L'analisi di sicurezza probabilistica usa un approccio completo e strutturato per identificare gli scenari di guasto (failure) nell'ambito della sicurezza del reattore.

Req. 16: Criteria for judging safety

I criteri di giudizio devono essere sviluppati per assicurare la conformità con i più alti livelli degli obiettivi, dei principi edei requisiti includendo i criteri di rischio relativi alla probabilità di accadimento degli anticipated events o degli eventi incidentali che possono produrre significativi rischi di radiazione.

Req. 17: Uncertainty[1] and sensitivity analysis

L'analisi di incertezza e sensitività deve essere sviluppata e tenuta in conto nei risultati dell'analisi di sicurezza e nelle conclusioni che ne derivano.

[1] Esistono due tipi di incertezza: l'incertezza aleatoria o stocastica e l'incertezza epistemica; l'incertezza aleatoria è riferita ad eventi o fenomeni che accadono con modalità random; questi aspetti di incertezza sono inerenti alla struttura logica del modello probabilistico. L'incertezza epistemica è associato allo stato di conoscenza relativo al problema che si sta considerando; in ogni analisi o modello di un fenomeno fisico vengono introdotte semplificazioni ed assunzioni; inoltre, anche per problemi relativamente semplici, un modello può omettere alcuni aspetti che sono stimati poco importanti per la soluzione cercata; tale incertezza è più attinente all'uso di modelli deterministici di analisi. Nell'analisi delle incertezze è necessario chiarire quale delle due tipologie si sta usando.

Le incertezze nell'analisi di sicurezza sono caratterizzate rispetto alle loro cause, alla loro natura e dal loro livello (di importanza) usando metodi quantitativi o il giudizio degli esperti (o entrambi).

Req. 18: Use of computer codes

Ogni metodo e codice di calcolo utilizzato nell'analisi di sicurezza deve essere sottoposto a verifica e validazione. Le attività di verifica del codice riguardano la revisione del codice sorgente in relazione alla sua descrizione nella documentazione a corredo. Le attività di validazione di un codice riguardano l'accuratezza dei risultati del codice stesso con riferimento ai dati sperimentali rilevanti e relativi ai fenomeni importanti.

Req. 19: Use of operating experience data

E' necessario fare una raccolta di dati relativi alle prestazioni operative di sicurezza, come gli errori umani e i quasi-incidenti, che dovranno essere registrati e valutati.

Req. 20: Documentation of the safety assessment

I risultati e le conclusioni del SA devono essere documentati in termini appropriati nella forma di un Safety Report che rifletta la complessità dell'impianto o dell'attività e il rischio di radiazione ad esso associato. Quanto sopra implica una parte preliminare illustrativa dell'impianto, necessaria a fornire una sufficiente familiarizzazione dello stesso sia dal punto di vista impiantistico sia funzionale. Lo scopo di tale rapporto è di dimostrare che l'impianto o l'attività è congruente con i FSP (Fundamentals safety principles), con i requirements stabiliti dalle presenti guide e con ogni altro requirement stabilito da leggi e regolamenti nazionali. I risultati qualitativi e quantitativi del SA costituiscono la base per tale rapporto di sicurezza.

Il Safety report deve documentare il SA con sufficiente evidenza e dettaglio al fine di supportare le conclusioni raggiunte e fornire dati adeguati per la verifica indipendente operata dai revisori delle Agenzie nazionali. Il Safety report include almeno:

a. *una giustificazione per la selezione degli "anticipated operational occurrences" nonchè degli eventi incidentali considerati nell'analisi;*

b. *una rassegna dei dettagli necessari alla raccolta di dati, alla definizione dei modelli, all'adozione dei codici di calcolo e delle assunzioni fatte;*

c. *i criteri usati per la valutazione e la modellizzazione dei risultati;*

d. *i risultati delle analisi riguardanti tutte le prestazioni dell'impianto o delle attività, i rischi di radiazione individuati e una discussione sulla valutazione delle incertezze;*

e. e conclusioni sull'accettabilità del livello di sicurezza raggiunto e le indicazione riguardanti necessari miglioramenti e misure addizionali previste.

Il Safety report deve essere aggiornato secondo necessità legali o tecniche. Il rapporto deve essere conservato fintanto che l'impianto non è completamente smantellato e decommissionato oppure fintanto che le attività sono state terminate e dimesse dal controllo normativo. Per le giacenze di residui radioattivi, il rapporto di sicurezza deve essere conservato per un lungo periodo di tempo dopo la chiusura del magazzino (con l'assenza di ogni materiale radioattivo).

Req. 21: Independent verification

I team operativi delle Utility devono sviluppare una verifica indipendente del SA prima che sia usato dalle organizzazioni operative o sottomesso alla revisione delle Agenzie.

Req. 22: Management of the safety assessment

Il processo con il quale il SA è prodotto deve essere pianificato, organizzato, applicato e sottomesso ad audit e revisione.

Req. 23: Use of the safety assessment

I risultati del SA dovranno essere utilizzati anche per specificare i programmi di manutenzione, sorveglianza ed ispezione. Devono, inoltre, essere utilizzati per specificare le procedure che regolano le attività operative e significative per la sicurezza e per rispondere agli eventi incidentali e a situazioni di anticipated events, nonché per verificare le competenze necessarie allo staff impiegato nell'impianto o nell'attività. Il SA costituisce la base per prendere decisioni relative alla gestione integrale del rischio.

Req. 24: Maintenance of the safety assessment

Il SA deve essere rivisto e aggiornato periodicamente.

I requisiti sono naturalmente governati dagli obiettivi e dai principi (Fundamentals Safety Principles). Qualora non fossero seguiti direttamente, nel SA, occorre aggiungere misure alternative per ottenere il livello di sicurezza richiesto. Il formato e l'esito dei requisiti è illustrato singolarmente al fine di facilitare il loro uso al gruppo operativo in termini armonizzati con il lessico e la struttura delle regolamentazioni internazionali.

Infine, sono tracciate le indicazioni/raccomandazioni di come osservare operativamente i requisiti richiesti adottando misure e procedure raccomandate da un largo consenso internazionale.

Tali indicazioni operative vengono indicate nella guida come “Safety Guides”. Esse dovranno riferirsi alle “buone pratiche internazionali” (international good practices) e sempre più riflettere le migliori consuetudini operative atte a supportare gli utilizzatori nel raggiungere elevati livelli di sicurezza.

La Figura 2 ripresa dal rapporto di riferimento No.GSR Part 4 (rif.[1]) indica la struttura del SA come ripartita nelle diverse funzioni richieste per l’impianto e rilevanti per la sicurezza.

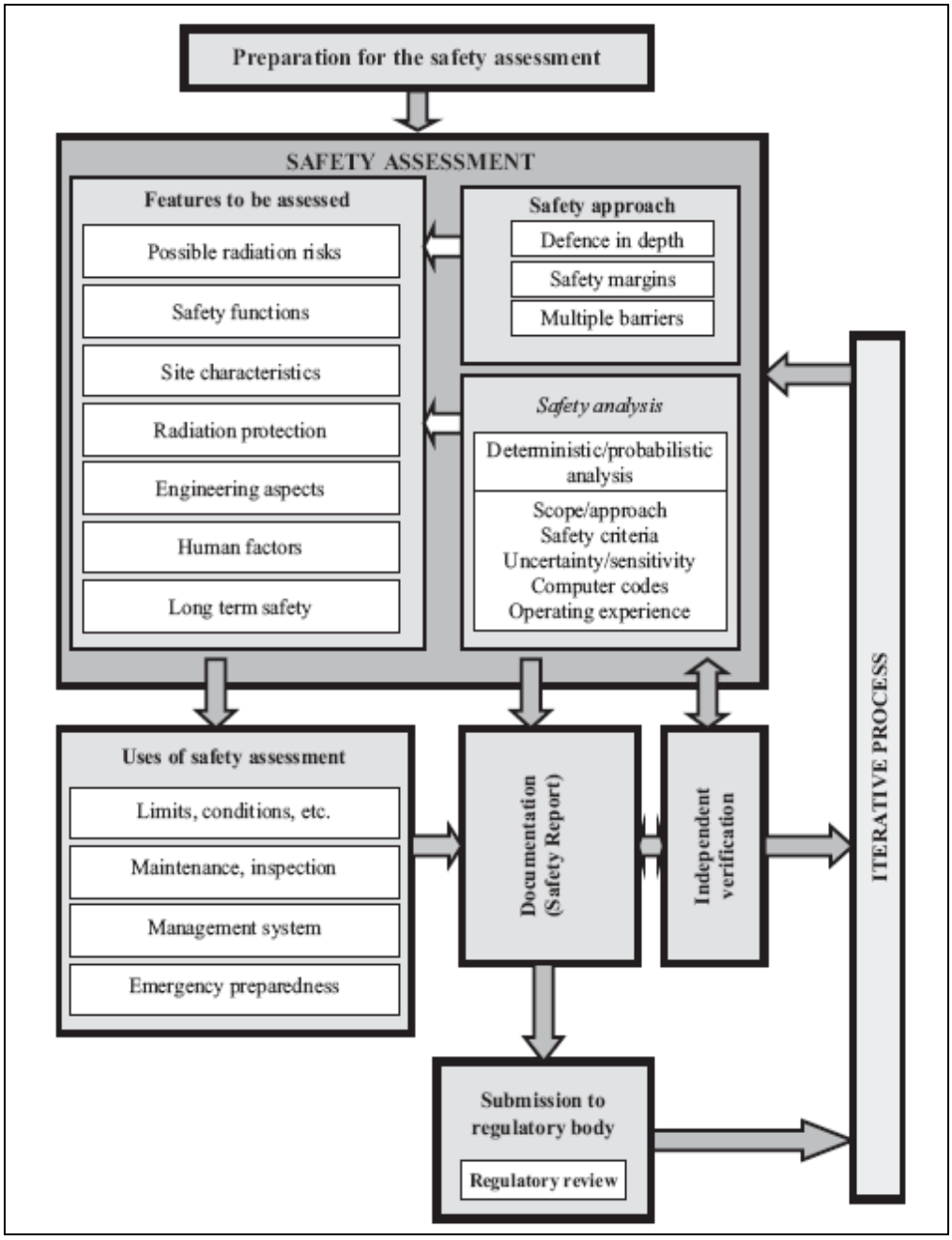

Figura 2 – Struttura del Safety Assessment (rif. [1])

Conformemente a quanto richiesto dal Req. 20 (Documentation of the safety assessment), i risultati e le conclusioni del SA, unitamente a tutte le valutazioni qualitative e quantitative sviluppate nell'analisi di sicurezza, devono essere

documentati nella forma di un “Rapporto di Sicurezza” indicato normalmente come PSA (Probabilistic Safety Assessment) o PRA (Probabilistic Risk Assessment). I due termini sono utilizzati con significato e validità equivalente.

La parte successiva del presente documento, ricollegandosi ai requisiti posti, indica le principali attività di verifica con cui valutare il rapporto di sicurezza (PSA). Essa percorre in tal modo l’intero processo dell’analisi di sicurezza quale richiesto sistematicamente per la valutazione del rischio di impianto che nella versione IAEA è ripartito su tre livelli base dell’analisi (PSA di livello 1 – PSA di livello 2 – PSA di livello 3).

3 LINEE GUIDA IAEA PER LA REVISIONE DI PSA

3.1 Riferimenti normativi

Le norme e gli standards di sicurezza emessi da IAEA, e riferiti ai PSA di impianto o di attività, sono contenute nei seguenti rapporti:

- [1] IAEA Safety Standards - Safety Assessment for Facilities and Activities - No. GSR Part. 4 (Vienna 2009);
- [2] IAEA-TECDOC-1135, Regulatory review of probabilistic safety assessment (PSA) – Level 1 (February 2000);
- [3] IAEA-TECDOC-1229, Regulatory review of probabilistic safety assessment (PSA) – Level 2 (July 2001);
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), Safety Series No. 50-P-12, IAEA,Vienna (1996);
- [5] Safety Reports Series No. 25 – Review of Probabilistic Safety Assessment by Regulatory Bodies, Vienna (2001).

Lo scopo del primo rapporto (rif. [1]) è la presentazione normativa del Safety Assessment quale strutturato nei propri elementi costitutivi principali (vedi §2).

I successivi rapporti (rif.[2], [3] e [5]) sono stati provocati dall'evidenza, emersa nel "IAEA technical committee meeting USA '94" e da "OECD – CNRA meeting '97", della mancanza di una linea guida formale per la valutazione di un PSA. Essi sono stati prodotti dalla collaborazione IAEA e OECD attraverso i rispettivi gruppi di studio.

I rapporti sono anche noti come PSA di livello 1 (rif.[2]), PSA di livello 2 (rif. [3]) e PSA di livello 3 (rif. [5]).

Il livello 1 identifica le sequenze di eventi incidentali che possono portare al danneggiamento del core nonostante i sistemi di sicurezza e le procedure operative predisposte per prevenire tali danneggiamenti. Non vengono considerati, a questo livello, le capacità di contenimento del sistema rispetto alle condizioni create dal danneggiamento.

Il livello 2 identifica le cause ed i percorsi attraverso i quali le sequenze considerate e le rispettive modalità di danneggiamento possono progredire fino a produrre carichi importanti sul contenimento e provocare eventuali modalità di rilascio radioattivo all'esterno.

Il livello 3 stima le conseguenze per la salute dell'uomo e per l'ambiente di ciascun rilascio radioattivo attraverso il trasporto dei materiali rilasciati.

Attualmente, sono stati elaborati nel mondo più di 200 PSA per la valutazione di livello 1, applicata quasi ovunque; le valutazioni di livello 2 sono sviluppate solo parzialmente con una analisi aggiornata; le valutazioni di livello 3 sono in

gran parte finalizzate solo alle conseguenze sull'uomo e non agli effetti ambientali ed economici prodotti nell'area.

L'ultimo rapporto (rif.[6]) riprende in un'unica versione i tre livelli considerati allineandoli in successione. I contenuti sono riportati con completezza e offrono una lettura più agevole agli operatori e ai revisori. Inoltre, è riferita più chiaramente la tracciabilità dei percorsi attraverso i tre diversi livelli analitici.

E' parso pertanto conveniente nell'impostazione del presente documento seguire la linea di tale rapporto (rif.[6]) apportando riferimenti complementari dei precedenti rapporti, ove ritenuto necessario.

3.2 Linee generali del processo di revisione

La scelta fatta per la normativa di riferimento IAEA SRS No. 25 in merito al processo di revisione di un PSA, ci induce ad anteporre alle verifiche applicate ai livelli di analisi, una parte metodologica riferita alla revisione in se, che la guida sviluppa con le sezioni "Introduction" e " The review process", in accordo con i requisiti generali, ma in un'ottica applicativa di ben 10 capitoli e 24 paragrafi.

Di questi viene ripresa la struttura generale di seguito indicata e gli argomenti di base trattati in alcuni paragrafi ritenuti di maggiore importanza, pur introducendo inevitabili ripetizioni.

1. INTRODUCTION

1.1 Background

1.2 Objective

1.3 Scope

1.4 Structure

2. THE REVIEW PROCESS

2.1 Introduction

2.2 Approach to review

- Timing of reviews
- Extent of review
- Documentation required for reviews
- Setting up the review team
- Agreement on methods
- Identification of/focus on important issues
- Comparison with other PSA
- Reworking of an analysis by a regulatory bady
- Documentation of the review findings
- Interaction with the Utility

- Research

2.3 Review of the aims, objectives and scope of PSA

- Development of regulatory principles for the review of PSA
- Aims and objectives of PSA
- Scope and applications of PSA
- Applications of PSA
- Sensitivity studies and uncertainty analysis

2.4 Review of methods and assumptions

- State of arte
- Level of detail
- Methods of analysis
- Source of data
- Use of best estimate methods, assumptions and data
- Validation and verification of computer codes

2.5 Review/audit of the Utility's PSA production process

- Scope of review/audit
- Quality assurance
- Organization of the PSA production team
- Future updating/development of the PSA.

3.2.1 Introduzione

3.2.1.1 Background

Il PSA fornisce un approccio sistematico per determinare se i sistemi di sicurezza sono adeguati, se il progetto dell'impianto è ben bilanciato (non esistono parti che da sole producono una forte criticità), se i requisiti relativi alla "defence in depth" sono stati osservati e se è stato ottenuto un basso livello di rischio.

I compiti del PSA possono essere diversi. Essi possono avere tutti gli eventi iniziatori riferiti alle condizioni di piena potenza dell'impianto o, in alcuni casi, estesi a potenze minori o allo stato di shut-down. I PSA dovranno considerare sia gli eventi interni riferiti all'impianto sia gli eventi interni riferiti alle condizioni generali di pericolo come incendio o allagamento. Dovranno inoltre considerare la possibilità di eventi esterni come i terremoti o gli impatti aerei.

3.2.1.2 Obiettivi

Il rapporto di sicurezza IAEA SRS No.25 (rif.[6]) fornisce una Linea guida per assistere l'Agenzia nella fase di revisione del PSA prodotto dalle Utilities. Tale

guida dovrà verificare che il PSA è stato condotto ad uno standard accettabile e che pertanto può essere utilizzato per le applicazioni a cui è indirizzato. In tal senso il processo di revisione diventa una fase importante nella determinazione di accettabilità del PSA. Oltre a ciò, il processo di revisione sarà in grado di fornire una migliore comprensione del funzionamento e dei limiti dell'impianto e di assistere i team tecnici nel gestire e sviluppare le revisioni di PSA.

3.2.1.2 Scope

Il compito di questo rapporto è la revisione del PSA ai citati livelli 1, 2 e 3 e per tutte le sequenze di evento che possono capitare con qualunque modalità durante l'esercizio di impianto includendo la piena potenza, la media potenza e lo shut-down.

Si deve rilevare che i risultati delle prestazioni di un PSA, sono spesso le identificazioni di variazioni del progetto o delle operazioni dell'impianto che possono aumentare il livello della sicurezza. Questo può comprendere l'aggiunta di ulteriori sistemi di sicurezza o di misure gestionali degli eventi incidentali.

3.2.1.3 Struttura

La struttura con la quale l'Agenzia può condurre la revisione del PSA ai sensi del presente rapporto è ripresa nel seguito in riferimento alla revisione dei livelli 1, 2 e 3.

3.2.2 Processo di revisione

3.2.2.1 Introduzione

La presente sezione della guida intende indicare le modalità con le quali l'Agenzia si propone di impostare la revisione del PSA relativo ad un Impianto Nucleare di Potenza al fine di valutare se il PSA stesso è stato condotto con uno standard accettabile.

