L'MBSE come supporto alla definizione di un Data Model per la messa in sicurezza delle Infrastrutture Critiche

IBM System Symposium Italia
29 Novembre 2012

ASTER
TECHNOLOGY & ENGINEERING

Sommario

- Il Gruppo di Lavoro Data Model dell'AIIC
- Definizione del Piano di Lavoro
- Definizione del Glossario dei Termini
- Il Processo di Analisi della Sicurezza
- Tre Architetture per l'Infrastruttura Critica
- Relazioni tra le Architetture
- Elementi del Data Model
  - ✓ Dimensione Componenti
  - ✓ Dimensione Viste
  - ✓ Dimensione Contromisure
- Data Model Completo
- Applicazioni del Data Model
  - ✓ Torre di Controllo
  - ✓ Un nuovo modello per l'analisi del Rischio nelle IC

Il Gruppo di Lavoro Data Model dell'AIIC

- L'Associazione Italiana esperti in Infrastrutture Critiche (AIIC) ha istanziato nel 2012 un gruppo di lavoro denominato GDL PSO-DM, Gruppo di Lavoro Piano di Sicurezza dell'Operatore – Data Model, con l'obiettivo di

«definire un modello dei dati per la costruzione di una base di conoscenza a supporto di una analisi dei rischi mirata alla protezione delle Infrastrutture Critiche»

- Il contributo di Aster al GdL si è caratterizzato da subito nell'applicazione dei principi del Systems Engineering, sia a livello metodologico (**visione di sistema**, particolare cura nel consolidamento del **glossario dei termini**, definizione dei **processi** dell'attività) che applicativo (descrizione formale delle entità e delle loro interrelazioni mediante linguaggio **SysML**)

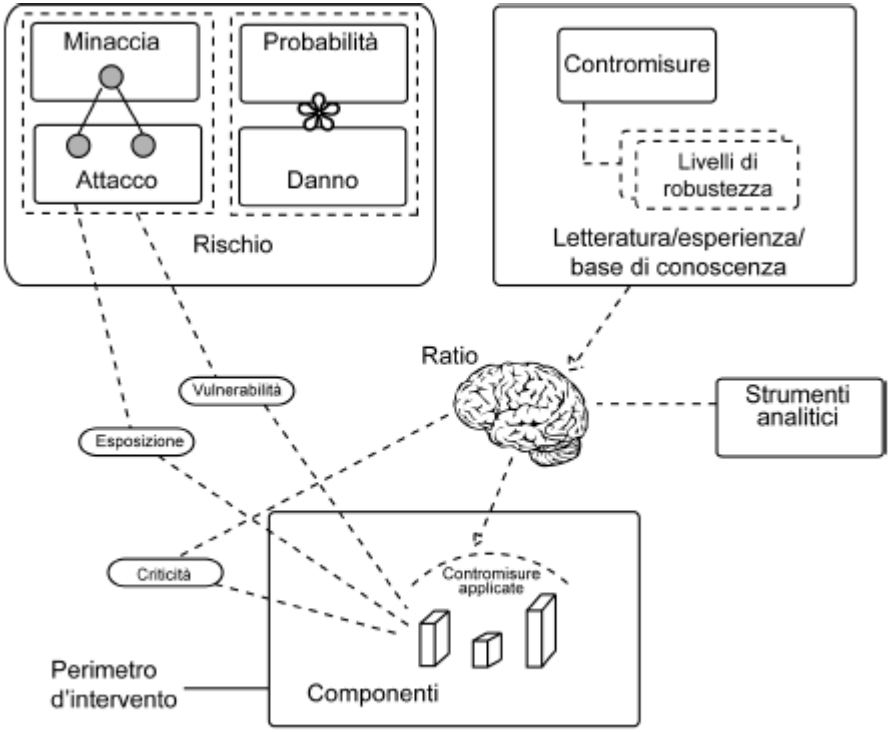
Il Gruppo di Lavoro Data Model dell'AIIC

- L'obiettivo dell'applicazione dei principi SE è quello di compiere un primo passo nella direzione della **«Security by Design»** per le Infrastrutture Critiche.

- Come definito dallo U.S. Department of State:
  - ✓ *"Security by Design" is a concept that incorporates security into **all phases** and aspects of facility **design**, **construction**, and **operations** […]*
  - ✓ *Security is viewed from a **life-cycle management** perspective, ensuring that the facility is designed and constructed in a manner to ensure efficient and effective physical security operations.*
  - ✓ *Early in the facility design phase, the design is tested against **a spectrum of threats through vulnerability assessment and use of modeling and simulations tools**. The design is modified to address any identified issues and subsequent design changes are evaluated in the same manner.*

Il Gruppo di Lavoro Data Model dell'AIIC: requisiti

- L'attività si è basata su quanto già prodotto dal GdL "Infrastrutture Critiche Europee Piano di Sicurezza dell'Operatore: Proposta di linee guida operative"