3.2.2.2 Approccio alle revisioni

Tempistica (Timing)

Le revisioni condotte dalle Agenzie possono essere "on-line" o "off-line", a seconda del tempo in cui la revisione è condotta.

Una revisione on-line è condotta immediatamente dopo che un team dell'Utility ha finito una particolare task. Il vantaggio di questo approccio è che molte delle revisioni possono essere incorporate tempestivamente nel PSA, riducendo in tal modo il numero di riedizioni necessarie. Lo svantaggio è che la revisione può essere basata su rapporti che sono cambiati significativamente durante il prosieguo dell'analisi, di conseguenza le precedenti revisioni devono essere riviste.

Una revisione off-line è condotta dopo che il team dell'Utility ha presentato il rapporto finale all'Agenzia. Il vantaggio di questo approccio è che i documenti PSA sono rivisti una volta sola (se non sono richieste diverse edizioni). Lo

svantaggio è che la revisione può trovare problemi ed inadempienze significativi che potevano essere identificati e corretti più agevolmente nelle fasi iniziali dell'analisi.

L'approccio più efficiente per l'Agenzia è di percorrere la strada della review on-line ogni volta sia possibile in modo tale da controllare ciascuna task prima del completamento dell'analisi.

Il timing richiede un accordo preliminare tra Agenzia e Utility con la stesura di una programmazione ben definita. Ciò consente di mediare i bisogni di entrambe le organizzazioni e di assicurare che il processo di revisione sia condotto in modo efficiente e sia in grado di minimizzare ogni ritardo per il completamento del PSA o della sua revisione.

La revisione di dettaglio del PSA dovrebbe, comunque, partire con l'analisi di livello 1, procedere con l'analisi del livello 2 e terminare con l'analisi di livello 3. Ciò è importante per assicurare che le mancanze delle parti precedenti dell'analisi siano identificate e non siano portate avanti in modo tale da generare conclusioni incorrette.

Estensione della revisione (Extent)

L'estensione della revisione da parte dell'Agenzia deve essere concordata con la Utility durante la fase di partenza del processo decisionale. In particolare, si può parlare di revisione estesa (extent review) e di revisione limitata a seconda del livello di dettaglio stabilito a livello nazionale.

In una revisione estesa, si hanno vantaggi significativi in termini di comprensione, di confidenza nel PSA e di riduzione degli sforzi richiesti per effettuare successive revisioni. Lo svantaggio è relativo all'elevato costo; pertanto questo approccio è difficilmente applicabile nel caso le revisioni riguardino numerosi progetti di impianto e nel caso in cui le risorse disponibili dell'Agenzia sono limitate.

In una revisione limitata l'obiettivo perseguitato è di assicurare che tutti gli aspetti delle sequenze incidentali che conducono al danneggiamento del core, ad un largo rilascio o a particolari conseguenze esterne all'impianto siano adeguatamente modellati e i dati usati per determinare le frequenze delle sequenze di evento siano rappresentativi dell'impianto. Nel fare questo la revisione dovrebbe focalizzare quegli aspetti del PSA che hanno il più alto impatto sui risultati. Il vantaggio di questo approccio è che richiede minori risorse all'Agenzia; lo svantaggio è che comporta una minore capacità di lettura e un minor livello di confidenza nei risultati ottenuti. Questo metodo aumenta gli sforzi richiesti per revisionare applicazioni successive.

Una revisione estensiva deve essere preferita nei seguenti casi:

a. quando il livello di rischio di un impianto è relativamente alto;

b. per il primo PSA redatto da una Utility;

c. per il PSA di un nuovo tipo di reattore;

d. per il PSA dove il progetto di impianto o le procedure operative sono significativamente differenti dall'esperienza precedente.

Documentazione richiesta per le revisioni

La documentazione richiesta per una revisione comprende sia la documentazione descrittiva dell'impianto e delle procedure operative di un impianto nucleare di potenza sia l'analisi e il rapporto di sicurezza (PSA) dell'impianto stesso. Questa documentazione è di vitale importanza dal momento che essa è sottoposta in termini formali dalla Utility all'Agenzia e costituisce la base per la revisione ufficiale e per ogni utilizzo del PSA.

Il punto di partenza per l'elaborazione e la revisione di un PSA deve essere una chiara descrizione (definizione) del progetto di impianto e di come si intende operarlo anche in rapporto al tipo di sito prescelto.

Un PSA di un impianto esistente è invece parte di una più generale revisione della sua sicurezza che può condurre ad un programma di modifiche dell'impianto.

E' importante che la documentazione deve fornisca i dati e le informazioni sufficienti e necessarie per permettere ai revisori una familiarizzazione con il progetto e con l'operatività dell'impianto. Ciò include la descrizione dei sistemi, delle procedure operative, delle procedure di test e di manutenzione, delle procedure di gestione delle situazioni incidentali. Tutto ciò è coordinato con visite all'impianto.

L'Agenzia deve accordarsi con la Utility sul format e sul contenuto della documentazione prima dell'avvio del PSA. Ciò assicurerà che la quality assicurance (QA) osservata dai processi di revisione sia condotta molto più efficacemente.

La prima task del team di revisione è di testare che la documentazione del PSA corrisponda a quanto descritto sopra. Se questo non è rispettato i revisori devono indicare alla Utility quale documento addizionale è richiesto in modo che sia fornito in tempi brevi. Ciò include un check che assicuri che:

- l'informazione sul progetto e sulla operatività dell'impianto sia chiaramente documentata;
- le metodologie usate per sviluppare le singole task del PSA siano chiaramente documentate e che rendano possibile la ripetizione dell'analisi senza informazioni addizionali;
- le analisi di supporto siano incluse nella documentazione del PSA o siano disponibili per la consultazione da parte dei revisori;
- tutte le tabelle, figure e appendici siano fornite;
- ci siano adeguati riferimenti della letteratura di supporto (referenze);
- tutte le informazioni siano consistenti con i "freeze date" del PSA.

Inoltre, i revisori devono verificare che le informazioni del PSA di livello 1 necessarie per valutare le prestazioni del contenimento e il trasporto di radionuclidi siano descritte e trasferibili a livello 2 e a livello 3 della corrispondente analisi con sufficiente completezza e precisione.

Per quanto attiene la documentazione della fase analitica dei tre livelli di analisi, è utile riprendere le richieste del Req. 20 di IAEA-SRS No.25 (rif.[1]), discusso nel §2, che comprendono:

- una giustificazione per la selezione degli "anticipated operational occurrences", nonchè degli eventi incidentali considerati nell'analisi;
- una rassegna dei dettagli necessari alla raccolta di dati, alla definizione dei modelli, all'adozione dei codici di calcolo e delle assunzioni fatte;
- i criteri usati per la valutazione e la modellizzazione dei risultati;
- i risultati delle analisi riguardanti tutte le prestazioni dell'impianto o delle attività, i rischi di radiazione individuati e una discussione sulla valutazione delle incertezze;
- le conclusioni sull'accettabilità del livello di sicurezza raggiunto e le indicazione riguardanti necessari miglioramenti e misure addizionali previste.

Infine, sul piano pratico e valutativo, è considerato utile che i revisori dispongano copie informatiche del PSA piuttosto che di copie cartacee, particolarmente per le analisi eseguite mediante Alberi degli eventi e Alberi dei guasti. Ciò permette, infatti, ai revisori:

- una più agile ricerca delle informazioni specifiche nei modelli;
- di effettuare degli spot checks sui modelli e sulle specifiche quantificazioni;
- di effettuare una analisi di identificazione delle aree del PSA che richiedono una particolare revisione;
- di effettuare valutazioni di sensitività per verificare quanti variazioni nelle assunzioni fatte possono incidere sui risultati del PSA;
- di utilizzare il PSA come base per una regolamentazione riferita al rischio.

Struttura del team di revisori

Il dimensionamento del team di revisori deve essere sufficiente a condurre una revisione di tipo esteso quale definito dall'Agenzia.

E' importante che il team di revisori abbia esperienza nelle tecniche di elaborazione dei vari livelli di PSA e competenze sufficienti a valutare gli aspetti più critici e con maggiori probabilità di approfondimento, durante la revisione del PSA. Per supportare il lavoro, l'Agenzia può avvalersi di consulenti esterni.

Il range di attività include tipicamente le seguenti competenze:

- analisti di sistemi;
- staff con un backgroud operativo e familiarizzazione con le procedure di emergenza;
- esperti nei fenomeni che possono accadere per eventi severi a seguito di fusione del nocciolo;

- specialisti strutturali atti ad analizzare la prestazione di contenimento a seguito dei carichi imposti da incidenti severi;
- specialisti di PSA.

Il team di revisori deve, inoltre, includere personale con esperienza in analisi deterministica.

Accordo sui metodi

Nell'ambito degli accordi preliminari tra Agenzia ed Utility sono da definire i metodi di base e/o principali da utilizzare ai vari livelli 1, 2 e 3 di PSA e/o nelle corrispondenti sezioni dell'analisi di sicurezza.

Identificazione e focalizzazione degli spetti più importanti

L'attività dei revisori richiede di focalizzare le aree che hanno l'impatto più significativo sui risultati del PSA.

Una rassegna preliminare (di tentativo) può essere condotta per identificare tali aree alle quali dovrà essere rivolta una revisione di maggior dettaglio.

Confronto con altri PSA

E' spesso utile condurre un confronto dei metodi utilizzati da un PSA con quelli adottati in altri PSA di impianti similari. E' nella pratica di molti paesi usare la valutazione dello stato dell'arte di un PSA di riferimento per sviluppare/revisionare un nuovo PSA.

Rielaborazione di un'analisi da parte di una Agenzia

I revisori dovranno considerare se esista la necessità di condurre delle valutazioni indipendenti o di rivedere particolari parti del PSA per ottenere una migliore comprensione del PSA stesso, dei suoi aspetti di sensitività ed incertezza.

Documentazione delle conclusioni della revisione

Le conclusioni della revisione devono essere documentati in uno specifico rapporto di revisione di PSA (PSA review report). Il format, i contenuti e la struttura del rapporto dipendono, oltre che dallo scopo della revisione stessa, dalle prescrizioni nazionali.

Un rapporto di revisione deve contenere le informazioni di base che consistono in una breve descrizione dell'impianto e dell'organizzazione del PSA, lo scopo, gli obiettivi e il compito del PSA e le informazioni generali sul processo di revisione effettuato.

In particolare, il rapporto deve contenere le informazioni relative alle conclusioni del processo di revisione espresse in termini di corretta applicazione del metodo scelto per ognuno dei compiti del PSA, di principali preoccupazioni espresse dai revisori, di risposte fornite e di risoluzioni finali raggiunte.

Deve inoltre contenere le conclusioni relative ai risultati raggiunti mediante l'analisi di sensitività, incertezza e di importanza.

Informazioni aggiuntive potrebbero riguardare eventuali raccomandazioni per migliorare l'ambito di applicazione, la metodologia e la qualità del PSA o eventuali modifiche da apportare al progetto o alle attività dell'impianto.

E' buona pratica includere al rapporto la lista dei componenti del team di revisori indicando i principali responsabili per ciascuna area della revisione.

Se è stata effettuata una revisione on-line, i revisori dovranno completare l'esame in breve tempo; ciò vale, a livello di principio, anche se il processo di revisione è off-line, pur riconoscendo che i tempi saranno molto più lunghi.

E' necessario mantenere traccia di tutta la documentazione utilizzata nel processo di revisione di un PSA in accordo ai requisiti del QA.

Interazione con le Utility

E' importante, durante la fase di revisione, che i revisori concordino con l'Utility su come gestire i rapporti tra di loro e i rapporti con progettisti e consulenti. L'ottimizzazione di tale processo è di notevole importanza, poiché può avere impatto significativo sul tempo di revisione e sullo sforzo richiesto ai revisori.

Ciò implica un equilibrio tra una interazione libera, che può essere produttiva ed efficiente, ed il grado di conformità formale al processo regolamentare, con possibili ed eventuali sanzioni legali come conseguenza. I revisori, avendo presente il loro ruolo di riferimento normativo, devono evitare un rapporto troppo stretto con il personale della Utility, che può percepire ciò come una limitazione della loro indipendenza, mentre dovrebbero adoperarsi per mantenere un rapporto amichevole e professionale con il quale è possibile realizzare un ragionevole scambio di punti di vista e di informazione.

L'obiettivo delle parti è un rapporto finale PSA, sul quale la Utility sia convinta di assumere piena responsabilità e che sia nel contempo ritenuto accettabile dall'Agenzia e dai suoi revisori. Per questo scopo occorre aspettarsi che alcune interazioni siano necessarie. Alcuni commenti dei revisori, infatti, possono richiedere che parti del PSA siano rielaborate usando diverse assunzioni o metodi mentre altri commenti possono richiedere soltanto che la documentazione del PSA sia più chiaramente leggibile e maggiormente giustificata.

Alla fine della revisione, è buona pratica per i revisori comunicare le loro osservazioni al team PSA della Utility, benché essi abbiano normalmente ricevuto tali giudizi durante il corso della revisione. Ciò sarà normalmente fatto spedendo una copia del rapporto dei revisori.

3.2.2.3 Revisione delle finalità, obiettivi e compiti del PSA

Il punto di partenza per il processo di revisione è idealmente da porre quando è assunta la decisione di effettuare il PSA. Tale decisione deve essere presa dall'Agenzia in termini di requisiti o di raccomandazioni, può essere presa volontariamente dalla Utility o può essere il risultato di una richiesta governativa (ciò si riferisce, in modo particolare, ad impianti esistenti).

Scopi e obiettivi del PSA

L'Agenzia può ritenere utile formulare le finalità e gli obiettivi di un PSA. In questo caso è necessario un confronto con le proposte della Utility in modo da raggiungere un accordo.

Il PSA deve essere in grado di evidenziare le debolezze di impianto e di raggiungere le decisioni di miglioramento del livello di sicurezza.

Se sono stati specificati i target o i criteri di rischio il PSA deve essere adeguatamente indirizzato alla loro valutazione..

I target di rischio sono tipicamente espressi in termini di frequenza di danneggiamento del core, come richiesto dal PSA di livello 1, espressi in termini di frequenza di accadimento di larghi rilasci, come richiesto a PSA di livello 2 o come criteri di valutazione del rischio sociale (nel sito esterno all'impianto) come richiesto dal PSA di livello 3 (può essere utile per confronto evidenziare che l'elaborazione di un PSA/PRA eseguita con procedure NRC, identifica gli stessi target di rischio collocandoli agli stessi livelli di analisi senza classificare espressamente il livello).

L'Agenzia e la Utility devono accordarsi sui compiti e sugli usi di un PSA atti ad assicurare il raggiungimento degli obiettivi e delle finalità generali dell'analisi. E' buona pratica per l'Agenzia specificare i compiti del PSA che si aspetta siano condotti dalla Utility. Ciò deve essere comparato con quello che la Utility ha proposto e deve essere raggiunto un accordo.

La Linea guida di riferimento (rif.[6]) pone 10 specifiche per i compiti usualmente richiesti al PSA.

3.2.2.4 Revisione dei metodi e delle assunzioni

Stato dell'arte

I revisori determinano lo stato del PSA che l'Agenzia si aspetta dalla Utility. Questo potrebbe essere lo stato dell'arte dei metodi usati nel PSA per introdurre miglioramenti rispetto ai metodi precedentemente esistenti.

E' riconosciuto, infatti, che i metodi del PSA sono in fase evolutiva. Pertanto, è importante che l'Agenzia e la Utility determinano lo stato dell'arte del PSA da garantire.

Livello di dettaglio

I revisori necessitano di determinare se il livello di dettaglio nel PSA è sufficiente per includere tutte le interdipendenze significative delle applicazioni fissate. Tuttavia, è riconosciuto che il livello di dettaglio dell'analisi di sistemi ha una incidenza significativa sul costo e sulla credibilità dei risultati.

Dipendenze significative possono essere omesse, se il livello di dettaglio non è sufficiente.

E' buona pratica raggiungere un livello che assicuri che tutte le dipendenze significative sono incluse nel modello, in altre parole, la cura del dettaglio serve per non tagliare dipendenze, tra componenti e sistemi, significative per l'analisi.

Metodi di analisi

I revisori devono determinare se i metodi utilizzati nell'analisi sono adeguati per raggiungere le finalità del PSA. La Linea guida sottolinea in particolare le valutazioni per il PSA di livello 2 che dovrebbe includere:

- l'indicazione dei codici usati per modellare la progressione dell'incidente severo;
- lo strumento generale per modellare le sequenze di evento severo;
- l'indicazione delle quantificazioni probabilistiche applicate alle sequenze di evento.

Sorgente dei dati

I revisori devono poter confermare che tutte le sorgenti di dati sono state identificate e sono rilevanti.

Lo scopo è di assicurare che dati specifici dell'impianto sono usati ogni volta che è possibile. Se ciò non è possibile, l'uso di dati provenienti da operazioni fatte da sistemi dello stesso tipo o di dati generici è accettabile.

3.3 Revisione del PSA di livello 1 (Impianto operante a piena potenza)

L'indicazione dei vari passi analitici che la guida suggerisce per la revisione del PSA di livello 1, in condizione operativa di piena potenza, è formulata secondo il percorso che segue:

- Identificazione e raggruppamento degli eventi iniziatori;
- Analisi delle sequenze incidentali;
- Analisi dei sistemi;
- Analisi dei guasti dipendenti;
- Analisi dei sistemi passivi, componenti e strutture;
- Approccio all'affidabilità umana;
- Dati richiesti per il PSA;
- Analisi dei sistemi computerizzati;
- Analisi dei pericoli interni ed esterni;
- Quantificazione delle sequenze incidentali;
- Analisi di sensitività;
- Analisi delle incertezze;
- Analisi di importanza;
- Interpretazione dei risultati del PSA;
- Audit del PSA QA.

3.3.1 Identificazione e raggruppamento degli eventi iniziatori

Generalità

Nella Linea guida la tematica in oggetto, che costituisce la sezione relativa all'analisi di sicurezza a livello 1 del PSA , articola gli eventi iniziatori usando una combinazione dei due metodi base, Alberi di guasto e Alberi degli eventi. L'approccio più comune è quello costituito da Alberi di evento relativamente piccoli e Alberi di guasto di grandi dimensioni, con i quali sono, in particolare, modellati i sistemi di supporto e sicurezza.

Identificazione e raggruppamento

L'identificazione per gruppi di eventi iniziatori che hanno la possibilità di produrre danneggiamenti al core, in concomitanza con un guasto ai sistemi di sicurezza, è il primo passo dell'analisi che può essere condotta con diverse procedure sistematiche:

- metodi analitici, come Hazop (Hazard and Operability Analysis), FMEA (Failure Mode and Effects Analysis);
- analisi deduttive, come Master Logic Diagram;
- confronto con le liste di eventi iniziatori sviluppate in PSA per impianti simili e in linee guida esistenti;
- identificazione di eventi iniziatori evidenziati dall'esperienza operativa su impianti del tipo in esame o su impianti simili.

In accordo con lo scopo del PSA, il set di eventi iniziatori includerà:

- eventi interni come il LOCA e il conseguente transitorio;
- pericoli interni (incendio, esplosioni, allagamenti di origine interna);
- perdita dell'alimentazione di potenza.

Ai revisori è chiesto di testare gli eventi iniziatori considerati e di valutarne la completezza, anche se si riconosce la difficoltà di dimostrarla in termini assoluti. Si ritiene, tuttavia, che utilizzando una combinazione dei metodi indicati, il rischio di ulteriori contributi di danneggiamento del core, non considerati, sia piccolo. Una attenzione particolare è richiesta ai revisori per le prestazioni delle funzioni che siano di tipo nuovo o peculiari dell'impianto in esame.

Un set di eventi iniziatori, che in particolare può essere individuato dall'applicazione della metodologia FMEA, è dato da eventi generati da errori operativi (errori di esecuzione o di omissione delle normali procedure di esercizio).

Un set di eventi iniziatori può comprendere eventi di frequenza molto bassa spesso non considerati dal PSA. I revisori devono valutarne l'esistenza e la validità delle scelte poiché se lo sviluppo dell'analisi comprenderà anche i PSA di livello 2 e 3, eventi a bassa frequenza in situazioni particolari potrebbero generare potenziali conseguenze rilevanti (radiological consequence).

L'insieme dell'analisi che si sta descrivendo e dei criteri di valutazione impiegati attengono evidentemente al metodo probabilistico di analisi, che deve svilupparsi orizzontalmente, con un livello di dettaglio sufficiente ad includere ogni interdipendenza significativa dovuta ad esempio alle connessioni con i sistemi ausiliari e di supporto.

In merito, occorre considerare anche le situazioni prodotte da eventi indotti (esempio: missili prodotti dalla disintegrazione di una turbina) o eventi che coinvolgono più unità dell'impianto (esempio: perdita dell'alimentazione elettrica).

Analoga attenzione va posta su eventi che possono investire interconnessioni tra diverse unità di impianto, determinando la perdita di indipendenza effettiva di sistemi.

Si richiede infine che sia confrontato il set di eventi iniziatori indicato nel PSA con quelli relativi ad impianti simili.

I team di revisione e valutazione della Utility devono conoscere il livello di dettaglio che l'Agenzia si aspetta di trovare nel PSA e che l'Utility conferma corrispondere a ciò che è stato concordato prima dell'avvio del PSA stesso.

I revisori devono inoltre verificare e confermare l'adeguatezza delle fonti dei dati utilizzati nelle analisi citate, quali la frequenza di accadimento degli eventi iniziatori, la probabilità di guasto dei componenti, l'indisponibilità del componente durante il periodo di test e manutenzione, la probabilità inerente le cause comuni di guasto, la probabilità di errore umano e la mancata risposta su chiamata dei sistemi di protezione e supporto.

Tenuto conto delle raccomandazioni segnalate dalla linea guida, al fine di limitare il numero di Alberi di eventi da costruire per l'analisi, alcuni eventi iniziatori possono essere raggruppati e considerati congiuntamente.

La guida segnala categorie di eventi iniziatori che tipicamente possono manifestarsi in un impianto nucleare di potenza. Esse sono citate per tipologie con particolare attenzione a quelle più soggette a sviluppare sequenze gravose e con maggiori probabilità di indurre perdite del contenimento (PSA di livello 2).

Una prima categoria comprende eventi espressi in termini generali: aumento o diminuzione del calore dal core, anomalie nella distribuzione della reattività e della potenza, aumento o diminuzione del fluido refrigerante nel reattore. Una seconda categoria comprende la modalità di perdita di refrigerante nei canali del core (LOCA). Una terza categoria comprende modalità di guasto od anomalie funzionali che producono dei transitori (esempio: rottura sulle linee vapore o sulle linee alimentazione).

A quanto sopra si aggiungono le anomalie o interruzioni dei sistemi ausiliari e la totale o parziale perdita di alimentazione elettrica (blackout) con diversi tempi di durata.

Riprendendo gli eventi del tipo LOCA, una lista di eventi iniziatori include usualmente tutte le diverse possibili sezioni di rottura e le loro localizzazioni, che possono condurre ad una perdita di refrigerante primario. Essa è basata

sul progetto esecutivo e sul layout di impianto ed include guasti di valvole con particolare riferimento alle “relief valves”.

I LOCA sono identificati per categorie e raggruppati con riferimento al criterio di successo applicato ai sistemi di sicurezza che possono intervenire per prevenire o limitare danneggiamenti al core.

Per LOCA relativi alle condotte del sistema di refrigerazione del reattore, è richiesta una revisione particolarmente attenta alle localizzazioni dell’eventuale guasto, poiché esse possono influenzare il successo degli interventi richiesti ai sistemi di sicurezza. Infine, i LOCA sono ripartiti in “large”, “medium” and “small” LOCA sulla base dei sistemi di sicurezza di cui è richiesto l’intervento.

Per quanto riguarda i transitori originati da eventi iniziatori l’attenzione dovrà essere rivolta ad alcune specifiche prestazioni dell’impianto. Esempi tipici di eventi iniziatori per PWR, che dipendono dalle prestazioni di impianto riguardano: la rottura della condotta di un generatore di vapore e la perdita di refrigerazione secondaria a causa della perdita di acqua di alimentazione o della perdita di vuoto nel condensatore.

3.3.2 Analisi delle sequenze incidentali

Criteri di successo e analisi delle sequenze di eventi

Il passo successivo dell’analisi è la determinazione della risposta dell’impianto a ciascun gruppo di eventi iniziatori sopra indicato. Le sequenze valutate come possibili possono condurre sia ad uno stato sicuro in cui il reattore è in condizioni di shut down ed il calore residuo è adeguatamente rimosso (o in fase di rimozione), sia a situazioni con danneggiamento del core (cfr. req. 20 e 21).

In conformità con i safety standards sono definite le safety functions richieste per prevenire danneggiamenti del core in rapporto a ciascun gruppo di eventi iniziatori.

Le safety functions richieste dovranno tipicamente comprendere: il rilevamento dell’evento iniziatore, il reactor shut down, la rimozione del calore residuo e le protezioni di contenimento, in riferimento al tipo di reattore e dalla natura dell’evento iniziatore.

I sistemi di sicurezza in grado di eseguire ciascuna di queste funzioni devono essere chiaramente identificati nel PSA e dai revisori. Occorrerà definire i criteri di successo per l’intervento di ciascun sistema, normalmente valutati come “livello minimo” della prestazione richiesta ed espressi in termini di numero di dispositivi (trains) di un sistema ridondante richiesti ad operare o dal numero di “relief valves” richieste per aprire/chiudere (esempio 2 su 3, 1 su 2).

Quanto sopra attua i requisiti derivati dalla “transient analysis”, espressi in termini di criteri prestazionali (performance criteria) come i valori di portata, di pressione e tempi di risposta.

E’ importante per i revisori verificare i livelli di successo dei sistemi di sicurezza per determinare se dipendono solo da un proprio funzionamento o dal guasto

di altri sistemi di sicurezza (verifica di dipendenza) e per verificare se ciò è considerato nella definizione di detti criteri.

Un esempio è dato per i large LOCA in reattori PWR dall'intervento del "low pressure injection system" (LPIS), che può essere diverso a seconda del numero di accumulatori che devono iniettare acqua nel circuito primario.

Il criterio di successo deve inoltre identificare e valutare l'intervento richiesto dall'operatore per portare l'impianto in sicurezza seguendo le procedure di emergenza indicate.

Tali procedure dovranno essere a loro volta valutate dall'analisi tecnica del tipo "diagramma delle sequenze di evento" (ad esempio l'insufficienza di acqua di refrigerazione può essere data da una rottura della "gamba" fredda di refrigerazione; la portata può essere ripresa da un gruppo di ECCS connessi con questa gamba e ciò deve essere considerato nella definizione del criterio di successo).

Da quanto sopra risulta che la parte di analisi descritta deve entrare a considerare il dettaglio dell'impianto in questione e pertanto presenta diversità anche notevoli da impianto ad impianto. Ciò è tanto più evidente in rapporto ai reattori di terza generazione.

La Linea guida indica così la modalità di base per procedere in ciascuna condizione. Appropriati codici di calcolo sono utilizzati per definire i criteri di successo ed è richiesto ai revisori di considerare la validità di tali codici confrontando diversi aspetti suggeriti dalla Linea guida stessa. Con riferimento ai codici di calcolo utilizzati per definire i criteri di successo, i revisori hanno bisogno di controllare che:

- i metodi di calcolo utilizzati siano definiti chiaramente per poter modellare i transitori e gli incidenti da analizzare in modo da ottenere una miglior stima dei risultati;
- sia i codici di calcolo sia gli utilizzatori dei codici siano soggetti a procedure di QA;
- i codici di calcolo utilizzati siano documentati, referenziati, verificati e validati a seconda del campo di applicazione;
- tutte le fonti di dati relativi all'impianto siano referenziate;
- per ciascun caso analizzato sia fornita una descrizione dei dati di ingresso, delle assunzioni fatte e dei sistemi di sicurezza prefissati;
- tutti i calcoli siano documentati, così come i risultati delle analisi che verranno utilizzati nello studio del PSA.

E' buona pratica per le procedure di QA usate nell'elaborazione di un PSA (comprese le procedure tecniche) che esse siano viste ed approvate dall'Agenzia nelle prime fasi di attività.

Per quanto riguarda l'analisi effettuata mediante Alberi di eventi, per ciascun evento iniziatore i revisori devono verificare la conformità e la completezza con le "safety functions" richieste ad intervenire e con i sistemi di sicurezza identificati con i criteri di successo. Lo stato dei "front line" dei sistemi di

sicurezza rappresenta l'aspetto principale sull'Albero degli Eventi sul quale sono indirizzati gli interventi operativi e le azioni di "recovery" che influiscono direttamente sul decorso incidentale.

L'analisi degli Alberi degli eventi è ormai sufficientemente conosciuta e praticata per permettere la modellizzazione di ogni dipendenza che possa intervenire tra guasti di componenti ed errori operativi.

Alcuni particolari di tali valutazioni sono riportati dalla Linea guida insieme con gli aspetti di documentazione che devono essere inseriti nel PSA (Event sequence analysis).

Plant Damage States (PDS)

La fase successiva dell'analisi è finalizzata al raggruppamento delle sequenze incidentali identificate come tali da indurre il danneggiamento del core. I raggruppamenti costituiscono un'interfaccia tra l'analisi del PSA di livello 1 e quella successiva del PSA di livello 2. Essi richiedono che tali sequenze siano caratterizzate in rapporto alle condizioni di impianto cui essi conducono ed alla disponibilità dei sistemi di sicurezza che possono prevenirlo o mitigarlo.

E' pertanto necessario verificare che tali sequenze siano state correttamente identificate dall'analisi con Alberi degli eventi e siano state definite per ciascuna di esse le cause che hanno potuto produrre il danneggiamento stesso.

I revisori necessitano pertanto di conoscere la definizione dei PDS (Plant Damage States) per poter considerare la caratterizzazione di ciascuna sequenza di danno che può influenzare la risposta di contenimento o causare il rilascio di radioattività verso l'ambiente. Queste informazioni o verifiche richiedono (su indirizzo della Linea guida) che siano precisate le seguenti voci in rapporto alla tipologia di PDS prodotto:

- il tipo di evento iniziatore;
- il guasto del sistema di sicurezza (sistema di protezione, sistema di rimozione del calore residuo, ECCS, nella relativa modalità di mancato intervento;
- la condizione di pressione (alta o bassa) del circuito primario al momento del danneggiamento del core;
- l'istante di tempo in cui avviene il danneggiamento del core;
- l'integrità del contenimento;
- il LOCA con o senza soppressione di pressione (per BWR);
- piscina sotto-raffreddata o satura nell'istante di tempo in cui avviene il danneggiamento del core per BWR);
- la disponibilità dei sistemi di protezione del contenimento (sistemi di rimozione del calore e di ricombinazione dell'idrogeno);
- la disponibilità degli AC/DC di potenza e il tempo di ripristino;
- le azioni operative che sono state adottate e che sono fallite.

La valutazione delle sequenze con possibile danneggiamento è normalmente il risultato dello sforzo congiunto delle analisi di PSA di livello 1 e 2. Gli aspetti di affidabilità riferiti alle tipologie dei PDS possono essere approcciati in vario modo. Uno di questi consiste nel considerare l'affidabilità dei sistemi di contenimento direttamente negli Alberi degli eventi di livello 1 in modo da collegare gli Alberi di guasto di tali sistemi e poter considerare gli inevitabili effetti di dipendenze per la valutazione complessiva dei PDS.

3.3.3 Analisi dei sistemi

Il passo successivo consiste nel modellare i guasti dei sistemi identificati mediante analisi con Alberi degli eventi. Tale modellizzazine viene condotta mediante Alberi di guasto dove il Top-event è lo stato (o gli stati) di fallimento del sistema considerato. L'analisi mediante Alberi di guasto si estende fino ad individuare gli eventi singoli di base che in genere includono i guasti o l'indisponibilità di componenti durante il periodo di manutenzione o di test, le cause comuni di guasto di componenti in configurazione ridondata e gli errori operativi.

Fault tree analysis

I revisori devono verificare che gli Alberi di guasto siano stati sviluppati per lo stato di guasto di ciascun sistema di sicurezza identificato mediante la precedente analisi con Alberi degli eventi.

Si richiede che il set degli eventi base da inserire nel modello degli Alberi di guasto, va identificato mediante una analisi sistematica ad esempio mediante metodologia FMEA, che può essere condotta in fase di progetto proprio per identificare le modalità di guasto dei componenti più importanti, e mediante una revisione degli interventi operativi per identificare i potenziali errori.

L'analisi deve inoltre comprendere i componenti passivi i cui guasti possono condurre al guasto del sistema stesso (ad esempio, blocco dei filtri non rilevato, perdita da condotta, ecc).

L'analisi mediante Alberi dei guasti deve inoltre identificare le dipendenze hardware e funzionali, e le interdipendenze tra i sistemi in modo da poter valutare le possibili cause di incidenti significativi.

L'analisi degli Alberi di guasto costituisce uno degli aspetti analitici più ricchi di elementi e di particolarità, anche in rapporto ai possibili errori operativi, per diverse tipologie di reattore, spesso non considerati e che pertanto richiedono una attenzione particolare in sede di revisione.

3.3.4 Analisi delle dipendenze

La Linea guida segnala che nei passati PSA è risultato particolarmente rilevante il contributo dei "guasti dipendenti" alla frequenza di danneggiamento del core. Le differenti tipologie di dipendenza che possono verificarsi sono le seguenti:

- dipendenze funzionali;
- dipendenze fisiche;

- interazioni umane;
- dipendenze tra guasti di componenti.

Le dipendenze funzionali possono sorgere quando il funzionamento di del sistema o di un gruppo di componenti dipende dal funzionamento di un altro sistema o di altri componenti. Queste dipendenze sono dovute a diversi motivi: sistemi con attuazione comune, requisiti di isolamento comune, sistemi di supporto comuni, ecc.

Le dipendenze fisiche possono insorgere per due motivi:

1. un evento iniziatore può causare il guasto di un sistema di sicurezza o di un componente che a sua volta provoca il guasto di altri sistemi di sicurezza o di altri componenti con funzioni protettive;
2. un pericolo interno (incendio) o esterno (evento sismico) possono causare un evento iniziatore grave (un transient o LOCA) ed insieme il guasto di altri sistemi di sicurezza o componenti con funzioni protettive.

Le interazioni umane (operative) nascono soprattutto quando gli operatori commettono errori durante gli interventi di riparazione, manutenzione, testing e calibrazione che conducono a guasti o indisponibilità di sistemi di sicurezza.

Le dipendenze tra guasti di componenti si riferiscono a tutti quei guasti di componenti identici che non sarebbero altrimenti analizzati. Questi guasti possono essere causati da errori umani in fase di progettazione, costruzione, istallazione e calibrazione.

I revisori, pertanto, devono verificare se è stata condotta un'analisi sistematica per identificare potenziali dipendenze che possono ridurre l'affidabilità dei sistemi di sicurezza o dei componenti con funzioni protettive.

3.3.5 Analisi dei sistemi passivi, componenti e strutture

Nel progetto degli attuali reattori c'è la tendenza ad incorporare, nello sviluppo delle "safety functions", i sistemi di sicurezza passivi quali il sistema di rimozione del calore e il sistema di raffreddamento di emergenza del core. Il PSA deve tener conto dell'affidabilità dei sistemi passivi nella stessa misura in cui tiene in considerazione i sistemi attivi. Particolare attenzione va rivolta a tutti quei guasti che coinvolgono strutture o componenti passivi come, ad esempio, le condotte ad alta energia e i vessel.

3.3.6 Approccio all'affidabilità umana (Human Reliability Assessment)

Una parte importante del PSA è la valutazione dell'affidabilità umana (HRA) e in particolare l'organizzazione delle attività necessarie ad effettuare tale valutazione. Queste attività includono l'identificazione delle azioni umane da considerare, l'inserimento di tali azioni in un modello logico (Albero degli eventi e Albero dei guasti) e la quantificazione degli eventi connessi.

I revisori dovranno verificare che la HRA sia stata elaborata coerentemente e che tutte le fasi dell'analisi siano state documentate in modo tracciabile. Ciò è

particolarmente importante, poiché esiste una vasta gamma di metodologie utilizzate per la valutazione dell'affidabilità umana e perché lo stato dell'arte in questo campo è ancora in fase di evoluzione.

La procedura HRA generalmente usata include:

- l'identificazione delle interazioni umane (interventi operativi);
- la definizione di importanza degli interventi operativi;
- l'inserimento delle azioni umane nel modello analitico/logico;
- la selezione del metodo HRA appropriato;
- la quantificazione degli eventi di intervento operativo;
- la documentazione dell'analisi sviluppata.