Il modello di analisi del rischio

Le tre dimensioni del PSO

ASTER TECHNOLOGY & ENGINEERING

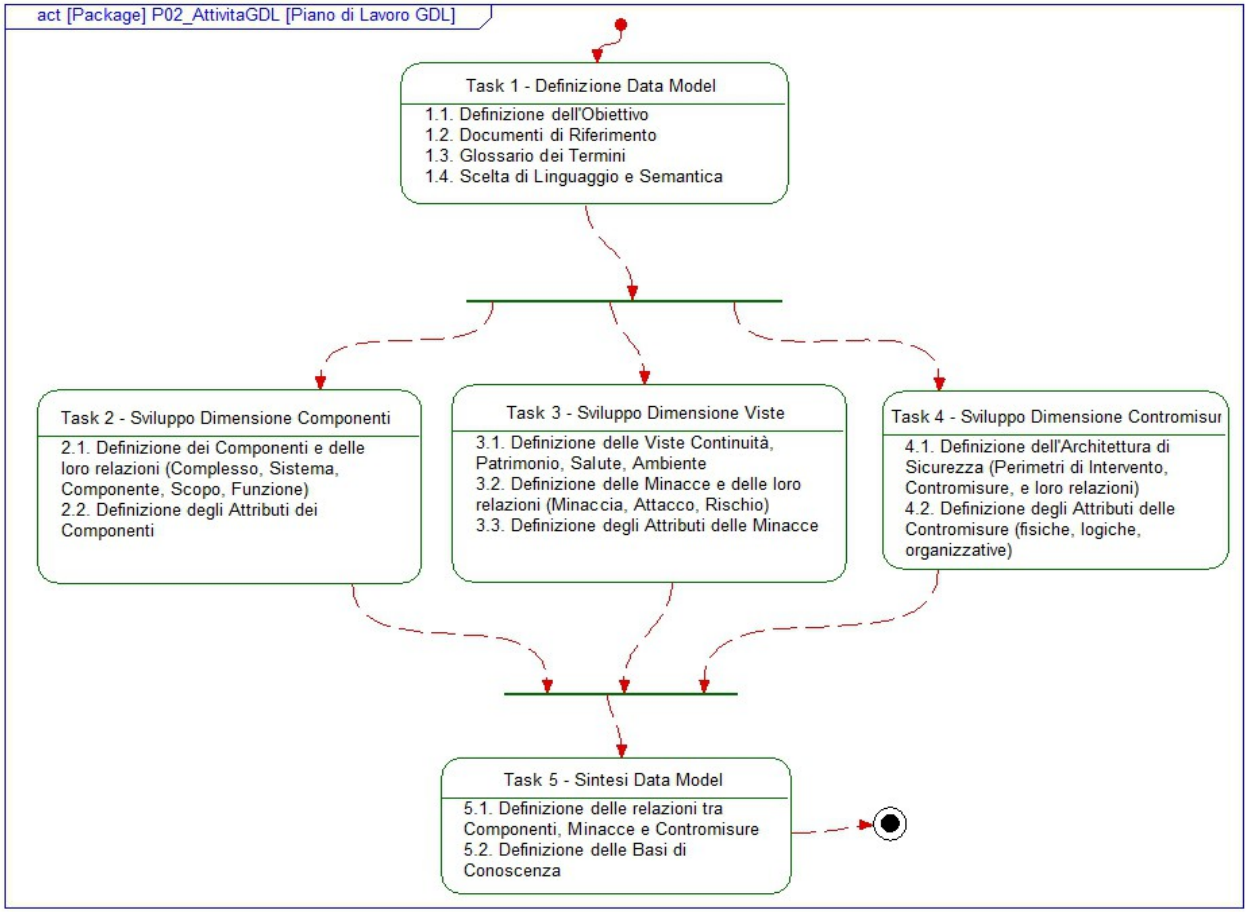
Il Gruppo di Lavoro Data Model dell'AIIC: requisiti

- **Requisito 1**: «Il modello concettuale ipotizzato consisterà nel raffinamento delle entità e delle relazioni già ipotizzate (perimetro, componenti, attacchi, contromisure) nell'ambito delle relative viste»

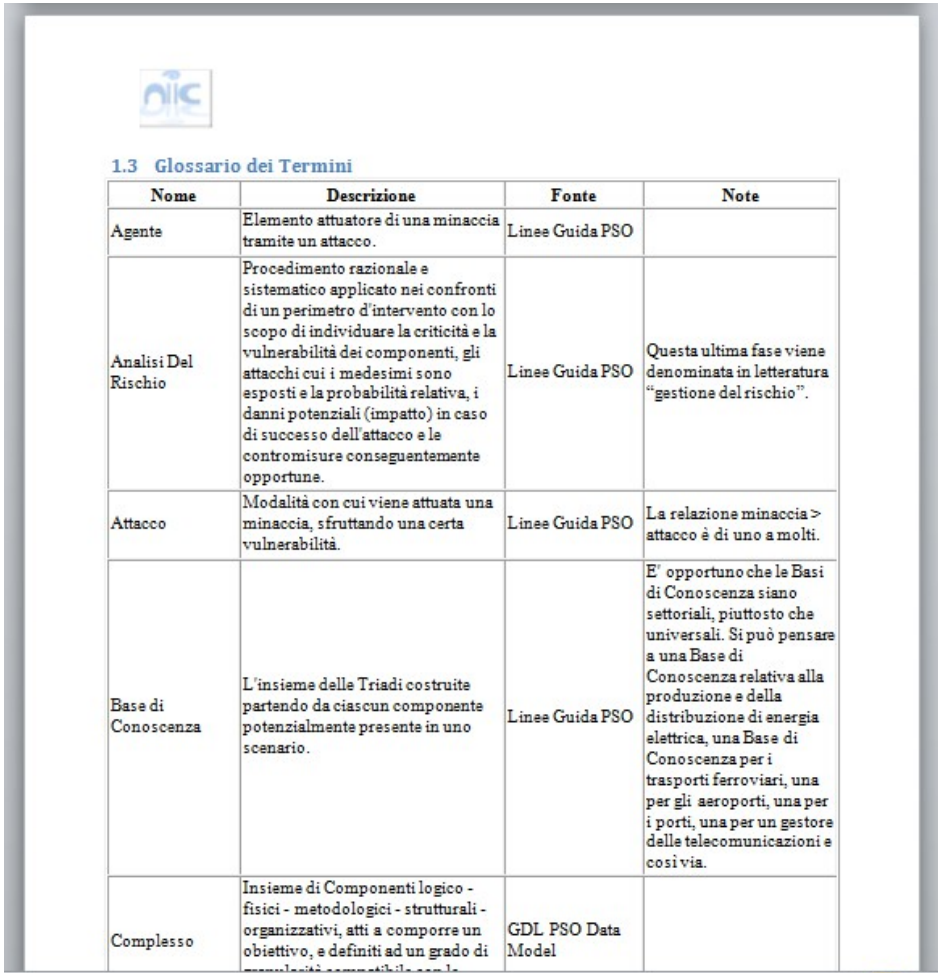
- **Requisito 2**: «Il deliverable finale sarà un modello logico, comprensivo dell'aspetto semantico, atto ad individuare le entità, gli attributi e le relazioni di una base di conoscenza finalizzata alla progettazione di un consequenziale modello di analisi dei rischi. Questo ultimo aspetto potrà essere oggetto di una successiva attività del GDL»