Le interazioni umane (o interventi operativi) sono classificati come segue:

- Tipo A - intervento operativo effettuato prima che l'evento iniziatore comprometta il sistema o la disponibilità del componente;
- Tipo B - intervento operativo che causa l'evento iniziatore;
- Tipo C - intervento operativo che viene effettuato in risposta ad un evento iniziatore.

Come guida sugli aspetti organizzativi e metodologicio per l'elaborazione della HRA è suggerita la procedura SHARP (Systematic Human Action Reliability Procedure).

E' sufficiente che i revisori confrontino il processo HRA usato nel PSA con la procedura SHARP per verificare che tutti i passi successivi siano stati considerati. Più in generale, i revisori devono verificare che i metodi specifici e le tecniche usate per il PSA siano appropriati e correttamente applicati rispetto al metodo HRA scelto e con completezza rispetto a ciascuna sequenza di eventi.

3.3.7 Dati richiesti per il PSA

La Linea guida indica le tipologie di base per i dati richiesti, le cui fonti devono essere adeguatamente documentate:

- frequenza degli eventi iniziatori;
- probabilità di guasto dei componenti;
- frequenza e durata del fuori servizio di componenti.

I dati richiesti per le probabilità di causa comune di guasto e le probabilità di errore umano sono riprese e discusse dalla Linea guida in una sezione indipendente (§3.4 e §3.5).

Uno degli aspetti più critici dei dati richiesti per il PSA riguardano la loro applicabilità all'impianto in questione, ai suoi componenti particolari e al regime d'esercizio praticato. Spesso sono disponibili e applicabili moltissimi dati generici; gli analisti non avranno che da scegliere tra le migliori fonti per

ciascun caso. Ovviamente i dati specifici di impianto sono da preferire ai dati generici. Purtroppo, anche per impianti che hanno operato per un certo numero di anni, i dati specifici di impianto risultano piuttosto limitati e devono essere combinati in qualche modo con i dati generici.

Per ciascuna tipologia di guasto la Linea guida fornisce ai revisori un indirizzo valutativo considerando l'opportunità dell'uso dei dati specifici di impianto, purchè supportati da una operatività di riferimento maggiore di qualche anno.

3.3.8 Analisi dei sistemi computerizzati

L'utilizzo sempre più esteso di "sistemi computerizzati " (Computer based system o Software based system) per le funzioni di controllo e di protezione, in luogo dei "sistemi cablati" (Hard wired system), pone nuove problematiche da affrontare nelle valutazioni di affidabilità e di sicurezza di impianti nucleari e nella loro revisione.

Le valutazioni di affidabilità di sistemi cablati è in generale basata sull'assunzione che analisi deterministiche e attività di testing adeguate siano tali da assicurare l'assenza di errori di progettazione; le frequenze di guasto sono pertanto dominate da malfunzionamenti hardware di natura casuale, eventualmente dovuti a cause comuni.

Il principale problema posto dall'utilizzo di sistemi computerizzati riguarda l'elevato numero e possibilità di combinazione degli input acquisiti dai sensori installati nell'impianto, che riducono la confidenza sulla completezza ed esaustività delle attività di testing.

Allo stato dell'arte, occorre riconoscere l'impossibilità di valutare una frequenza di guasto associata ad errori software e la necessità di giungere ad un giudizio complessivo di affidabilità sulla base delle specificità del sistema e delle modalità di esecuzione delle attività di progettazione, verifica e validazione.

Non essendo possibile garantire l'assenza di errori nei codici software di sistemi computerizzati, l'enfasi è rivolta alla qualità dei processi di progettazione e produzione e delle procedure adottate nelle attività di verifica del codice (static analysis) e di test (dynamic testing), che devono essere tali da massimizzare la probabilità di rilevazione di errori e minimizzare la probabilità di errori latenti.

Occorre inoltre distinguere tra errori pericolosi, in quanto potenzialmente causa della mancata o non errata esecuzione delle funzioni di sicurezza, ed errori che non hanno impatto sulla sicurezza dell'impianto. A tal fine è buona pratica mantenere separate le risorse destinate alla implementazione delle funzioni di sicurezza e delle restanti funzioni, concentrando le attività di verifica e testing sulle prime.

Per le valutazioni di affidabilità di sistemi computerizzati si procede in modo analogo a quanto fatto per i sistemi convenzionali, mediante una loro decomposizione in sottosistemi deputati alla esecuzione di funzionalità elementari; tale approccio permette di rivolgere le attività di verifica e testing su parti di minore complessità e indagare specificatamente le interfacce che tra queste intercorrono.

La stima dell'affidabilità di sistemi computerizzati deve includere le valutazioni dedicate ai guasti hardware indipendenti e dovuti a cause comuni. Se il sistema implementa ridondanze e misure di indipendenza opportune, si attende una probabilità di guasto relativamente bassa, circa un ordine di grandezza inferiore al contributo atteso dagli errori software non rilevati. Indicativamente, valori di probabilità di guasto (su chiamata) per malfunzionamenti hardware maggiori di 10^{-5} dovrebbero sollecitare i revisori ad una indagine in dettaglio su possibili debolezze del progetto o delle analisi probabilistiche; valori di probabilità di guasto (su chiamata) per malfunzionamenti software molto minori a 10^{-4} dovrebbero sollecitare i revisori ad una indagine in dettaglio sull'adeguatezza delle valutazioni.

Il giudizio sull'affidabilità del software e sul suo contributo alla probabilità di guasto complessiva dovrebbe tener conto delle seguenti caratteristiche:

- dimensione e complessità del sistema (ad esempio, con riferimento al numero di linee di codice);
- livello di innovazione del sistema;
- funzionalità implementate e relativo impatto sulla sicurezza dell'esercizio;
- conformità alle procedure ed agli standard applicabili in merito alle attività di progettazione, produzione, verifica e testing;
- esperienza del personale coinvolto nella progettazione e indipendenza con il personale in carico delle attività di verifica e testing;
- utilizzo di strumenti e metodi formali per le attività di verifica e numero di test realizzati;
- numero di errori identificati nelle attività di verifica e testing.

Un aspetto di particolare rilevanza riguarda l'indipendenza tra i sistemi deputati alla implementazione delle funzioni di controllo e delle funzioni di protezione dell'impianto e, in entrambi i casi, tra i sistemi predisposti in configurazione ridondata. Una completa indipendenza può essere assunta solo in presenza di una completa "diversity", quale quella dovuta all'utilizzo di un sistema computerizzato e di un sistema cablato.

Nel caso in cui le funzioni di controllo e di protezione siano entrambe realizzate da sistemi computerizzati, occorre tener conto nelle analisi probabilistiche (mediante Alberi degli eventi) delle possibili dipendenze per le quali un errore software potrebbe comportare l'occorrenza di un evento iniziatore (errore di controllo) ed il mancato intervento dei sistemi di protezione. Un discorso analogo è applicabile nella valutazione dell'affidabilità di sistemi in configurazione ridondata. In tal caso le misure di diversity che dovrebbero essere utilizzate riguardano, per esempio, l'indipendenza tra i team di sviluppo, l'utilizzo di differenti linguaggi di programmazione software e di differenti fornitori dell'hardware.

Da quanto detto emerge la presenza di incertezze significative sulle probabilità di guasto assegnate a sistemi computerizzati e sulle dipendenze esistenti tra diversi sistemi installati nel medesimo impianto. E' pertanto necessario procedere ad un adeguato studio di sensitività dei risultati del PSA.

Infine, si evidenzia la maggiore vulnerabilità dei sistemi computerizzati alle condizioni ambientali ed alle interferenze elettromagnetiche, rispetto a sistemi cablati. L'analisi probabilistica del rischio dovrebbe includere tali aspetti con un livello di dettaglio da definire in relazione alla presumibile adeguatezza delle attività di test (prove climatiche e prove di compatibilità elettromagnetica) e delle procedure operative (ad esempio, per prevenire l'utilizzo di dispositivi mobili di comunicazione).

3.3.9 Analisi dei rischi (specifici) interni ed esterni

La presente sezione fornisce una guida per la revisione del PSA rispetto ai rischi interni ed esterni.

La Linea guida non considera in questa sede quelli che non danno contributo importante alla frequenza di danneggiamento del core e si focalizza su tre aspetti specifici - terremoto, incendi interni e allagamenti interni - tali da provocare contributi significativi al rischio.

Si ritiene che alcuni eventi pericolosi delle tipologie indicate, la loro definizione come eventi iniziatori e la valutazione quantitativa dei loro effetti sull'impianto, in termini di probabilità condizionata di danno sulle strutture, sui sistemi e sui componenti, devono costituire un'area del PSA.

Poiché tali rischi possono influenzare in modo significativo l'analisi, i revisori devono porre particolare attenzione alle modalità con cui sono stati considerati.

Per essere inserita nel PSA, la valutazione dei pericoli in oggetto parte da una lista di possibilità di evento, la più completa possibile per quanto riguarda la loro potenzialità di causare danni o perdita di difese entro l'impianto. Un riferimento importante per tale lista è costituito dalle liste presenti in "USNRC NUREG/CR-2300 PSA" (rif. [7]) in cui sono distinte nelle seguenti categorie:

- Internal hazards;
- Natural external hazards;
- Human made external hazards.

Da tali liste di pericoli si possono eliminare quelli inapplicabili al sito/impianto in oggetto, quelli a frequenza trascurabile (ad esempio, guasti interni con incidenza minimale sulle frequenze di danni al core (CDF), quelli con impatto poco significativo, ecc.).

Ciascun pericolo/rischio deve essere definito in relazione alle proprie cause specifiche ed ai parametri che rendono il loro impatto potenzialmente dannoso.

Per l'analisi di ciascun pericolo/rischio (terremoto, incendio, allagamento interno), la Linea guida introduce i passi e gli elementi che i revisori sono chiamati a considerare.

3.3.10 Quantificazione dell'Analisi

Il passo successivo della revisione è riferito alle valutazioni quantitative e finalizzate a determinare la frequenza di danneggiamento del core (CDF) e all'identificazione delle sequenze che ad esse contribuiscono.

La modalità suggerita è una valutazione (riduzione) Booleana da operare sui modelli logici sviluppati (Alberi degli eventi ed Alberi di guasto) per ciascun gruppo di eventi iniziatori.

La valutazione quantitativa risulta dai dati di frequenza e di probabilità utilizzati con cui calcolare le frequenze da associare alle sequenze incidentali. Un certo numero di codici di calcolo sono disponibili per effettuare tale valutazione.

I revisori devono verificare che il processo di quantificazione del PSA sia tecnicamente corretto e che le reciproche dipendenze siano adeguatamente considerate. Tale processo di quantificazione richiede di essere condotto con codici di calcolo che devono essere completamente valicati e verificati. Inoltre gli utilizzatori di tali codici devono dimostrare di possedere un'esperienza adeguata e di comprenderne a pieno gli usi e le limitazioni.

Una controllo particolare è richiesto per verificare che i cut sets identificati nelle sequenze portino effettivamente al danneggiamento del core. Tale controllo può essere condotto per campionatura delle sequenze che danno un contributo significativo alla quantificazione del rischio.

Nel caso siano presenti cut-off, i revisori devono verificare che essi siano stati posti a livelli sufficientemente bassi dell'analisi in modo da evitare una significativa sottostima della frequenza del danneggiamento del core.

3.3.11 Analisi di sensitività, incertezza ed importanza

Qualunque sia l'approccio seguito, il calcolo della CDF dovrebbe essere completato da uno studio di sensitività per esplorare le maggiori incertezze contenute. In aggiunta sono richieste "analisi di importanza" per identificare i gruppi più significativi di eventi iniziatori, il sistema e gli eventi base da essi prodotti che contribuiscono maggiormente al rischio.

L'Analisi di sensitività è rivolta a quegli elementi quali assunzioni poste su modelli e dati che sono sospettabili di avere potenzialmente un impatto significativo sui risultati. Queste assunzioni o dati caratterizzano generalmente le aree dove esiste una significativa carenza di informazioni che deve essere colmata dal giudizio degli analisti.

L'analisi di sensitività può essere effettuata sostituendo assunzioni alternative e valutando il loro impatto individuale sui risultati. Nel caso dei dati, è anche da dare un giudizio sul "valore peggiore possibile" che deve essere usato sulle misure di incertezza.

I revisori devono aver identificato le caratteristiche dei dati e delle assunzioni che sono candidate agli studi di sensitività a causa dell'incertezza che li caratterizza o della fiducia data ai giudizi che li sostengono.

Le assunzioni modellistiche andrebbero considerate caso per caso, dal momento in cui non compaiono tali nei risultati del PSA, ma può essere possibile usare una valutazione a campione piuttosto che ripetere l'intera valutazione del PSA.

L'Analisi di incertezza ha lo scopo di ottenere misure quantitative e valutazioni qualitative dei risultati del PSA; in particolare: la frequenza del danneggiamento

del core, la frequenza delle sequenze incidentali dominanti e le categorie considerate per le sequenze incidentali.

Le incertezze possono essere classificate in tre categorie generali riguardanti:

- l'incompletezza del modello;
- le incertezze modellistiche;
- le incertezze parametriche.

La prima categoria è valutabile considerando tutti i possibili scenari che possono condurre a conseguenze indesiderabili.

La seconda categoria rappresenta sempre un compito difficile. Essa comprende l'inadeguatezza dei modelli concettuali, dei modelli matematici, le approssimazioni numeriche, gli errori di codice ed i limiti computazionali.

La terza riguarda la scarsità o mancanza di dati attendibili per i parametri utilizzati nei modelli, la variabilità insita nei processi stocastici e le assunzioni fatte dagli esperti. L'incertezza parametrica è, ad oggi, la più quantificabile delle tre categorie e pertanto può essere considerata dai revisori come il "focus" dell'analisi delle incertezze. La base di informazioni utilizzate nella stima dei valori nominali e delle distribuzioni di probabilità, che rappresentano l'incertezza associata, è l'aspetto essenziale per assicurare la correttezza delle valutazioni.

L'Analisi di importanza è chiamata a considerare il contributo dei parametri del modello alla CDF (core damage frequency), alla frequenza delle sequenze incidentali rilevate ed alla disponibilità dei sistemi.

Tale analisi è particolarmente importante per le applicazioni del PSA a modifiche di progetto e per l'identificazione di punti deboli. L'analisi di importanza e l'analisi di sensitività sono tra loro correlate.

Esistono diverse tipologie di indici di importanza calcolati analiticamente dai codici utilizzati e riferiti a ciascun evento base.Tra questi citiamo: il Fussell-Vesely, l'indice di Birnbaum, il Risk Reduction Worth e il Risk Achievement Worths. Occorre specificare nel PSA il tipo di indice da calcolare (ci si aspetta di vedere almeno il Fussell- Vesely). I revisori potrebbero testare se i risultati dell'analisi di importanza sono in accordo con i risultati dell'analisi di sensitività e se hanno un senso logico.

3.3.12 Risultati del PSA

Ai risultati è consigliato aggiungere anche tutti i possibili contributi al rischio che non sono stati considerati.

I revisori sono generalmente dell'avviso di non accettare una presentazione dove i risultati (es. la frequenza di core-damage) lasciano al lettore l'onere di cercare tutte le relative qualificazioni, disperse in varie parti del testo del rapporto PSA.

Un'osservazione interessante suggerita dalla Linea guida si riferisce alle operazioni di "recovery" o misure della gestione incidentale, che comprendono

azioni e passi di intervento presi quando la situazione è molto oltre il "design basis" dell'impianto. Poiché tali azioni sono considerate delle agenzie con un minor livello di confidenza rispetto alle operazioni eseguite dai sistemi di sicurezza qualificati, è ritenuta buona pratica presentare i risultati del PSA tenendo conto o meno di tali azioni di ripristino e di gestione della situazione incidentale.

I risultati del PSA di livello 1 devono fornire una stima numerica del CDF e includere sufficienti informazioni per identificare i contributi principali.

Tali risultati dovranno tipicamente includere:

- le frequenza dei danneggiamenti del core (CDF);
- i contributi alla CDF di ciascun gruppo di eventi iniziatori;
- le sequenze incidentali dominanti che contribuiscono alla CDF;
- i risultati degli studi di sensitività;
- i risultati dell'analisi delle incertezze che diano i limiti di confidenza (tipicamente tra 5% e 95%) per ciascuno dei principali risultati del PSA;
- le misure di importanza riferite agli eventi base ed agli eventi associati all'intervento dei sistemi di sicurezza.

La completezza di tali informazioni dovrà naturalmente essere oggetto della verifica dei revisori, insieme ad un loro giudizio di "verosimiglianza" (plausibilità e logica) e di conseguimento di tutti gli obiettivi del PSA e della rispondenza ai requisiti di sicurezza richiesti.

La CDF dovrà essere confrontata poi con gli obiettivi probabilistici e di sicurezza dell'impianto. I risultati sono usualmente utilizzati per identificare eventuali punti di debolezza nel progetto o nell'operatività dell'impianto e per considerare i miglioramenti da apportare alle procedure attuate.

I revisori devono infine verificare che l'intero progetto e le procedure operative dell'impianto siano ben bilanciati e cioè che non esistano singole sequenze incidentali, singoli componenti o sistemi di sicurezza capaci di causare contributi troppo significativi nella valutazione di CDF, né sull'incertezza associata al rischio complessivo.

3.4 Revisione del PSA di livello 1 in condizioni di bassa potenza o di shut-down del reattore

Le condizioni operative di bassa potenza e shut down possono essere particolarmente rilevanti in quanto, come mostrato dai PSA condotti negli ultimi anni, possono indurre contributi significativi alla CDF.

Ciò è causato dal vasto campo di attività intraprese nelle due citate fasi di esercizio. La simultanea indisponibilità dei componenti e sistemi di sicurezza, l'affidabilità operativa chiamata a ristabilire le funzioni di sicurezza, una minore attenzione data in fase di progetto e in fase di operatività a tali operazioni, sono le cause di eventi iniziatori pericolosi.

Un elemento addizionale a quanto già considerato, con riferimento all'impianto a piena potenza, è dato da situazioni indicate con l'acronimo POS (Plant Operating States), in cui possono insorgere condizioni gravi di rischio.

La Linea guida rimanda alla sezione precedente di piena potenza molti argomenti di valutazione e modellizzazione, con la variante che le POS da considerare non siano solo relative al reattore ma anche ad altre condizioni capaci di produrre rilascio di materiale radioattivo. Esse sono, in particolare:

- stoccaggio del combustibile spento;
- transito del combustibile spento dal core del reattore all'impianto di stoccaggio;
- scorie radioattive presenti, ad esempio, in tanche di contenimento e negli impianti di trattamento.

Il processo analitico di base segue la linea impiegata per l'alta potenza, con ampio uso di combinazioni di Alberi degli eventi e Alberi di guasto. Tale processo, tuttavia, non è altrettanto ben consolidato come nella condizione precedente ad alta potenza.

3.5 Revisione del PSA di livello 2

Per l'identificazione dei vari passi che la guida suggerisce alle Agenzie per la revisione del PSA di livello 2 (in condizioni operative a piena potenza) si consiglia un approccio preliminare che rivisita l'analisi a livello 1 e considera scopi ed obiettivi dell'analisi del PSA di livello 2.

Tale percorso sviluppa nel suo insieme il modello probabilistico dell'analisi dei PSA.

L'analisi di livello 1, infatti, tende a raggruppare gli eventi iniziatori ed a considerare le relative sequenze incidentali, in particolare quelle capaci di creare danni al core (severe accidents).

Segue la quantificazione delle sequenze identificate, che coinvolge un'analisi deterministica ed il giudizio di esperti (ove necessario), con la valutazione delle incertezze che danno effetti su fenomeni incidentali severi nella modalità in cui possono accadere.

L'analisi può focalizzare in particolare l'incidente più severo (massimo incidente credibile), sia intermini di frequenze (CDF), che di caratterizzazione delle reattività rilasciate all'ambiente (Source term). Ciò investe, naturalmente, l'analisi PSA di livello 2.

La revisione del processo di livello 2 si sviluppa secondo i seguenti passi:

- Familiarizzazione con i dati di impianto e sistemi;
- Interfaccia tra il livello 1 e il livello 2 del PSA (secondo quanto sopra indicato);
- Analisi dell'efficacia del contenimento;

- Sviluppo del modello probabilistico relativo allo sviluppo delle sequenze incidentali;
- Quantificazione della capacità di contenimento (event trees);
- Caratterizzazione dei source term di rilascio radiologico;
- Risultati del PSA di livello 2;
- Audit del PSA di livello 2 – Q.As.

3.5.1 Familiarizzazione con i dati ed i sistemi dell'impianto

Questo primo task ha lo scopo di rendere i revisori familiari col progetto e con la sua operatività ed in particolare con la risposta con gli eventi (phenomena) che possono capitare durante un incidente grave (severe accident).

Pertanto i revisori devono acquistare particolare dimestichezza con il progetto ed il funzionamento dei sistemi che devono intervenire durante un "severe accident", per mitigare le conseguenze. Particolare attenzione dovrà essere posta alle caratteristiche del contenimento che possono indurre (se mancanti o difettose) una progressione dannosa dell'evento e produrre potenziali vulnerabilità.

Le informazioni richieste sono:

- la documentazione di progetto dei "safety systems" e dei "containment systems";
- l'efficacia (capacity) dei sistemi, i limiti operativi ed i criteri di attenuazione;
- i sistemi ausiliari richiesti per l'operazione.

I sistemi rilevanti per le eventuali conseguenze di un "severe accident" sono:

- Sistemi di controllo della reattività qauli:
  - "broken system";
  - Moderator system (dipendenti dal tipo di reattore, es. per i reattori tipo Candu);
- Sistemi per il raffreddamento del core quali:
  - ECCS di alta e bassa pressione;
  - Accumulatori (per reattori PWR);
  - Sistemi di rimozione del calore dal reattore a lungo termine (long term);
  - Sviluppi alternativi ed iniezione (Injection System);
- Sistemi di contenimento quali:
  - Sistemi di contenimento ed isolamento;

- Sistemi e bypass di contenimento (Es. sistemi di interfaccia fra alta e bassa pressione, led-down lines/PWR);
- Spray di contenimento;
- Raffreddatori ad aria per contenimento (containment fan coolers);
- Sistemi di controllo dell'idrogeno;
- Sistemi di rimozione del calore a lungo termine;
- Sistemi di "venting" per contenimenti (filtrato);
- Sistemi ad iniezione per contenimento alternativo (sistemi di ventilazione del reactor-building/BWR);

▪ Altri sistemi quali:

- Sistemi di raffreddamento (RCS), sistemi di depressurizzazione;
- Altri sistemi per bypass di contenimento.

Se l'analisi dei sistemi di contenimento è considerata parte del PSA di livello 2, le procedure di verifica sono le stesse indicate nel documento IAEA-TECE-DOC-1229 (rif.[3]) dove le dipendenze dei sistemi sono considerate di massima importanza.

Inoltre, il PSA di livello 2, deve modellare gli interventi operativi "post-core damage" atti a mitigare lo sviluppo/conseguenze delle sequenze di un "severe accident2"

Il PSA di livello 2 deve anche considerare l'intervento automatico dei sistemi al variare delle condizioni fisiche durante l'evoluzione di un incidente dopo il danneggiamento del core. Ad esempio gli ECCS, se disponibili, possono essere attuati qualora durante il transitorio ad alta pressione qualche meccanismo causa la depressurizzazione del sistema primario.

Plant and containment data

Un modo realmente pratico per raggiungere una comprensione generale delle caratteristiche d'impianto è di confrontare i dati e parametri tecnici operativi di base del reattore in esame, con quelli di uno della stesa tipologia e simile configurazione. Tale confronto può fornire una prima indicazione delle vulnerabilità fisiche che inducono "severe accidents" e orientare i revisori nelle verifiche di livello 2.

Le prestazioni caratteristiche dell'impianto e del contenimento che possono influenzare lo sviluppo di un "severe accident" includono aree, sistemi e parametri tipici ripresi della Linea Guida SRS No.25 (rif.[6]) ai quali, per semplicità, si rimanda.

[2] I termini "incidente severo" e "severe accident" sono da considerare equivalenti, usando il secondo per non confonderlo con il termine di evento incidentale.

3.5.2 Interfaccia tra il Livello 1 ed il Livello 2

L'interfaccia tra le verifiche a PSA di livello 1 e quelle a PSA di livello 2 è usualmente effettuata definendo lo stato di danno dell'impianto (PDS:Plant damage state) che fornisce le condizioni iniziali e le condizioni di contorno (boundering) per l'analisi di un "severe accident". L'analisi può partire dal livello 1 ed essere estesa ai sistemi di contenimento, benché tali sistemi siano considerati nella loro globalità nell'analisi di livello 2.

A PSA di livello 2 sono identificati, in particolare, gli interventi operativi "post core damage" quali definiti dalle valutazioni dei PDS di cui sopra.

Raggruppamento dei PDS

L'obiettivo dell'analisi dei PDS è di combinare la sequenza degli eventi tratta dall'analisi a livello 1 e che risultino in progressioni simili del corrispondente incidente severo, presentino simili sollecitazioni al contenimento ed abbiano la stessa potenzialità di rilascio radioattivo all'ambiente. Operando in tal modo, il numero di condizioni accidentali che che devono essere considerate risulta di molto ridotto.

Per esempio, un PSA di livello 1 utilizza diversi modelli di Alberi di evento per considerare possibili danni al core a seguito di uno spegnimento spurio del reattore (reactor spurious trip) causato da perdite di acqua d'alimentazione (feed water). Tuttavia, dal punto di vista della risposta del contenimento, il raggruppamento di sequenze può essere simile a quello sopra descritto e perciò combinato a PSA di livello 2.

Occorre però osservare che in altri casi le sequenze di livello 1 possano essere suddivise in diversi PDS (piuttosto che combinate), ad esempio perché a livello 1 non sono stati considerati Alberi degli eventi relativi ad interventi operativi richiesti dal contenimento.

Tipici criteri di raggruppamento usati per reattori ad acqua leggera, includono:

- il top di evento iniziatore (es. LOCA);
- lo stato dei sistemi di sicurezza (nei loro diversi obiettivi funzionali);
- la disponibilità dell'alimentazione elettrica (AC, DC);
- la pressione del circuito primario (alta o bassa) in caso di danneggiamento del core;
- lo stato dei sistemi di riduzione della pressione (RCS) quali il sistema automatico di depressurizzazione, etc.;
- i tempi ai quali si manifesta il danneggiamento del core rispetto allo "scram del reattore" ;
- lo stato di integrità del contenimento (intatto, fessurato, con tenuta difettosa, etc.);
- lo stato del sistema di soppressione ("Suppression System") nel momento di danneggiamento del core;

- l'affidabilità dei sistemi di protezione del contenimento (containment spray, heat removal system, etc).

I revisori devono essere consapevoli del fatto che per molte sequenze accidentali, lo stato di particolari sistemi può non essere noto fin dal livello 1 e considerato nei modelli utilizzati nel PSA di livello 1.

Per esempio i criteri di successo contro un LOCA con larga rottura può richiedere che almeno uno degli accumulatori (PWR) funzioni, per prevenire un danneggiamento del core.

In conclusione i revisori dovrebbero essere soddisfatti se i modelli del livello 1 sono stati estesi per includere lo stato dei sistemi non normalmente considerati in modo completo a quel livello, ma importanti per il PSA di livello 2 e quindi includendo le definizioni di PDS.

Gli interventi gestionali che devono essere definiti dopo un evento di danneggiamento includono:

- la depressurizzazione del sistema primario;
- l'avvio di sistemi alternativi di iniezione nel core;
- l'allagamento del contenimento;
- l'allagamento della cavità del reattore;
- il venting del contenimento;
- il venting del "reactor pressure vessel" (BWR);
- il riempimento degli steam generators (PWR);
- l'attuazione dei sistemi di controlo-idrogeno;
- l'attuazione degli spray di contenimento dei sistemi alternativi di iniezione.

Analisi e quantificazione dei PDS

Le caratteristiche di disponibilità dei sistemi, in relazione alle varie definizioni dei PDS, possono essere introdotte nel modello di valutazione del rischio mediante diversi metodi.

Uno primo metodo consiste nell'estensione degli Alberi degli evento di livello 1 fino ad includere la disponibilità dei sistemi di contenimento, in modo che i rispettivi Alberi di guasto possano essere collegati e le corrispondenti dipendenze prese in conto nella valutazione.

Un secondo metodo consiste nel considerare un modello comprendente tutti i sistemi in un unico Albero degli eventi con contenimento (livello 2) avendo cura di assicurare che le correlazioni con le sequenze di livello 1, come le dipendenze dai sistemi ausiliari di supporto, siano mantenute;

Un terzo metodo consiste nell'utilizzare un programma computerizzato che raccolga le informazioni delle equazioni dei cut-set degli Alberi d'evento sviluppati a livello 1, crei i collegamenti negli Alberi di guasto con i sistemi di contenimento e, nel caso, con i sistemi di gestione, realizzando in sostanza

un'estensione degli Alberi di livello 1 (Alberi-fonte). Tale programma può tener conto dei raggruppamenti per sequenze in accordo con le definizioni dei PDS.

E' bene notare che i contenuti dell'analisi sono identici, variando gli aspetti applicativi dei metodi, con un massimo di coordinamento e completezza nella realizzazione ed utilizzo dell'ultimo programma sinteticamente descritto.

Sono richieste, inoltre, analisi relative alla quantificazione dell'affidabilità negli interventi operativi post-danneggiamento. La valutazione delle probabilità di errore umano associato a tali interventi richiede una revisione specifica. In particolare la valutazione della HEP deve tener conto delle "prior performances" e delle conseguenti dipendenze, dei livelli di stress del personale, delle incertezze sulla disponibilità delle informazioni e dei segnali nello stato di un severe accident.

Il livello 2 deve considerare le possibilità di errore umano tenendo conto delle condizioni severe dell'impianto.
I revisori devono verificare che sono stati presi in considerazione gli aspetti più critici riguardanti:

- le dipendenze da precedenti errori umani a livello 1;
- il guasto di sistemi (strumentazione) che possano rendere inattuabili azioni a livello 2;
- le difficoltà di accesso in locali dove dovrebbero essere attuate azioni di gestione dell'incidente;
- un alto livello di stress (e workload).

Risultati dell'analisi dei PDS

I revisori devono verificare che tutte le sequenze con danneggiamento di core fanno capo ad una PDS (ad una condizione di danno d'impianto) e che la somma delle frequenze associate a ciascun PDS è approssimativamente pari alla frequenza totale di "core damage".

In alcuni PSA le sequenze d'evento con frequenze molto basse sono ignorate nel raggruppamento per PDS. In generale i revisori dovrebbero verificare che:

- la frequenza complessiva delle sequenze incidentali sotto il valore di cut-off sia una frazione piccola della frequenza totale di core damage (ad esempio, meno del 1%);
- le sequenze incidentali che potrebbero determinare conseguenze gravi (es. sequenze di bypass di contenimento, incidenti con rotture di tubi generatori di vapore, etc) non siano sistematicamente rimosse nel processo di valutazione dei PDS.

3.5.3 Modelli di percorsi (progressioni) incidentali

L'analisi deterministica del comportamento del reattore e del contenimento durante definite sequenze incidentali rappresenta la principale base per una quantificazione fenomenologica delle probabilità di accadimento di eventi, in sede di analisi di livello 2.

Il contesto probabilistico del PSA di livello 2, quale illustrato nel seguito, è il meccanismo per delineare e quantificare le incertezze sulle analisi deterministiche degli incidenti severi (severe accident).

Gli aspetti riguardanti i modelli di valutazione deterministica del comportamento dell'impianto sono vari, ma hanno in comune l'utilizzo di specifici codici di calcolo, il confronto tra i risultati ottenuti da codici diversi, il confronto con i dati sperimentali disponibili ed i modelli dei dati di ingresso.

Le tematiche principali affrontate dai codici di calcolo includono:

a) la risposta termodinamica del sistema di raffreddamento del reattore;

b) la valutazione del sovra-riscaldamento del core (core heat-up), della degradazione del combustibile e della riallocazione del materiale entro il vessel del reattore;

c) la rottura (fessurazione, etc) del "pressure boudering" del vessel del reattore e conseguente il rilascio di combustibile fuso e frammenti di core (debris);

d) l'interazione termica e chimica tra frammenti di core e la struttura di contenimento, la pavimentazione, le piscine d'acqua, etc.

e) il comportamento del contenimento (incluso l'andamento temporale pressione/temperatura), il mixing con idrogeno e l'effetto dell'operatività dei sistemi di retroguardia del contenimento.

La Linea guida fornisce indicazioni su codici di calcolo utilizzati più comunemente: MAAP, MELCOR, ESCARE e THALES.

Spesso gli obiettivi generici di questi codici ed i requisiti che tali calcoli richiedono possono essere completati in tempi brevi operando opportune semplificazioni dei modelli evoluti altrimenti utilizzabili.

Esempi di tali semplificazioni riguardano l'utilizzo di parametri "complessivi" sul trasporto di materia e di equazioni termodinamiche conservative, nonché l'uso di correlazioni empiriche per processi fisici complessi.

I revisori dovrebbero essere informati delle aree in cui sono stati introdotte tali semplificazioni e valutare se sono stati presi in considerazione gli effetti relativi.

I revisori dovrebbero essere soddisfatti se i fenomeni relativi ai comportamenti delle sequenze accidentali importanti sono stati approssimati in un'ottica di "plant specific analysis", applicando informazioni ricavate da altre fonti credibili e rilevanti, come dati sperimentali o referenze di "plant analysis".

Le tematiche sopra riportate sono in ogni caso, con sviluppi di dettaglio di volta in volta specifici, le linee d'analisi principali comunemente seguite.

Model input data

I dati d'ingresso, provenienti da fonti diverse, sono necessari –a livello qualitativo e quantitativo adeguati- per l'analisi degli eventi severi. La Linea guida sviluppa l'identificazione dei dati principali, articolandoli nelle seguenti aree:

- dati specifici usati per rappresentare l'impianto (nelle condizioni incidentali);
- volume totale di acqua nel sistema di raffreddamento del reattore (RCS) e nel lato secondario (freddo) presente nei generatori di vapore;
- volumi dei vari compartimenti del contenimento e modalità di collegamento tra loro;
- tipi di calcestruzzo utilizzato nella costruzione del contenimento;
- schema spaziale di strutturazione nodale relativa alla modellazione dell'impianto.

In particolare dovrà essere esaminato il livello di dettaglio usato per sviluppare il modello termodinamico nodale (incluso RCS, lo schema di nodalizzazione del contenimento e delle strutture del core).

I dati di input per l'analisi degli scenari accidentali includono:

- le aree di perdita e loro localizzazione;
- le specifiche funzionali della strumentazione e dei sistemi (es numero di gruppi operativi (trains) e portate attivate);
- i tempi di intervento delle azioni operative.

Dati di input per i modelli relativi ai fenomeni accidentali

E' segnalata la necessità della conformità tra le diverse valutazioni sviluppate nell'ambito del modello (e tra i relativi dati di input), dedicate ai diversi fenomeni compresi nell'evoluzione degli scenari incidentali. Fanno naturalmente eccezione i calcoli di sensitività effettuati con l'esplicito scopo di caratterizzare l'effetto di modelli alternativi credibili nell'ambito delle valutazioni di incertezza.

Risultati del PSA di livello 2

E' riconosciuto non praticabile l'esame dei dettagli di ciascuno dei calcoli eseguiti in relazione al PSA di livello 2.

I revisori dovrebbero essere soddisfatti che i risultati fossero, in termini generali, consistenti con le analisi condotte su impianti similari. Si rimanda su questo punto all'insieme dei numerosi dati di letteratura contenuti nei rapporti di dettaglio riguardanti calcoli sugli incidenti severi, effettuati con vari codici di calcolo e riferiti alle sequenze incidentali comunemente individuate nelle analisi di livello 2.

Pur riconoscendo che tutti i calcoli ingegneristici contengono varie forme di incertezza, non è definita una modalità rigorosa di trattamento per quanto attiene il PSA di livello 2.

La revisione può tuttavia essere fatta considerando su singole tematiche la "structured sensitivity studies" o altri approcci similari. Le tematiche affrontate con tale analisi di sensitività strutturali sono indicate nella Linea guida ripartiti per:

- "In vessel accident phenomena";
- "Ex vessel core/debris phenomena";

- “Containment performance”;
- “Containment phenomena”;
- “Effect of operative actions”.