Definizione del Piano di Lavoro

- Analisi dei Task e loro relazioni



Definizione del Glossario dei Termini



1.3 Glossario dei Termini

Nome	Descrizione	Fonte	Note
Agente	Elemento attuatore di una minaccia tramite un attacco.	Linee Guida PSO	
Analisi Del Rischio	Procedimento razionale e sistematico applicato nei confronti di un perimetro d'intervento con lo scopo di individuare la criticità e la vulnerabilità dei componenti, gli attacchi cui i medesimi sono esposti e la probabilità relativa, i danni potenziali (impatto) in caso di successo dell'attacco e le contromisure conseguentemente opportune.	Linee Guida PSO	Questa ultima fase viene denominata in letteratura "gestione del rischio".
Attacco	Modalità con cui viene attuata una minaccia, sfruttando una certa vulnerabilità.	Linee Guida PSO	La relazione minaccia > attacco è di uno a molti.
Base di Conoscenza	L'insieme delle Triadi costruite partendo da ciascun componente potenzialmente presente in uno scenario.	Linee Guida PSO	E' opportuno che le Basi di Conoscenza siano settoriali, piuttosto che universali. Si può pensare a una Base di Conoscenza relativa alla produzione e della distribuzione di energia elettrica, una Base di Conoscenza per i trasporti ferroviari, una per gli aeroporti, una per i porti, una per un gestore delle telecomunicazioni e così via.
Complesso	Insieme di Componenti logico - fisici - metodologici - strutturali - organizzativi, atti a comporre un obiettivo, e definiti ad un grado di	GDL PSO Data Model	

- Acquisizione ed integrazione dei glossari derivanti da varie sorgenti di riferimento
- Armonizzazione delle definizioni in base agli scopi specifici del GdL

Processo di Analisi della

...o di messa in sicurezza d... ...ne

...na

...alisi di Rischio

- ...dentificazione Minacce
- Qua...ficazione ...nera...

Processo ciclico, viene ripetuto fino a quando le vulnerabilità sono tutte sotto una soglia definita

Attività del GDL PSO-Data Model:

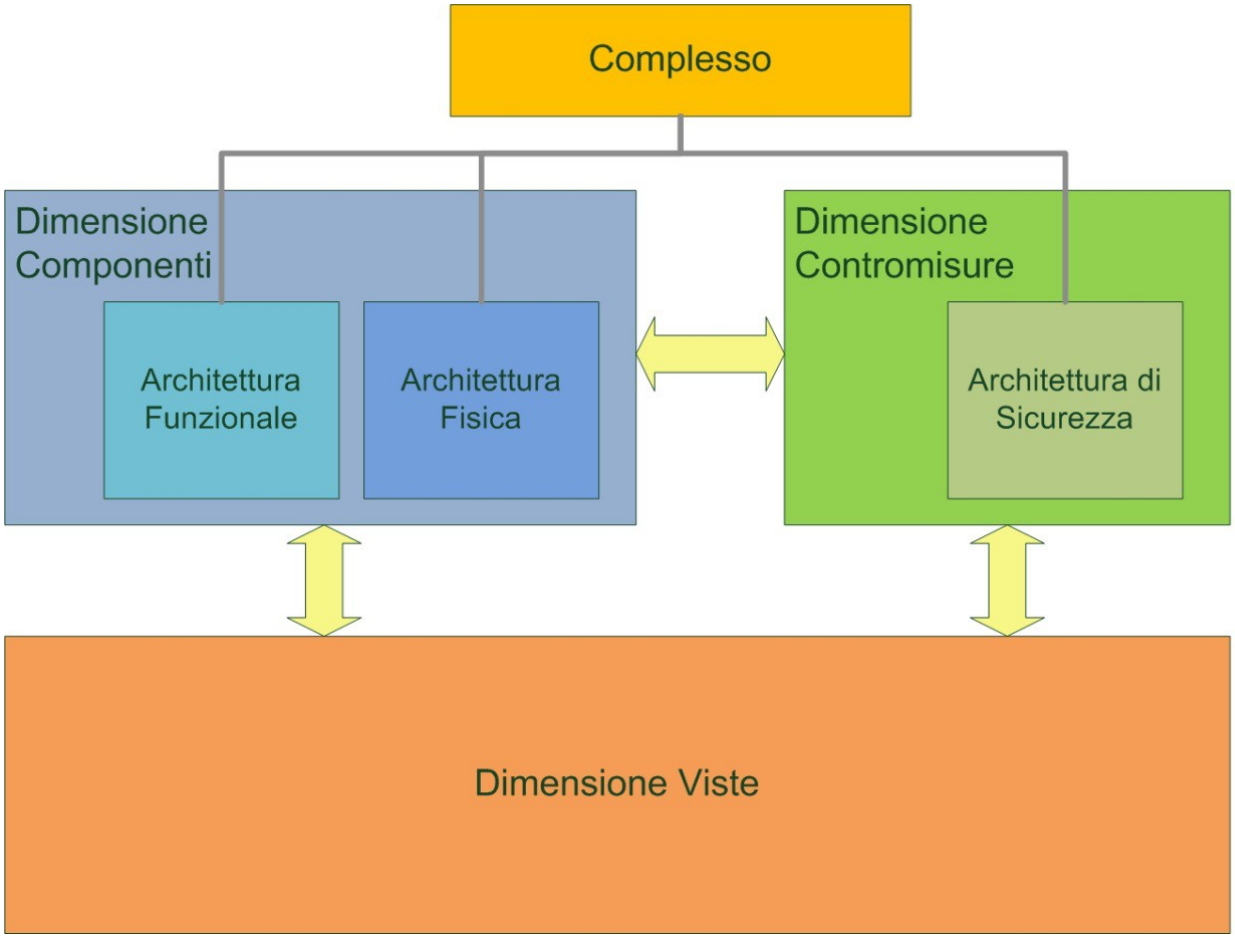
Generazione di un Modello dei Dati e di una Terminologia condivisa a supporto di tutte e tre le fasi

Analisi d...

- Definizio... Interv...
- De...

Tre Architetture per l'Infrastruttura Critica

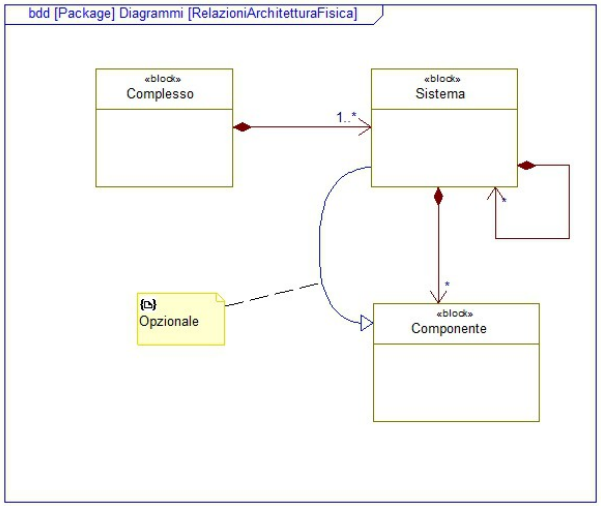
- Si è scelto di rappresentare un Complesso come descritto da tre "architetture" concorrenti

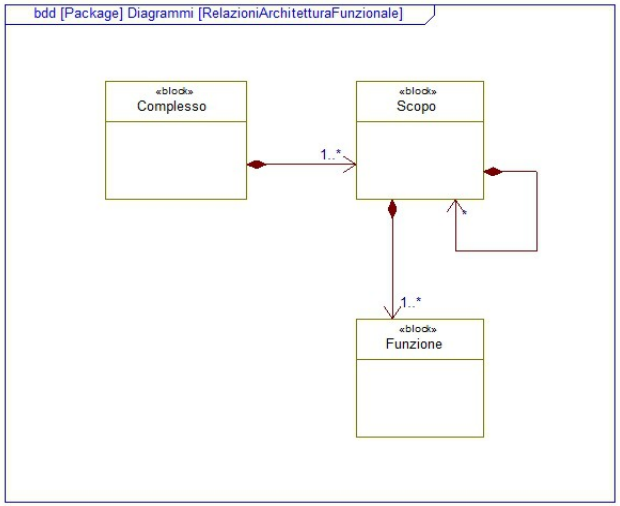


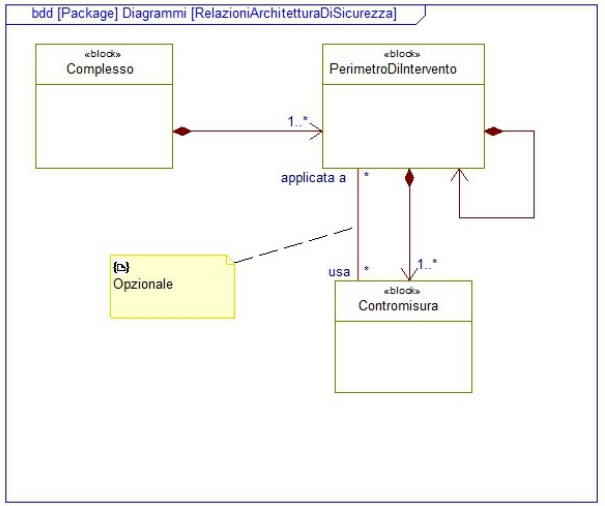
- Architettura Fisica (composta da Sistemi e Componenti)
- Architettura Funzionale (composta da Scopi e Funzioni)
- Architettura di Sicurezza (composta da Perimetri di Intervento e Contromisure)

Tre Architetture per l'Infrastruttura Critica

- Le tre architetture rappresentano diversi "punti di vista" dello stesso Complesso. Le prime due esistono indipendentemente l'una dall'altra, per quanto poi vada analizzata la fitta serie di relazioni tra di esse; la terza invece ne fa una sintesi dal punto di vista della sicurezza.