3.5.4 Containment performance analysis

I fenomeni prodotti dagli incidenti severi identificati dall’analisi sono costituiti principalmente da alta pressione ed alta temperatura all’interno del contenimento. Lo scopo dell’analisi in oggetto è di valutare se il contenimento può essere capace di sopportare i carichi derivanti da:

- Transitori rapidi di pressurizzazione, maggiori di quelli ipotizzati nelle condizioni nominali di progetto;
- alte temperature;
- erosione termo-meccanica del calcestruzzo e nelle strutture in acciaio;
- impatto con missili generati all’interno;
- carichi dinamici localizzati, quali le “shock waves”.

3.5.5 Inquadramento della modellizzazione probabilistica

Questa parte del PSA di livello 2 è finalizzata a fornire un inquadramento strutturato che descriva le evoluzioni alternative a partire da un certo PDS. Questo inquadramento, indicato con il termine CET (Containment Event Trees), parte dalla valutazioni di PSA di livello 2 e richiede di essere rivista interamente.

La struttura è articolata nei seguenti passi, tenendo conto che fenomeni intensi possono essere generati in rapporto alla natura ed intensità di impatto con l’integrità del contenimento e col rilascio e dispersione di radionuclidi, quali una situazione incidentale può produrre.

Sono indicati gli intervalli temporali da considerare:

- dopo l’evento iniziatore, ma prima del danneggiamento del core (è un tempo che stabilisce le condizioni iniziali per la risposta del contenimento);
- dopo l’inizio del danneggiamento del core, ma prima della fessurazione del Vessel;
- immediatamente dopo la fessurazione del vessel;
- andamento a lungo termine.

La probabilità associata agli eventi di un CET sono almeno di due tipi. Uno rappresenta la probabilità condizionata che un sistema riesca ad operare o fallisca in seguito ad una richiesta di intervento, o che l’operatore effettui o fallisca una specifica azione; queste probabilità sono trattate con Alberi di evento in modo analogo a quanto sviluppato per il PSA di livello 1. L’altro tipo di probabilità rappresenta l’incertezza associata all’accadimento o all’effetto dei fenomeni costituenti il “severe accident”.

E' importante verificare che tale distinzione sia stata fatta e trattata convenientemente, anche mediante il confronto con situazioni sperimentate o altrimenti valutate. Un esempio tipico di incertezza è applicato alla valutazione della massa totale di idrogeno generato durante il degrado del core, che può essere coinvolto in una combustione all'interno del contenimento. Se la massa è elevata, tale evento può compromettere seriamente la capacità di contenimento.

In sede di revisione della PSA, è importante verificare che siano distinte le situazioni relative ad una perdita di contenimento dovuta ad una larga combustione e ad un rilascio di idrogeno in un primo (breve) periodo di tempo che non deve precludere la capacità di contenimento.

Presentazione dei risultati

Il numero totale dei "severe accidents" singolarmente considerati e rappresentati a livello 2 può essere elevato. Conseguentemente, è spesso applicata una logica di raggruppamento per determinare la frequenza relativa ad aggregati di sviluppi incidentali aventi comuni caratteristiche. Queste caratteristiche possono comprendere tempi e/o modi di perdita di contenimento, azioni umane/manuali atte a limitare/portare a termine il danneggiamento del core, sistemi ingegneristici di mitigazione (salvaguardia). Se queste caratteristiche sono selezionate appropriatamente, gli sviluppi incidentali possono essere raggruppati in modo da ammettere una comune fonte di prodotti di fissione a cui riferirsi.

I maggiori contributi alle differenti modalità di perdita di contenimento devono essere evidenziati e descritti.

I risultati devono essere presentati sia in termini di frequenza globale ai vari livelli di capacità di contenimento, sia in termini di probabilità condizionata che porta a danneggiamento del core.

Usualmente sia le alte o basse probabilità di mantenimento del contenimento, come i più importanti modi di perdita, devono essere tracciabili con l'analisi deterministica degli sviluppi incidentali.

3.5.6 Quantificazione dei Containment Event Trees (CET)

I revisori dovrebbero verificare l'adeguatezza dei metodi e delle basi tecniche utilizzate per definire le probabilità dei singoli eventi nella quantificazione del CET.

Le basi tecniche usate per quantificare gli eventi devono essere esaminate attentamente per assicurare la tracciabilità dei dati e garantire che le probabilità da esse generate presentino una caratterizzazione imparziale nell'andamento incidentale.

Vari approcci sono utilizzabili per trasformare le evidenze tecniche relative alla tenuta del contenimento in una stima di probabilità di perdita. La Linea guida suggerisce alcuni metodi più frequentemente usati:

- il giudizio degli esperti;

- il calcolo della probabilità condizionata di perdita, per una certa sequenza incidentale, come convoluzione di due funzioni di densità.

Le funzioni di densità di probabilità sono sviluppate cercando di rappresentare la distribuzione di valori credibili per un parametro interessato (ad esempio, carico di pressione sul contenimento) e per i corrispondenti criteri di cedimento (ad esempio, capacità limite di resistenza a pressione). La base per sviluppare queste distribuzioni è un set collettivo di informazioni generate da codici di calcolo e dai corrispondenti calcoli di sensitività, relative alle caratteristiche specifiche dell'impianto.

E' importante che i revisori possano accertare che l'approccio adottato conduca ad una adeguata tracciabilità tra la probabilità stimata e la qualità dei dati di supporto (da codici di calcolo, verifiche, dati sperimentali).

I "Metodi di decomposizione" possono essere utilizzati per la valutazione della resistenza ai carichi, in alternativa ai due metodi sopra indicati.

L'idea di base è di disaggregare (break down) un'operazione generale, del tipo "fallisce il contenimento per una combustione di idrogeno?", in una sequenza o set di sequenze che possono essere più facilmente analizzate. Per esempio il problema precedente può essere disaggregato nel seguente modo:

a) quanto idrogeno è generato?"

b) qual è la pressione dell'idrogeno bruciato?"

c) qual è la probabilità che il contenimento ceda dietro un aumento della pressione dovuto ad a/b?

Questa decomposizione è spesso sviluppata mediante il ricorso ad Alberi degli eventi.

Le questioni poste nelle decomposizione sono scelte in modo che sia più facile riferirle ad informazioni tratte da esperimenti (prove) o da metodi di calcolo. La Linea guida suggerisce tuttavia una certa prudenza nell'utilizzo del Metodo della decomposizione ed afferma che la maggior parte delle analisi a livello 2 utilizza un approccio "misto" dei tre metodi precedentemente descritti. Un'interpretazione significativa dei risultati deve tenere conto che i risultati possono essere pesantemente influenzati da valori soggettivi per la probabilità, nel caso di eventi poco probabili.

Sintetizzando, il giudizio sull'analisi del contenimento ed in particolare sugli Alberi degli evento del contenimento (CET) può avvalersi di varie fonti (mediamente) affidabili:

- il calcolo con codici di calcolo dell'andamento incidentale (severe accidents);
- l'interpolazione di risultati di codici diversi;
- l'applicazione di esperimenti rilevanti;
- i calcoli ingegneristici;
- il giudizio degli esperti (riferiti alle fonti di cui sopra);

- l'analisi di sistemi ingegneristici;
- l'analisi dell'affidabilità umana (HRA).

Tuttavia, l'assegnazione dei valori di probabilità ai vari rami del CET richiede di essere revisionata e di attenersi alle seguenti considerazioni.

Una adeguata qualità del PSA di livello 2 richiede un ampio uso di calcoli deterministici specifici per l'impianto. L'uso di informazioni generiche (da una analisi di impianto di riferimento) deve essere opportunamente giustificato.

Le operazioni di interpolazione od estrapolazione devono essere attentamente esaminate per assicurare che i risultati siano applicati in modo consistente con il contesto nel quale sono stati sviluppati i calcoli. L'uso di analisi di "reference plant" è accettabile solo se accompagnato da analisi od argomentazioni che supportino la sua applicabilità all'impianto in esame.

I revisori devono testare solo i codici non standard o i calcoli specifici (manuali) che sono stati sviluppati nell'ambito della applicazione specifica, con particolare risalto alle assunzioni fatte.

E' previsto che le informazioni derivanti dall'analisi del sistema di contenimento necessiti di essere rivista con particolare attenzione alla consistenza con i modelli utilizzati per il PSA di livello 1.

3.5.7 Caratterizzazione dei "Radiological Source term"

Il successivo passo del PSA di livello 2 consiste nella stima del rilascio dei prodotti di fissione nell'ambiente esterno, indicato come " radiological source term".

Tale attività è propedeutica allo sviluppo del PSA di livello 3, finalizzato alla valutazione del danno potenziale sulla salute della popolazione e del danno economico e dei rischi associati. Tale attività non è invece necessaria se il livello 2 è finalizzato alla sola "capacità di contenimento".

Le sequenze incidentali definite dal CET sono solitamente raggruppate secondo le caratteristiche che influenzano maggiormente lo sviluppo di "severe accident". Tra le caratteristiche è necessario includere i parametri che influenzano l'evoluzione dei prodotti di fissione, la loro ritenzione e propagazione attraverso ciascuna delle barriere maggiori verso l'ambiente.

Le condizioni finali così raggruppate sono riferite come "categorie di rilascio" o " source term".

I revisori dovrebbero ritenere sufficiente che i "source term" siano raggruppati in base a caratteristiche simili di rilascio radiologico e delle conseguenze esterne (off-site).

Questi attributi sono spesso specifici dell'impianto e del confinamento dello stesso; per un impianto PWR possono essere:

- Tempo di rilascio, distinto in:
  - molto rapido - perdita di confinamento anteriore al "core damage" o durante la fusione del vessel;

- rapido - prossimo al tempo di rottura del vessel;
- intermedio - parecchie ore dopo la fessurazione del vessel;
- tardivo - alla fine del tempo di missione del tipo livello 2;

▪ Stato del contenimento alla fine del tempo di missione del livello 2, distinto in:

- contenimento bypassato dal LOCA;
- contenimento bypassato da SGTR isolati;
- contenimento non isolato;
- rottura del contenimento (perdita maggiore);
- rottura strutturale del contenimento (dispersione in una vasta area);
- contenimento ventilato;

▪ Modalità di rilascio del vessel, distinte in:

- interazione secca tra core e calcestruzzo (Dry core-concrete interaction);
- interazione liquida tra core e calcestruzzo (Core-concrete interaction submerged);
- nessuna interazione tra core e calcestruzzo (No Core-concrete interaction).

▪ Meccanismi di rimozione dei prodotti di fissione, distinti in:

- nessuno;
- spray di contenimento e/o valvole di raffreddamento (è possibile anche specificare un tempo per tali operazioni);
- sistema di contenimento secondario.

▪ Pressure suppression pool, distinte in:

- sottoraffreddate;
- saturate;
- bypassate (e tempo di bypass).

▪ Tempo tra l'evento iniziatore e il danneggiamento del core, distinto in:

- poche ore;
- molte ore (più di 10).

La verifica della similitudine dei source term per le sequenze incidentali entro una categoria di rilascio può essere difficile senza calcoli deterministici dedicati ai fenomeni di rilascio e trasporto dei prodotti di fissione.

È pratica corrente effettuare un calcolo di source term per la singola specie rappresentativa dello sviluppo incidentale, entro ciascuna categoria di rilascio. L'affidabilità di tale calcolo costituisce un elemento importante nel giudizio dei revisori sui risultati ottenuti.

In relazione agli obiettivi del PSA di livello 2, può essere necessario identificare tutte le specie di prodotti di fissione. I prodotti di fissione con caratteristiche fisico-chimiche simili sono usualmente trattati collettivamente nell'analisi dei source term degli incidenti severi. I raggruppamenti sono tipicamente definiti negli stessi codici di calcolo utilizzati per generare le stime di source term. Le specie rappresentative per le diverse classi di radionuclidi sono riportate in Tabella 1.

Radionuclide class name	Representative species	Member elements
Noble gases	Xe	He, Ne, Ar, Kr, Xe, Rn, H, N
Alkali metals	Cs	Li, Na, K, Rb, Cs, Fr, Cu
Alkaline earths	Ba	Be, Mg, Ca, Sr, Ba, Ra, Es, Fm
Halogens	I	F, Cl, Br, I, At
Chalcogens	Te	O, S, Se, Te, Po
Platinoids	Ru	Ru, Rh, Pd, Re, Os, Ir, Pt, Au, Ni
Early transition elements	Mo	V, Cr, Fe, Co, Mn, Nb, Mo, Tc, Ta, W
Tetravalents	Ce	Ti, Zr, Hf, Ce, Th, Pa, Np, Pu, C
Trivalents	La	Al, Sc, T, La, Ac, Pr, Nd, Pm, Sm, Eu, Gd, Tb, Dy, Ho, Er, Tm, Yb, Lu, Am, Cm, Bk, Cf

Tabella 1 – Classe dei radionuclidi

I revisori devono esaminare i metodi usati per calcolare il rilascio di radionuclidi nell'ambiente ed essere confidenti che lo schema di raggruppamento sia consistente con il corrente stato dell'arte e l'esperienza accumulata.

Rilascio e trasporto dei prodotti di fissione

I modelli utilizzati per calcolare il rilascio ed il trasporto dei prodotti di fissione devono essere oggetto di verifica; i codici comunemente usati per tale scopo sono indicati in Tabella 2, seduta dalla IAEA – TECDOC1229 (rif.[3]). Per ciascun codice di calcolo sono indicati gli aspetti tenuti in considerazione, caratteristici dei fenomeni interni ed esterni al Vessel.

In-Vessel Phenomena					
Computer Code	**Termal-hydraulics**	**Core degradation**	**Fission product release from fuel**	**Fission product transport in RCS**	**Reactor vessel failure**
ART			X	X	
ATHLET-CD	X	X	X	X	X
BWRSAR	X	X			X
CATHARE	X				
ASCADRE	X	X	X	X	X
ESTER	X	X	X	X	
ICARE	X	X	X		
IFCI					X (FCI)
MAAP	X	X	X	X	X
MELCORE	X	X	X	X	X
PM-ALPHA/EPROSE					X (FCI)
SCDAP- RELAP5	X	X	X	X	X
STCP	X	X	X	X	X
TEXAS					X (FCI)
THALES-2	X	X	X	X	
VICTORIA			X	X	
EX-Vessel Phenomena					
Computer Code	**Core-concrete interaction**	**Fission product release from core debris**	**Fission product transport in containment**	**Hydrogen combustion**	**Containment response**
CONTAIN	X	X	X	X	X
CORCON/MOD3	X				
ASCADRE	X	X	X	X	X
FIPLOC			X		
HECTR				X	
HMS				X	
MAAP	X	X	X	X	X
MELCORE	X	X	X	X	X
RALOC				X	X
STCP	X	X	X	X	X
THALES-2	X	X	X	X	X
WECHSL	X	X			

Tabella 2 – Severe accident computer codes

L'utilizzo di sorgenti indipendenti di dati, ottenuti mediante differenti metodi di calcolo, è fortemente raccomandato, se tra gli obiettivi dell'analisi è inclusa la valutazione degli effetti di mitigazione, quali i sistemi filtranti di venting del contenimento.

Non sono accettabili, invece, degli adattamenti di source term da impianti di riferimento. Calcoli indipendenti di source term per sequenze selezionate possono essere permessi, se la frequenza di larghi rilasci di radionuclidi è eccezionalmente alta, oppure se il PSA deve essere esteso all'analisi di livello 3.

I source term devono essere rivisti con particolare attenzione nei casi in cui la frequenza d'accadimento delle seguenti condizioni accidentali è particolarmente significativa:

- rottura di tubo di un generatore di vapore;
- rilasci da incidenti con contenimento non isolato;
- rilasci da incidenti con perdite di contenimento "ritardate" (perdite ritardate possono capitare tra le 10 e le 48 ore dopo il danneggiamento del core; oltre tale tempo l'evaporazione delle specie volatili per surriscaldamento secco della superficie può dominare la caratterizzazione dei source term);
- rilasci da incidenti con erosione (scrubbing) prodotto da spray nel contenimento.

Trattamento delle incertezze e risultati del PSA di livello 2

La valutazione quantitativa delle incertezze associate ai source term non sono generalmente prodotte in sede di analisi di livello 2. Tuttavia, deve essere disponibile e verificata un'analisi di sensitività strutturata dei calcoli dei source term per gli scenari incidentali prioritari, unitamente all'identificazione delle maggiori assunzioni fatte ed alla quantificazione d'importanza (per esempio l'entità con la quale si assume che lo iodio sia permanentemente ritenuto in acqua durante l'ultima fase di un incidente è molto incerta).

La presentazione dei risultati di source term deve essere conforme alle prescrizioni di dettaglio definite nella Linea guida di riferimento (rif.[4]).

Le richieste fatte per la presentazione dei risultati avuti dal PSA di livello 1 sono valide anche per i risultati di livello 2; ciò è particolarmente importante stante la complicatezza dei fenomeni modellati, le incertezze presenti, e la non agevole comunicazione dei risultati ai non specialisti.

3.6 Revisione del PSA di livello 3

3.6.1 Introduzione

Il riferimento adottato per il PSA di livello 3 è unicamente il Safety Reports Series No. 25 (rif.[6]), per una maggiore uniformità e tracciabilità con il precedente livello di analisi, peraltro compreso nello stesso rapporto. Infatti è ovvio ed importante che i radiological source term -e le relative frequenze usate a PSA di livello 3 per determinare il rischio sulla popolazione- siano quelli identificati a livello 2.

Il rischio è riferito non solo alla salute, ma anche ad altri aspetti socialmente rilevanti quali la contaminazione del territorio (aria, acqua e prodotti alimentari). Ciò è dato modellando come i radionuclidi rilasciati dall'impianto si disperdono nell'ambiente ed alimentano tale tipologia di rischio.

L'esposizione degli individui alle radiazioni ionizzanti può portare ad effetti mortali classificati o per via deterministica o per via statistica. Gli effetti deterministici risultano dalla esposizione di tutto o parte del corpo ad alte dosi di radiazione. La loro severità cresce con la dose ed esiste una soglia di dose al di sotto della quale non è prodotta tale gravità d'effetto. Gli effetti stocastici di radiazione includono un'aumentata incidenza di tumori tra la popolazione esposta ed effetti ereditari sui loro discendenti. Per tali effetti, la probabilità di accadimento (ma non necessariamente la severità) dipende dalla dose di radiazione. Gli effetti indotti negli individui esposti sono chiamati dalla guida di riferimento "effetti somatici", mentre quelli osservati nei loro discendenti sono noti come "effetti ereditari". Gli effetti deterministici e stocastici sono spesso riferiti come effetti immediati o effetti ritardati, rispettivamente.