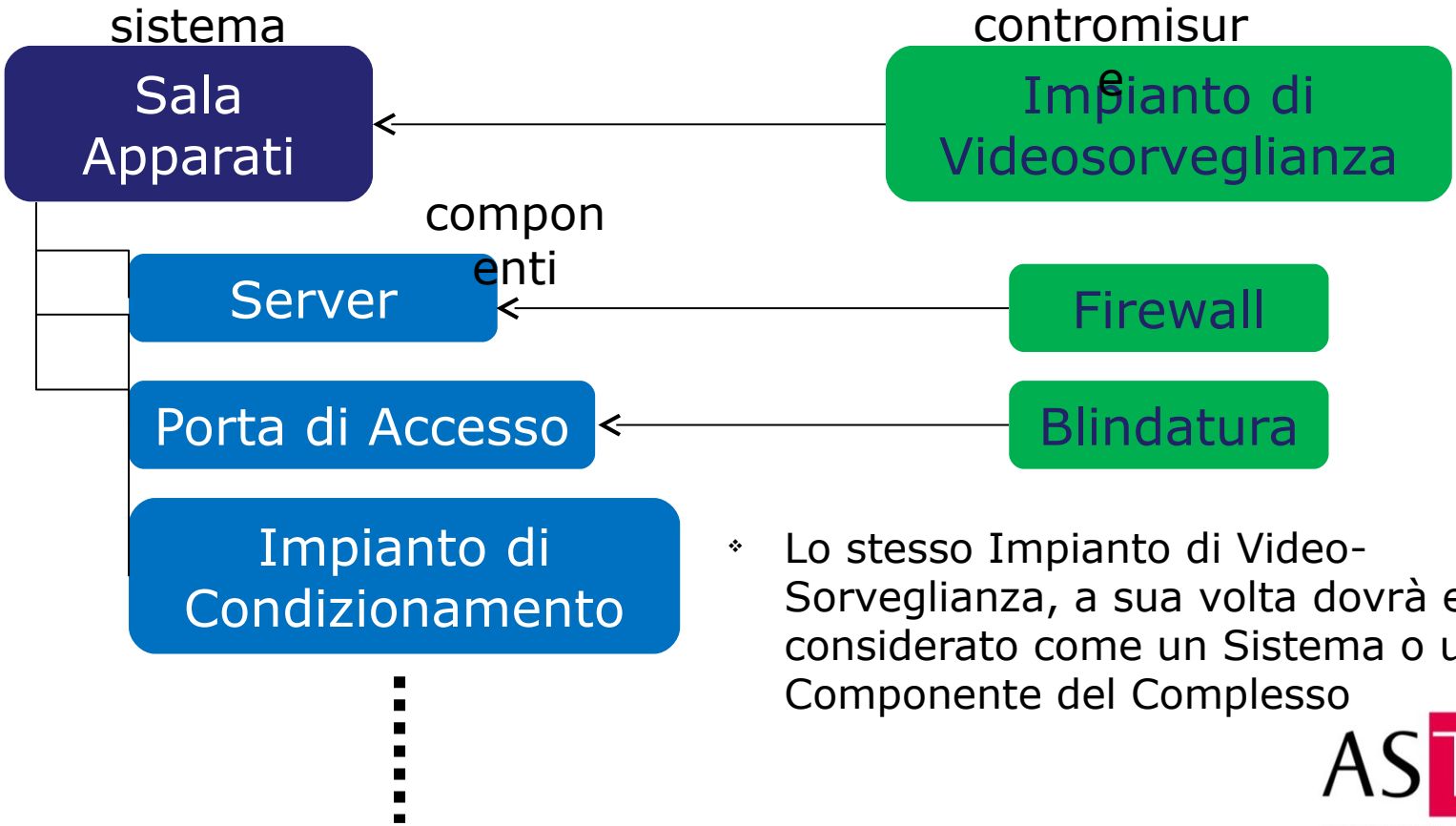




ASTER TECHNOLOGY & ENGINEERING

Tre Architetture per l'Infrastruttura Critica

- La granularità a cui spingere la scomposizione in Componenti si arresta ad un livello **coerente con le Contromisure** che vengono allocate su di essi
- Possibilità di identificare un Sistema come Componente: esempio di una Sala Apparati



- Lo stesso Impianto di Video-Sorveglianza, a sua volta dovrà essere considerato come un Sistema o un Componente del Complesso

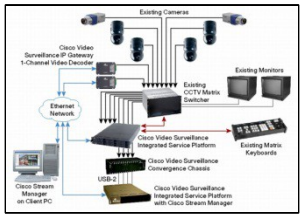
Relazioni tra le Architetture

Controllo Traffico Aereo

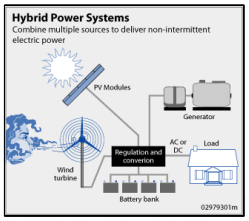
Gestione Sicurezza

Scopi

Produzione Energia



Sistemi



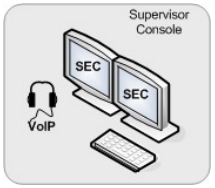
Interfaccia Uomo-macchina

Generazione energia primaria

Funzioni

Acquisizione eco radar

Componenti



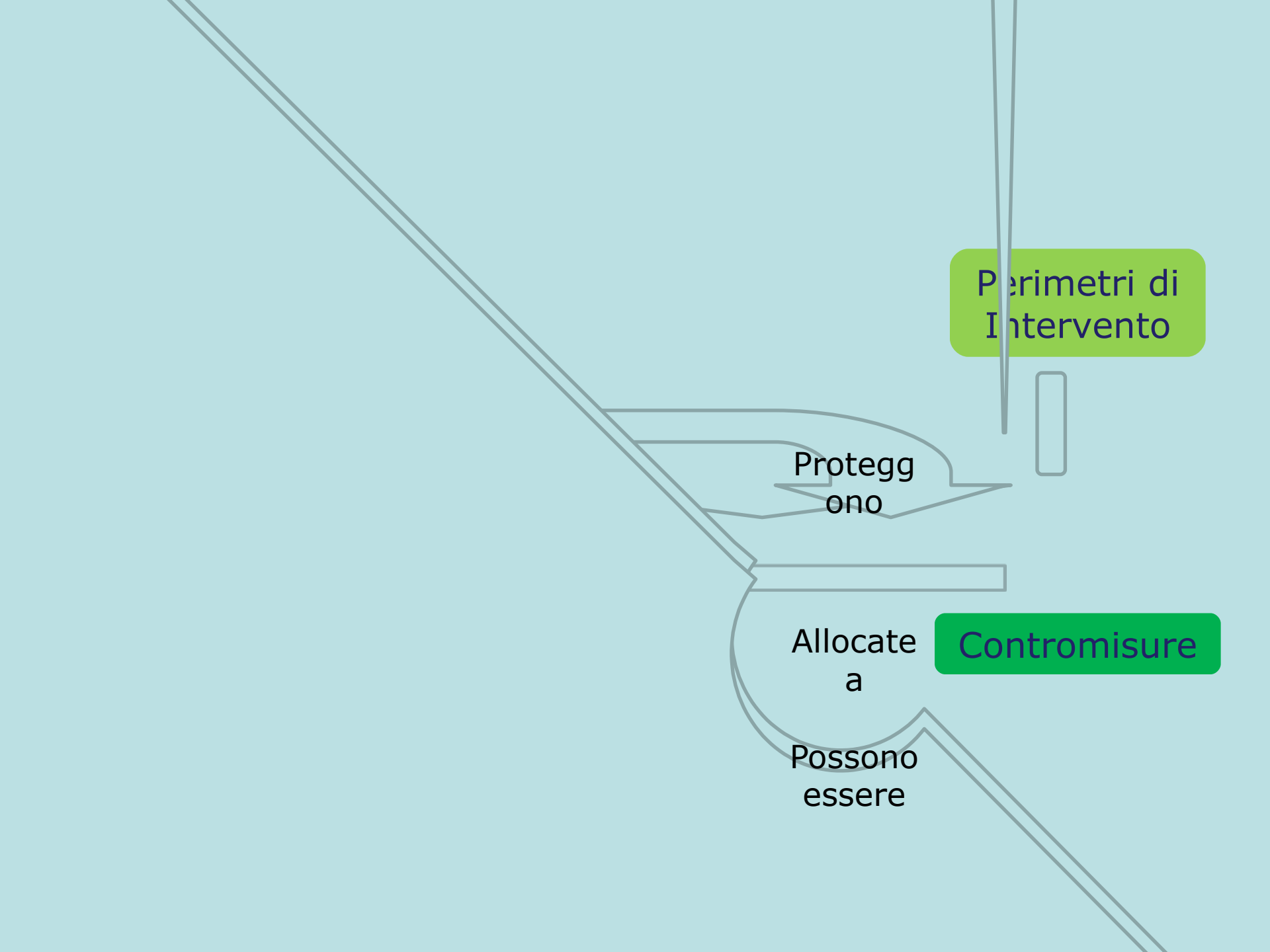
Messa in Sicurezza Processo di Generazione Energia