3.6.2 Analisi di PSA di livello 3

L'analisi di PSA di livello 3 comprende le seguenti attività:

- la definizione degli obiettivi dell'analisi;
- la caratterizzazione e raggruppamento dei source term;
- la scelta di un codice per l'analisi delle conseguenze;
- la selezione dei dati richiesti dall'analisi di conseguenze;
- l'utilizzazione del modello di dispersione atmosferica;
- l'identificazione e modellazione della pianificazione d'emergenze di contromisure;
- la quantificazione ed uso dei risultati.

3.6.3 Obiettivo del PSA di livello 3

Gli obiettivi del PSA di livello 3 possono variare dalla conduzione di un'analisi per determinare gli effetti sulla salute della popolazione presente sul sito (closet to the site), all'elaborazione di una più sofisticata analisi per ricavare stime riguardanti diverse tipologie di rischi sulla salute e sull'economia. Ciò influenza la scelta fatta del codice utilizzato per l'analisi delle conseguenze e per l'ammontare e la tipologia dei dati richiesti.

In generale, i revisori richiedono che gli obiettivi dell'analisi di livello 3 siano chiaramente definiti, insieme con i criteri utilizzati per valutare l'accettabilità dei risultati.

3.6.4 Caratterizzazione e raggruppamento dei source term

L'analisi di livello 3 parte ovviamente dai risultati di livello 2 in termini di radiological source term e relative frequenze di rilascio. In generale, questa identificazione comprende un largo numero di sequenze incidentali, ciascuna con i propri caratteristici source term. Questi possono essere raggruppati per limitare la valutazione delle conseguenze ad quantità gestibile.

Come presentato in sede di PSA di livello 2 i radiological source term includono un range di differenti radionuclidi con differente forma fisica e chimica, che determina la modalità di trasporto nell'ambiente e quindi il rispettivo contributo al rischio.

I revisori devono testare che i gruppi di radiological surce terms siano stati completamente e correttamente specificati in termini di quantità di ciascun radionuclide presente e relativa forma fisica e chimica. Viene richiesto (come tracciabilità) che tutte le sequenze incidentali identificate nel PSA di livello 2 siano mappate correttamente entro i gruppi dei radiological source term utilizzati nel PSA di livello 3. Per ciascuno dei gruppi dei source term devono essere specificate le caratteristiche temporali dei rispettivi rilasci:

- il tempo di avvio del rilascio;
- la durata del rilascio;
- la quantità di energia associata al rilascio;
- l'altezza del rilascio e la dimensione del fabbricato;
- il tempo di preavviso (warning time) per l'inizio delle contromisure.

Ove i dati dei radiological source term prodotti nel PSA di livello 2 fossero imprecisi, per esempio informazioni sulle dimensioni delle particelle negli aerosol emessi, possono essere accettate assunzioni ragionevolmente conservative.

3.6.5 Scelta di un codice per l'analisi delle conseguenze

Lo scopo dell'analisi delle conseguenze è la modellizzazione del trasporto dei radionuclidi rilasciati dall'impianto all'ambiente. Per un impianto nucleare il maggior contributo è dato dai rilasci in atmosfera e dalla relativa dispersione dei radionuclidi. Tuttavia, può essere necessario considerare altri contributi, quali la migrazione dei radionuclidi in falda.

Gli elementi principali di un'analisi di conseguenze sono:

- la campionatura dei dati meteo;
- i modelli di dispersione in atmosfera e di deposizione;
- la valutazione di dose per ciascuna linea di esposizione;
- la valutazione delle contromisure applicabili;
- la stima degli effetti sulla salute;

- la stima delle conseguenze economiche.

I codici utilizzati per l'analisi delle conseguenze permettono normalmente la modellazione:

- dei diversi fenomeni di trasporto in atmosfera;
- delle caratteristiche del terreno circostante il sito;
- delle strutture abitative e delle coltivazioni.

Le analisi di conseguenze devono tener conto delle varie vie di contaminazione (durante il passaggio di una nube): deposizione esterna di materiale radioattivo, irraggiamento esterno per deposizione su pelle, vestiti, etc., contaminazione per inalazione in varie forme.

Tra i codici di calcolo correntemente utilizzati per l'analisi delle conseguenze sono indicati i seguenti: ARANO, CONDOR, COSYMA, LENA, MACCS, MECA2 ed OSCARR (rif.[5]).

3.6.6 Dati richiesti dall'analisi di conseguenze

L'utilizzo dei codici di calcolo per l'analisi delle conseguenze è sufficientemente diffuso e praticato. I dati richiesti sono, pertanto, diffusi e ripartiti in categorie base:

- dati meteo;
- dati concernenti la popolazione, l'assetto agricolo ed economico.

La seconda categoria di dati è valutata normalmente in ripartizioni anulari centrate sul sito e distribuite in griglie definite in coordinate polari (R-θ).

Le valutazioni di conseguenze sulla popolazione riprendono la metodologia molto praticata e riferita alle modalità di esposizione.

Per quanto attiene l'analisi delle conseguenze dovute alla contaminazione dei prodotti agricoli, è richiesto un calcolo di "dose collettiva" relativa alla loro ingestione. Tali dati sono correlati ai tipi di codici di calcolo utilizzati e tipicamente includono il numero ed il tipo di bestiame, la produzione di latte e il tipo di foraggio coltivato. Se la distribuzione di prodotti alimentari è tenuta in conto è necessario specificare sia le regioni di produzione sia di consumo. I dati agricoli sono basati normalmente su informazioni istituzionali e devono essere mappati con la griglia R-θ utilizzata dai codici d'analisi. Anche i dati economici, che comprendono il valore del terreno e delle abitazioni, sono basati su informazioni istituzionali e devono essere mappati con la griglia R-θ.

3.6.7 Identificazione e modellazione della pianificazione d'emergenza di contromisure

La Linea guida fornisce indicazioni su un certo numero di contromisure che possono esser adottate per ridurre il rischio sulla popolazione e che includono le seguenti azioni di base:

- messa a riparo della popolazione esposta (sheltering);

- evacuazione della popolazione dalle aree pericolose mappate;
- decontaminazione delle persone.

Queste misure, da intraprendere a tempi brevi, permettono di limitare l'esposizione della popolazione sia all'irraggiamento sia alle contaminazioni, con lo scopo di prevenire gli effetti deterministici e minimizzare gli effetti stocastici.

Le contromisure a lungo termine includono:

la rilocalizzazione;

l'interdizione dei prodotti alimentari;

la decontaminazione del suolo.

I dati richiesti per la valutazione dell'efficacia e efficienza delle contromisure nel ridurre la dose ricevuta dagli individui includono i livelli di soglia (trigger levels), ai quali tali contromisure devono essere adottate.

Tali livelli di soglia, spesso definiti a livello governativo, si riferiscono alle condizioni dell'impianto o ai livelli di dose fuori dal sito. Le condizioni dell'impianto possono riguardare un rilascio di radioattività effettivamente avvenuto o una sequenza incidentale che si sviluppa in maniera tale da poter produrre un rilascio che supererebbe il livello di dose che richiede l'adozione delle contromisure.

Per esempio, i livelli di dose potrebbero essere stabiliti con riferimento alla distribuzione di iodio stabile e richiedere l'evacuazione o l'imposizione di divieti alimentari. I dati riguardanti la distribuzione di iodio stabile sono normalmente inclusi nel codice di analisi delle conseguenze

Per la messa a riposo, ulteriori dati richiesti riguardano il grado di schermatura e ricambio d'aria forniti dalla struttura dell'edificio che dipende dai tipi di edifici delle regioni vicine al sito. Per l'evacuazione, i dati richiesti sono relativi al tempo impiegato per dare inizio all'evacuazione, alla sua durata, ed alle modalità di attuazione.

I revisori devono essere convinti che le strategie di contromisure modellate nell'analisi di conseguenze siano realistiche e fattibili che i livelli di soglia definiti siano consistenti con i requisiti nazionali. L'esperienza maturata ha mostrato che le conseguenze di eventi di esposizione sono particolarmente sensibili alla tempestività di adozione delle contromisure, in relazione al tempo di rilascio.

3.6.8 Quantificazione e uso dei risultati di PSA di livello 3

I risultati del PSA di livello 3 sono normalmente presentati mediante una "Complementary cumulative distribution function (CCDF)", che fornisce la frequenza globale (overall) di accadimento con riferimento a livelli di danno predefiniti, per esempio al numero di morti immediati o dilazionati e/o all'area del territorio contaminato.

I codici disponibili sono generalmente usati per sviluppare l'analisi delle conseguenze per ciascun gruppo di radiological source term e fornire la distribuzione spaziale dei rischi sociali mediati sulle condizioni climatiche che possono essere presenti al momento del rilascio (public risk avarage). A tal fine, le conseguenze stimate sono pesate sulle frequenze associate ai gruppi di source term.

La CCDF dovrebbe essere presentata per ciascuno dei rischi (sulla salute ed economici) valutati nel PSA di livello 3. Maggiori dettagli sulle modalità con cui i risultati dell'analisi di conseguenze sono usati per ricavare la CCDF sono riportati nella IAEA SSN°50-P-12 (rif.[5]).

Lo scopo per cui sviluppare studi di sensibilità ed incertezza per il PSA di livello 3 è pressoché lo stesso di quello definito per i livelli 1 e 2. È necessario che venga condotto un set di studi di sensitività sufficiente, per le assunzioni e per i parametri principali dei modelli utilizzati per l'analisi delle conseguenze.

I risultati avuti dall'analisi di PSA di livello 3 dovrebbero essere confrontati con i criteri di sicurezza che si riferiscono al rischio sociale, usualmente definiti in termini di:

- rischio individuale - rischio di morte (immediato o ritardato) per i singoli membri della popolazione;
- rischio sociale - numero di morti (immediato o ritardato) nella popolazione nel suo insieme;
- conseguenze economiche (aree evacuate, aree contaminate, etc.).

4 U.S Nuclear Regulatory Commission

4.1 Premessa

L'approccio alla struttura del Safety Assessment quale sviluppata ed elaborata con lungo e proficuo percorso dalla US-NRC, con particolare riferimento ai reattori nucleari di potenza (NPP), è stato indirizzato nel presente studio particolarmente come confronto con i Safety Standards e ancor più con il processo di revisione dell'analisi di sicurezza, sviluppato dalle numerose Linee guida IAEA e ripreso nel dettaglio con riferimento al rapporto SRS No. 25 (rif.[6]) della precedente sezione.

Il confronto ha indicato l'identità di base nella strutturazione del processo di analisi che, benché non ripartito espressamente in tre successivi livelli nei PRA licenziati da NRC, ne segue puntualmente i contenuti e le connessioni logiche, nonché i metodi analitici di base utilizzati.

Per tale motivo, e riferendoci ad un documento che, pur datato, costituisce tuttora un riferimento di base, è stato deciso di non ripetere il dettaglio già presentato nella sezione precedente ma di focalizzare l'attenzione sull'integrazione delle valutazioni di incertezza nel processo di PRA, tematica trattata con un maggior approfondimento.

4.2 NUREG-1150

Nel 1975 il U.S Nuclear Regulatory Commission (NRC) completò il primo studio dei possibili eventi incidentali di impianti nucleari commerciali di potenza mediante Probabilistic Risk Assesment, i cui i risultati furono riportati nel famoso rapporto Rasmussen: "Reactor Safety Study - An Assesment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014)" (rif. [8]).

Nel 1988 iniziò lo sviluppo di cinque analisi di tipo PRA per altrettante tipologie di impianti, che portò alla pubblicazione dello standard NUREG-1150: "Severe Accident Risks: An Assesment for Five U.S. Nuclear Power Plants" (rif.[9]). La versione finale del Rapporto fu pubblicata nel 1990.

Il Rapporto fornisce i risultati avuti dallo studio dedicato a ciascuno dei cinque impianti e riassume le prospettive maturate nello sviluppo di analisi probabilistiche di rischio con riferimento alla frequenza di accadimento di incidenti severi, alle prestazioni dei contenimenti, alla valutazione dei rischi e delle incertezze associate ed al confronto con gli obiettivi e le responsabilità della NRC.

Il Rapporto è inoltre finalizzato a fornire metodi e modelli che possano supportare la definizione di priorità tra gli obiettivi di sicurezza e informazioni utili alla valutazione dei potenziali benefici derivanti da un programma di gestione per la riduzione della frequenza di accadimento di eventi incidentali.

Il Rapporto è articolato in tre parti: la prima parte riguarda gli obiettivi e i metodi utilizzati per la valutazione dei rischi; la seconda parte fornisce una sintesi dei

risultati avuti da ciascuno studio; la terza parte fornisce valutazioni di sintesi dei risultati, organizzate in relazione ai temi di interesse (frequenze di accadimento degli eventi iniziatori, evoluzione degli scenari incidentali, carichi agenti sui contenimenti, risposta delle strutture, trasporto di materiale radioattivo, conseguenze esterne e valutazione integrata del rischio) e delle loro possibilità di utilizzo da parte della NRC nelle attività di propria competenza.

Il processo di analisi di rischio definito dal NUREG-1150 è articolato in cinque fasi, che trovano riscontro nei tre livelli base definiti dalle linee guida IAEA, denominate in lingua inglese:

- "Accident Frequencies", finalizzata alla stima delle frequenze di accadimento delle sequenze incidentali che possono portare al danneggiamento del core;
- "Accident Progression, Containment Loadings and Structural response", finalizzata alla analisi dell'evoluzione dello scenario incidentale;
- "Transport of Radioactive Material", finalizzata alla valutazione dei processi di trasporto del materiale radioattivo, dal combustibile al refrigerante, alle strutture di contenimento ed infine all'ambiente circostante;
- "Off-site Consequences", finalizzata alla stima delle conseguenze degli eventi di rilascio identificati e valutati nei passi precedenti sull'ambiente circostante e sulla popolazione;
- "Risk integration", finalizzata alla integrazione dei risultati avuti dalle fasi precedenti - frequenze di accadimento e conseguenze - per la valutazione finale di rischio.

Le diverse combinazioni di eventi che possono accadere in una sequenza incidentale sono raggruppate in "plant damage state", definiti dalle condizioni operative dell'impianto (es. disponibilità dei sistemi di protezione) e dalle condizioni fisiche che caratterizzano lo scenario incidentale in oggetto (es. pressione del refrigerante). La frequenza di danneggiamento del core è il risultato della somma delle frequenze associate a vari tipi di incidente; in particolare, sono considerati i contributi derivanti dalla perdita di alimentazione elettrica, dai transitori derivanti dal guasto dei sistemi costituenti l'impianto e da eventi di LOCA.

Gli scenari incidentali conseguenti al danneggiamento del core possono evolvere in un elevato numero di modalità differenti, raggruppate in un numero minore di "accident progressione bins"

A causa della complessità delle valutazioni relative al trasporto di materiale radioattivo, realizzate mediante algoritmi semplificati, il numero di eventi analizzati è limitato.

In ultimo, i rilasci di materiale radioattivo sono raggruppati in accordo al danno potenzialmente prodotto, ai fini della successiva valutazione delle conseguenze sull'ambiente e sulla popolazione.

4.3 NUREG-1150 e valutazioni di incertezza

Il Rapporto NUREG-1150 ha introdotto significativi miglioramenti nella integrazione delle valutazioni di incertezza nella procedura di PRA, riconoscendo la necessità di integrare nella stima del rischio le incertezze associate alla frequenza di danneggiamento del core (CDF: core damage frequency), alla incompleta conoscenza delle risposte dei sistemi costituenti l'impianto, alla evoluzione degli scenari incidentali ed al trasporto di materiale radioattivo. A tal fine è esplicitamente identificata l'attività di "Uncertainty Analysis and Expert Judgment". Sono identificati quattro passi successivi per lo sviluppo delle valutazioni quantitative di incertezza, denominati in lingua inglese:

1) "Scope of Uncertainty Analysis";

2) "Definition of Specific Uncertainties";

3) "Development of Probabilistic Distribution";

4) "Combination of Uncertainties".

L'approccio utilizzato è di tipo probabilistico: in luogo della stima di valori puntuali dei parametri di ingresso del modello sono introdotte opportune distribuzioni di probabilità. Sono utilizzati metodi di elicitazione mediante giudizio degli esperti a supporto dei dati sperimentali disponibili e metodi simulazione per la "propagazione" delle incertezze. Le valutazioni quantitative di incertezza sono riferite tanto agli eventi "interni", che possono occorrere con l'impianto operante a piena potenza, quanto agli eventi "esterni" di incendio, allagamento e terremoto.

Nel Rapporto si sottolinea l'esistenza di fonti di incertezza in ciascuna fase in cui è articolato il processo di analisi di rischio e si evidenzia la necessità di includere solo le fonti principali a causa dell'onere computazionale richiesto. L'identificazione delle fonti principali di incertezza è realizzata sulla base dei risultati avuti da PRA precedenti, dal giudizio degli esperti e da analisi di sensitività mirate, fatte in misura limitata. In particolare, l'analisi considera le incertezze associate alla frequenza degli eventi iniziatori che hanno impatto sulla frequenza di danneggiamento del core e le incertezze associate ai parametri che determinano la successiva evoluzione dello scenario incidentale ed il trasporto di materiale radioattivo.

Nella prima fase del processo di analisi di rischio sono valutate le distribuzioni di probabilità associate alle frequenze di danneggiamento del core, dovuto ad eventi interni ed esterni (incendio e terremoto separatamente). Tali distribuzioni sono riportate in forma tabulare e mediante istogrammi e sono caratterizzate mediante misure statistiche quali media, mediana (50° percentile), 5° e 95° percentile. Nei casi in cui la distribuzione si estende fino a valori molto bassi di probabilità, le osservazioni al di sotto di un valore limite definito sono tra loro raggruppate e fornite separatamente.

Il processo di analisi include la valutazione di due misure di importanza: la prima misura è riferita agli effetti della riduzione della frequenza di guasto dei componenti, sulla frequenza di danneggiamento del core (trattasi pertanto di una misura di importanza in senso stretto); la seconda misura è riferita al

contributo dell'incertezza associata ai parametri di ingresso sulla incertezza associata alla frequenze di danneggiamento del core (trattasi pertanto di una misura di sensitività).

Al fine di includere nelle valutazioni le incertezze associate ai fenomeni che caratterizzano l'evoluzione degli scenari incidentali, queste devono essere espresse in termini di incertezze associate ai parametri del modello. Per tale scopo è necessario tener conto della non esatta conoscenza dei parametri chimico-fisici di base e delle relazioni esistenti con i parametri di sintesi del modello probabilistico di valutazione del rischio.