Perimetri di Intervento

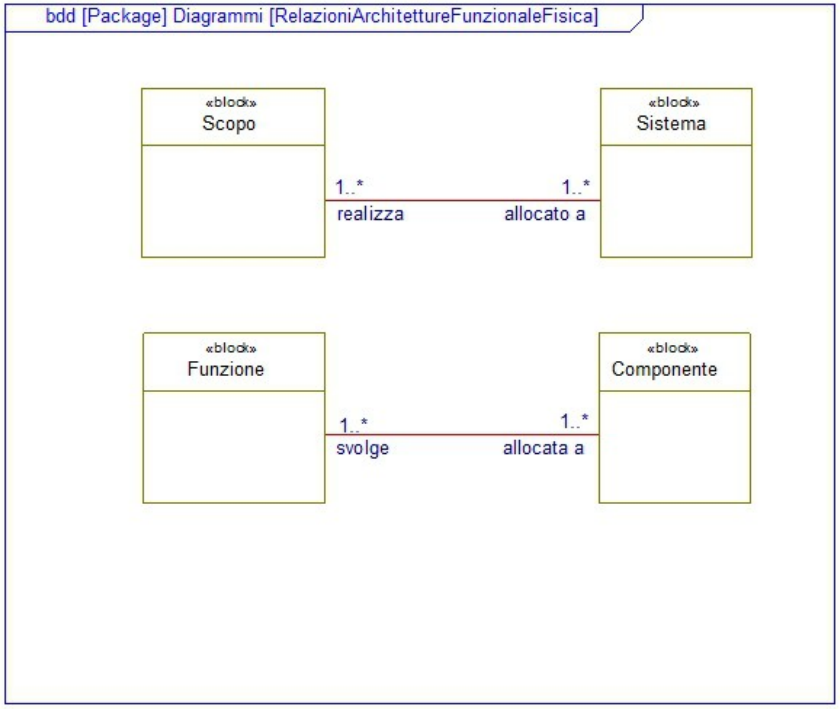
Protezione da attacchi informatici

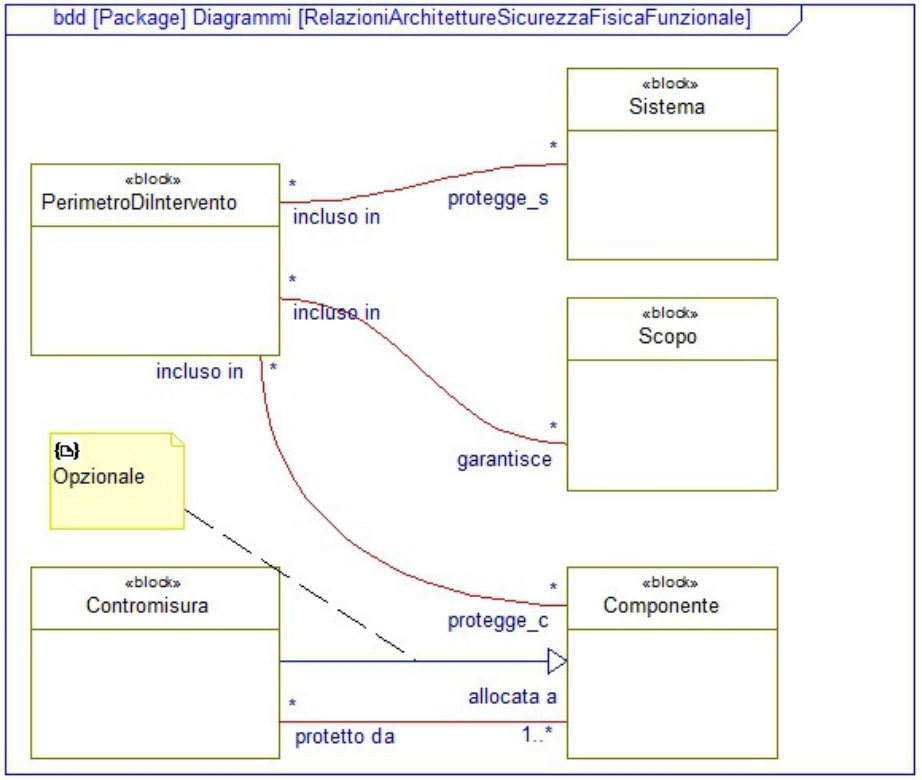
Sicurezza Accessi ed Aree Perimetrali

Contromisure


Perimetri di Intervento
Protegg ono
Allocate a
Contromisure
Possono essere

Relazioni tra le Architetture





ASTER