Le distribuzioni di probabilità che descrivono le incertezze associate ai parametri di ingresso del modello sono definite mediante metodi differenti. Per molti parametri sono utilizzate le informazioni derivanti dalla elaborazione statistica di dati di impianto e di dati derivanti da adeguate esperienze sperimentali. Per i parametri ritenuti importanti in termini di contributo sull'incertezza associata ai rischi oggetto di valutazione, per i quali non sono disponibili dati empirici condivisi e accettati, si procede alla valutazione delle distribuzioni di probabilità mediante giudizio degli esperti. A tal fine sono utilizzate differenti metodologie, formalizzate in opportune procedure al fine di minimizzare la soggettività dei giudizi e le non eliminabili forzature.

I passi principali che costituiscono il processo di elicitazione delle distribuzioni di probabilità riguardano la selezione degli esperti, il loro addestramento, la presentazione e la revisione delle informazioni di base, la preparazione delle analisi da parte di ciascun esperto, la revisione congiunta e la discussione sui risultati avuti, l'elicitazione di probabilità da parte di ciascun esperto, la composizione e l'aggregazione dei giudizi e la revisione finale dei risultati quantitativi.

Mediante metodi MonteCarlo, ed in particolare mediante tecniche di tecniche di campionamento Latin hypercube, le incertezze associate ai parametri di ingresso sono "propagate" attraverso il modello al fine di valutare l'incertezza associata alla frequenza di danneggiamento del core, alla successiva evoluzione dello scenario incidentale ed al trasporto di materiale radioattivo.

La tecnica Latin Hypercube costituisce l'estensione al caso multi-dimensionale del Campionamento stratificato, una delle possibili tecniche di Campionamento dell'Importanza. L'effetto complessivo è una riduzione della varianza associata alla stima delle variabili di interesse e, conseguentemente, una maggiore efficacia della simulazione rispetto a metodi MonteCarlo "analogici".

I risultati avuti dalle simulazioni sono analizzati mediante opportune tecniche statistiche ed in particolare mediante metodi di regressione che, in modo agevole, permettono di evidenziare e trattare le correlazioni esistenti tra i parametri.

Nell'ultima fase del processo di analisi si procede alla integrazione dei risultati avuti dalle fasi precedenti – frequenze di accadimento e conseguenze - per la valutazione finale di rischio. Il risultato ultimo è rappresentato dal rischio associato agli eventi interni ed all'evento di incendio (il rischio associato ad eventi di terremoto non è integrato nelle valutazioni finali), descritto in termini di densità di distribuzione di probabilità, in forma grafica (mediante istogramma) e

tabellare, insieme con le misure statistiche (media, 5°, 50 e 95° percentile) che lo caratterizzano.

Ulteriori risultati forniti dalla analisi riguardano la decomposizione del valore medio del rischio complessivo nei contributi associati ai diversi “plant damage states” e “accident progressione bins” e la valutazione mediante metodi di regressione del contributo dell’incertezza associata ai parametri di ingresso (singoli e/o per gruppi) sull’incertezza associata al rischio complessivo.

4.4 U.S Nuclear Regulatory Commission e orientamenti recenti

I criteri di difesa in profondità (defence in depth), riguardanti l’adozione di successive misure adeguate a prevenire l’accadimento di eventi incidentali o mitigarne il danno prodotto, sono alla base dell’approccio adottato dalla NRC (Structuralist approach). Le analisi probabilistiche di rischio possono e devono essere considerate come complementari a tali criteri.

Le incertezze residue insite nei modelli di valutazione del rischio devono essere riferite alle proprietà dei materiali, alle prestazioni dei contenimenti ed ai fenomeni per i quali esistono pochi e/o non adeguati dati sperimentali. La differenziazione tra incertezza aleatoria, riferita alla presenza di processi stocastici, ed incertezza epistemica, riferita ai valori non noti dei parametri, alle assunzioni dei modelli deterministici ed agli aspetti di non completezza delle analisi, finalizzata unicamente a scopi di comunicazione.

Lo sviluppo dell’analisi di rischio probabilistica deve essere finalizzata a ridurre gli aspetti di conservatività delle valutazioni, che non risultano strettamente necessari per il soddisfacimento dei requisiti ed il raggiungimento degli obiettivi di sicurezza.

Pertanto, i risultati delle analisi probabilistiche di rischio devono essere considerati come uno degli input da considerare nel processo decisionale in carico all’autorità competente, ad integrazione dei criteri di difesa in profondità, della conformità ai requisiti mondatori di sicurezza, del monitoraggio continuo delle prestazioni e del mantenimento di adeguati margini di sicurezza, secondo un approccio “Risk-informed”.

5 Spunti per l'elaborazione di una Linea Guida Italiana

5.1 Premessa

E' opportuno evidenziare i seguenti punti:

- il Rapporto di sicurezza, chiamato PSA o PRA con significati equivalenti, presenta un uso sempre maggiore ed una centralità nella documentazione inerente al processo decisionale di accettabilità del livello di sicurezza di un Impianto Nucleare di Potenza;
- gli obiettivi di un PSA sono soprattutto:
  - *a.* di fornire una convincente dimostrazione di conformità con i requisiti internazionali di sicurezza (IAEA) e di accettabilità anche nei riguardi delle normative nazionali;
  - *b.* di evidenziare i miglioramenti possibili per ottenere un sensibile aumento del livello di sicurezza;
  - *c.* di ottimizzare le procedure operative con particolare riferimento ai programmi di manutenzione dell'impianto;
- esiste una Regulatory Guide diretta alle Utility e finalizzata ad indirizzare le elaborazioni (come contenuti e forma) richieste dal PSA ed una Regulatory Guide diretta alle Agenzie al fine di supportare la revisione del PSA in ogni dettaglio rilevante, e che ovviamente le due Linee guida sono tra loro fortemente relazionate;
- nei vari paesi europei, coinvolti in campo nucleare, le Agenzie adottano, con riferimento all'impostazione e alla elaborazione del PSA, oltre alla conformità con i requisiti internazionali, regolamentazioni nazionali ed internazionali che determinano inevitabili differenziazioni;
- su tale aspetto il WENRA Working Group ha dedicato uno studio (Pilot study) per sviluppare una metodologia sistematica di confronto dei vari PSA al fine di indirizzare le Agenzie verso una omogeneizzazione ed implementazione europea intesa come il raggiungimento di una differenza non sostanziale da un punto di vista della sicurezza e dei conseguenti miglioramenti ottenibili per gli Impianti Nucleari di Potenza (la metodologia è stata applicata con risultati incoraggianti).

Ciò detto, si è ritenuto di interesse ricavare, dagli impianti normativi e dagli elaborati di studio, un set di spunti utili per una Linea Guida Italiana, relativi soprattutto agli aspetti di "safety operating organization" e "management system", con riferimento ai rapporti tra le diverse normative nazionali, ai requisiti internazionali e ai rapporti tra Agenzia ed Utility.

5.2 Spunti da WENRA Pilot Study e dal Rapporto [13] (gennaio 2006)

Gli Studi WENRA hanno innanzitutto, identificato nella considerazione dei vari Paesi europei le aree e le corrispondenti tematiche in cui è risultato più rilevante, dal punto di vista della sicurezza, effettuare una valutazione di dettaglio.

Aree e tematiche sono riportate nella seguente Tabella 3.

Safety Area	Safety Issue	
Safety Management	A	Safety Policy
	B	Operating organization
	C	Quality management
	D	Training and Authorization of NNP staff (jobs with safety importance)
Design	E	Verification and improvement of the design
	F	Design basis envelope for existing reactor
	G	Safety classification of structures, systems and components
Operation	H	Operational limits and conditions
	I	Ageing management
	J	System for investigation of events and operational experience feedback
	K	Maintenance, in-service inspection and functional testing
	LM	Emergency Operating procedures and severe accident management guidelines
Safety verification	N	Contents and updating of safety analysis report (SAR)
	O	Probabilistic safety analysis (PSA)
	P	Periodic safety review (PSR)
	Q	Plant modification
Emergency preparedness	R	On-site emergency preparedness
	S	Fine protection against internal fires

Tabella 3 – Aree e tematiche di sicurezza

Per chiarezza, i “safety issues” sono stati strutturati nelle cinque aree che corrispondono alla “Convention on Nuclear Safety” e alla struttura utilizzata da IAEA e da molte Agenzie nazionali.

Inoltre, occorre evidenziare che lo studio WENRA ha considerato nel quadro regolatorio e normativo nucleare gli aspetti afferenti le Agenzie di sicurezza nucleare (NSR), gli organismi di normazione ed i committenti, escludendo le disposizioni legali (leggi, decreti, delibere di ordinanza) vigenti in ciascun Paese, che fanno capo al Governo e al Parlamento.

Entro il processo di identificazione delle tematiche, lo studio WENRA ha evidenziato diversi aspetti che possono costituire spunti interessanti per l’elaborazione di una Linea Guida Italiana. Tali aspetti vengono riportati di seguito:

- per i 18 safety issues, elencati in Tabella 3, è stato sviluppato un insieme di “Reference Levels” che identifica i principali requisiti atti ad omogeneizzare la sicurezza dei reattori; tali livelli sono principalmente basati su gli IAEA Safety Standard;
- i vari Paesi hanno utilizzato questi livelli di riferimento per effettuare una autovalutazione sia sul piano giuridico normativo sia sul piano dell’attuazione, documentando la loro posizione;
- le posizioni nazionali sono state esaminate in un incontro collegiale (review panel) per validare le autovalutazioni;
- dove necessario, sono stati apportati cambiamenti alle posizioni nazionali e in alcuni casi sono stati modificati i livelli di riferimento (ciò aumenta la confidenza nei risultati ottenuti dall’attività del gruppo WENRA);
- infine, sono state identificate quelle aree in cui l’intervento di armonizzazione si è reso essenziale sia per quanto concerne gli aspetti normativi sia per quelli attinenti necessità di implementazione.

5.3 Spunti da SRS No.25 IAEA nell’area delle Operating Organization

In questa sede vengono ripresi gli argomenti riguardanti il duplice aspetto di elaborazione e di revisione del PSA che comprendono, oltre alle scelte metodologiche, i necessari rapporti tra Agenzia e Utility suggeriti dalla direttiva IAEA.

Con riferimento al processo di revisione di un PSA, è parso utile cogliere gli spunti inerenti i seguenti aspetti:

- la tempistica (timing);
- l’estensione della revisione (Extent)
- la documentazione richiesta.

Tempistica

Con riferimento alla tempistica, le revisioni condotte dalle Agenzie possono essere “on-line” o “off-line”.

Una revisione on-line è condotta subito dopo che un team dell’Utility ha finito una particolare task. Il vantaggio di questo approccio è che molte delle revisioni possono essere tempestivamente incorporate nel PSA, riducendo in tal modo il numero di riedizioni. Lo svantaggio è che la revisione può essere basata su rapporti che hanno subito cambiamenti significativi durante il prosieguo dell’analisi e quindi le precedenti revisioni devono essere riviste.

Una revisione off-line è condotta dopo che il team dell’Utility ha presentato il rapporto finale all’Agenzia. Il vantaggio di questo approccio è che i documenti PSA sono rivisti una volta sola (se non sono richieste diverse edizioni). Lo svantaggio è che la revisione può trovare problemi ed inadempienze significativi che sarebbero potuti essere identificati e corretti più agevolmente nelle fasi iniziali dell’analisi.

Il timing richiede un preliminare accordo tra Agenzia e Utility con la stesura di una programmazione al fine di mediare i bisogni di entrambe le organizzazioni e di assicurare che il processo di revisione sia condotto in modo efficiente e sia in grado di minimizzare ogni ritardo per completare il PSA o la sua revisione.

Estensione

L'estensione della revisione da parte dell'Agenzia deve essere concordata con la Utility alla partenza del processo decisionale. In particolare, si può avere una revisione estensiva più dettagliata ed una revisione più limitata a seconda di quanto viene praticato a livello nazionale.

In una revisione estensiva, si hanno vantaggi significativi in termini di comprensione, di confidenza nel PSA e di riduzione degli sforzi richiesti per effettuare successive revisioni. Lo svantaggio è relativo all'elevato costo per l'Agenzia e pertanto questo approccio è difficilmente applicabile se il numero di progetti di impianto è elevato o se le risorse disponibili dell'Agenzia sono limitate.

In una revisione limitata, deve essere perseguito l'obiettivo di assicurare che tutti gli aspetti delle sequenze incidentali che conducono al danneggiamento del core, ad un largo rilascio od a particolari conseguenze esterne all'impianto, siano adeguatamente modellati ed i dati usati per determinare le frequenze delle sequenze di evento siano rappresentativi dell'impianto. Per soddisfare tale obiettivo la revisione dovrebbe focalizzarsi su quegli aspetti del PSA che hanno il più alto impatto sui risultati dell'analisi. Il vantaggio di questo approccio è che richiede minori risorse all'Agenzia; lo svantaggio è che comporta una minore capacità di lettura e un minor livello di confidenza nei risultati ottenuti. Questo metodo aumenta gli sforzi richiesti per revisionare applicazioni successive.

Una revisione estensiva deve essere preferita nei seguenti casi:

a. quando il livello di rischio di un impianto è significativamente alto;
b. per il primo PSA fatto da una Utility;
c. per il PSA di un nuovo tipo di reattore;
d. per il PSA dove il progetto di impianto o le procedure operative sono significativamente differenti dall'esperienza precedente.

Da quanto sopra, ne consegue che le revisioni applicate ai PSA di Reattori di terza generazione debbano essere del tipo estensivo.

Documentazione

La documentazione richiesta per una revisione comprende sia la documentazione descrittiva dell'impianto e delle procedure operative di un impianto nucleare di potenza sia l'analisi e il rapporto di sicurezza (PSA) dell'impianto stesso. Questa documentazione è di vitale importanza dal momento che essa è sottoposta in termini formali dalla Utility all'Agenzia e costituisce la base per la revisione ufficiale, per il giudizio finale di accettabilità e per ogni altro utilizzo del PSA.

Il punto di partenza per la produzione e revisione di un PSA deve essere una chiara descrizione (definizione) generale del progetto di impianto e di come si intende operarlo anche in rapporto alla tipologia del sito prescelto.

L'Agenzia deve accordarsi con la Utility sul format e sul contenuto della documentazione prima dell'avvio del PSA. Ciò assicura che la Quality assicurance (QA) osservata dai processi di revisione sia condotta molto più efficacemente.

La prima task del team di revisione è di testare che la documentazione del PSA corrisponda a quanto descritto sopra. Se questo non è rispettato i revisori devono indicare alla Utility quale documento addizionale è richiesto, in modo che sia fornito in tempi utili.

Inoltre, i revisori devono verificare che le informazioni del PSA di livello 1 necessarie per valutare le prestazioni del contenimento e il trasporto di radionuclidi siano descritte e trasferibili a livello 2 e a livello 3 della corrispondente analisi con sufficiente completezza e precisione.

Può essere inserito come spunto interessante l'osservazione che tutti i Safety Assessment (SA) contenuti nei PSA accettati da Agenzie diverse sono sviluppati con una sostanziale ripartizione dell'analisi in tre fasi, che implicano metodi e strumenti diversificati (prevalentemente probabilistici per il primo livello, deterministici per il secondo livello finalizzato alla valutazione delle capacità di contenimento, probabilistici per il terzo livello finalizzato all'analisi del trasporto dei prodotti radioattivi rilasciati). Tuttavia, tali fasi non sono universalmente classificate con la numerazione del livello, come si è visto per NRC (vedi §4).

Per quanto attiene la documentazione della fase analitica dei tre livelli di analisi, è utile riprendere le richieste del Req. 20 di IAEA-SRS No.25 (rif.[1]), discusso nel §2, che comprendono:

- una giustificazione per la selezione degli "anticipated operational occurrences" nonchè degli eventi incidentali considerati nell'analisi;
- una rassegna dei dettagli necessari alla raccolta di dati, alla definizione dei modelli, all'adozione dei codici di calcolo e delle assunzioni fatte;
- i criteri usati per la valutazione e la modellizzazione dei risultati;
- i risultati delle analisi riguardanti tutte le prestazioni dell'impianto o delle attività, i rischi di radiazione individuati e una discussione sulla valutazione delle incertezze;
- le conclusioni sull'accettabilità del livello di sicurezza raggiunto e le indicazione riguardanti necessari miglioramenti e misure addizionali previste.

Ulteriori spunti ricavabili dalla normativa IAEA e di rilevante significatività sono riferiti ai seguenti aspetti:

1. <u>"Defence in depth"</u>

   Le misure adottate al fine di prevedere e minimizzare le conseguenze di eventi incidentali severi sono fortemente trattate nell'ambito di una sezione

appositamente dedicata e indicata come “defence in depth”. Il Req. 13 di IAEA-GSR Part 4(rif.[1]) è specificatamente dedicato ad essa e ripartisce le tipologie di difesa in tre principali modalità: quelle attinenti la gestione e il controllo, quelle attinenti i sistemi e le funzioni di sicurezza, quelle attinenti i sistemi di protezione con particolare riferimento alle barriere fisiche ed alle diverse strutture di contenimento (rispetto al danneggiamento del core) presenti.

2. Analisi di sensitività, incertezza ed importanza

   Le analisi richieste dalla struttura del Safety Assessment, in particolare quelle sviluppate con metodi deterministici, nonché quelle relative alla valutazione finale del rischio, devono comprendere con approccio metodologicamente definito e quantificato, gli studi di sensitività, incertezza ed importanza. Tale aspetto è richiesto dalle analisi e spinto con forza nelle procedure di revisione dalle rispettive Linee guida IAEA.

Infine, sul piano pratico e valutativo, è considerato utile che i revisori dispongano copie informatiche del PSA piuttosto che di copie cartacee, particolarmente per le analisi eseguite mediante Alberi degli eventi e Alberi dei guasti. Ciò permette, infatti, ai revisori:

- una più agile ricerca delle informazioni specifiche nei modelli;
- di effettuare degli spot checks sui modelli e sulle specifiche quantificazioni;
- di effettuare una analisi di identificazione delle aree del PSA che richiedono una particolare revisione;
- di effettuare valutazioni di sensitività per verificare quanti variazioni nelle assunzioni fatte possono incidere sui risultati del PSA;
- di utilizzare il PSA come base per una regolamentazione riferita al rischio.