TECHNOLOGY & ENGINEERING

Realizzano

Quantificat
i da

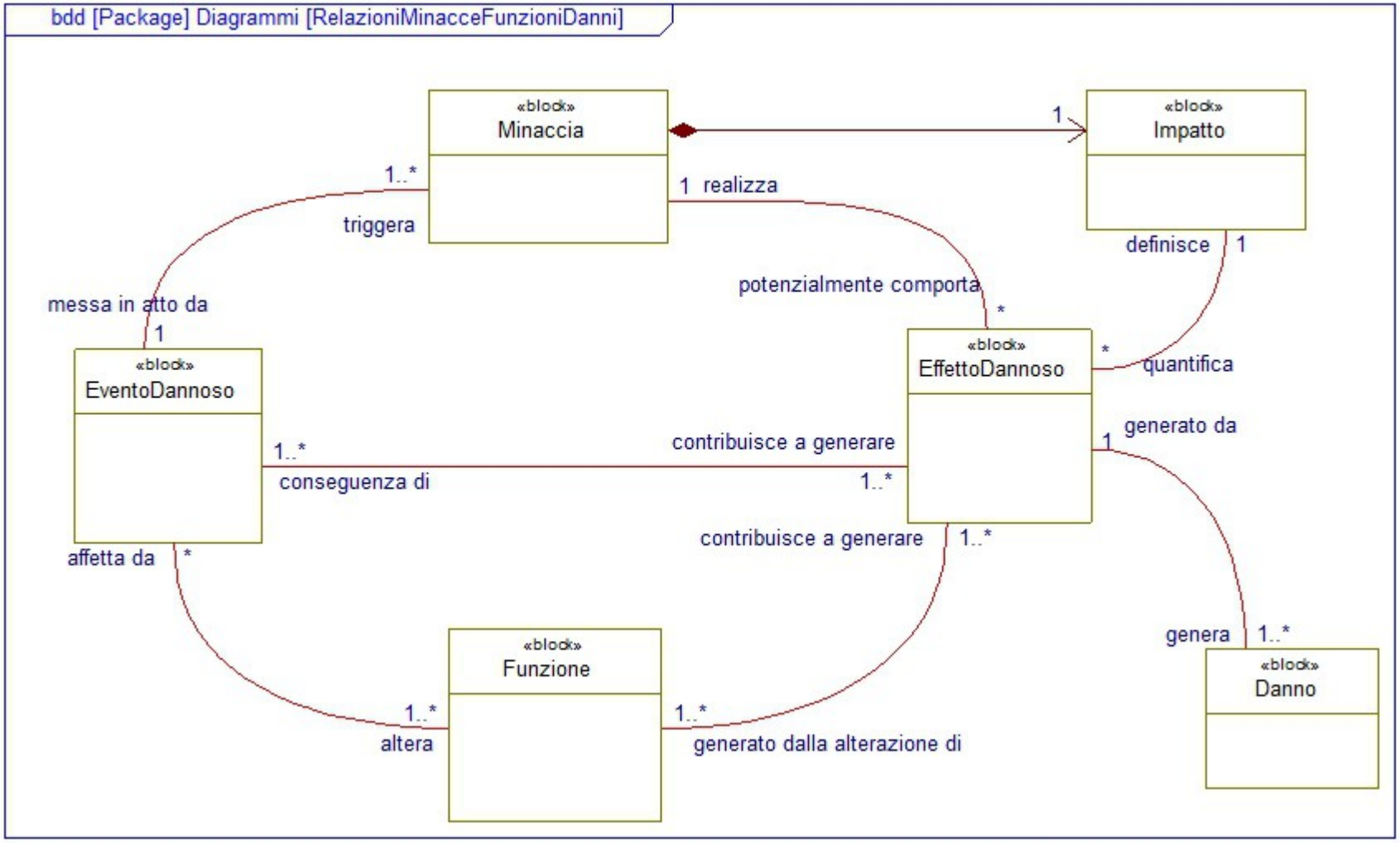
Che
generano

Danni

dei
ponen
l
o

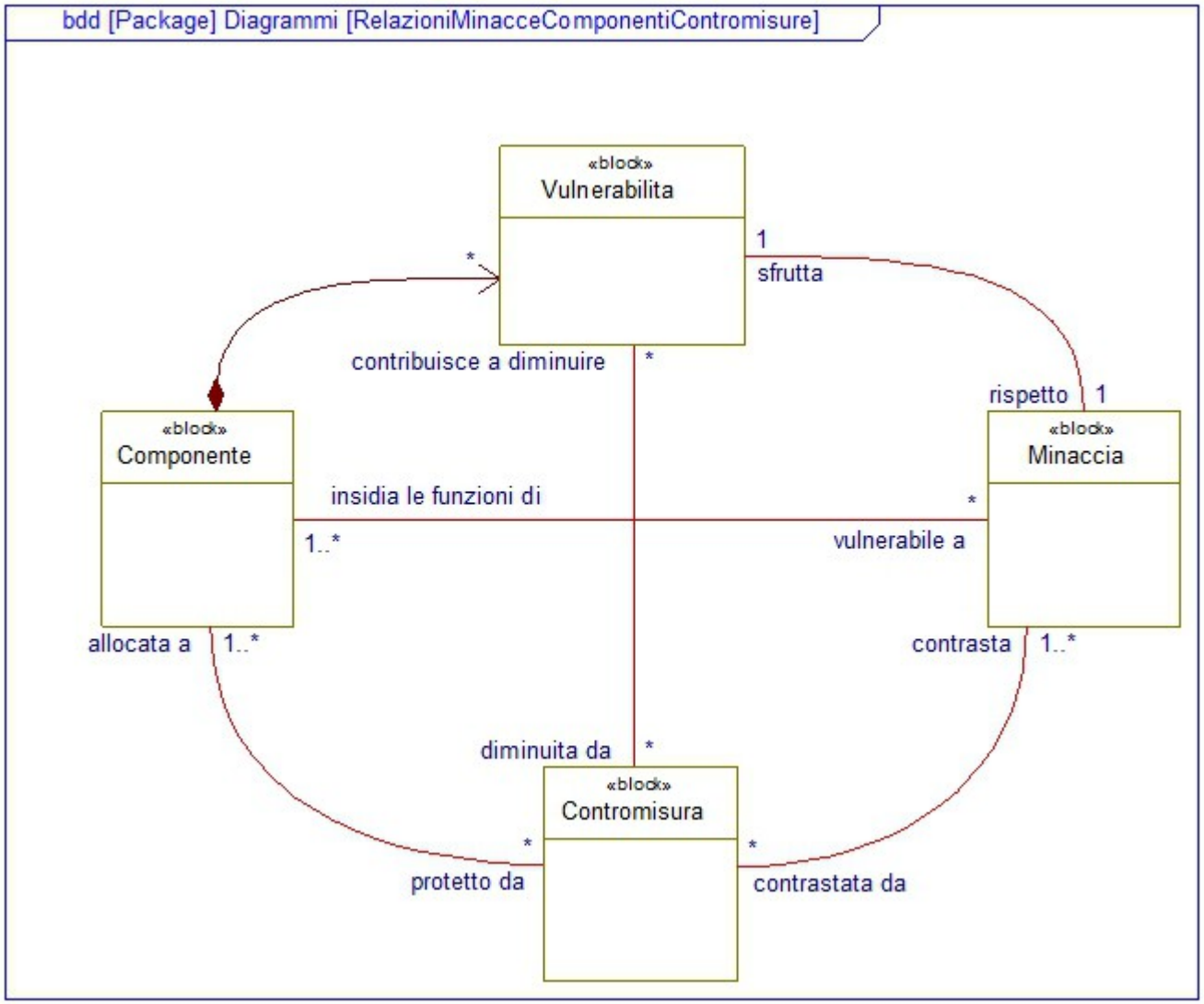
ASTER
TECHNOLOGY & ENGINEERING

Analisi delle Minacce




Si installano sui
Diminuiscono
Contrastano

Analisi delle Minacce: la Vulnerabilità



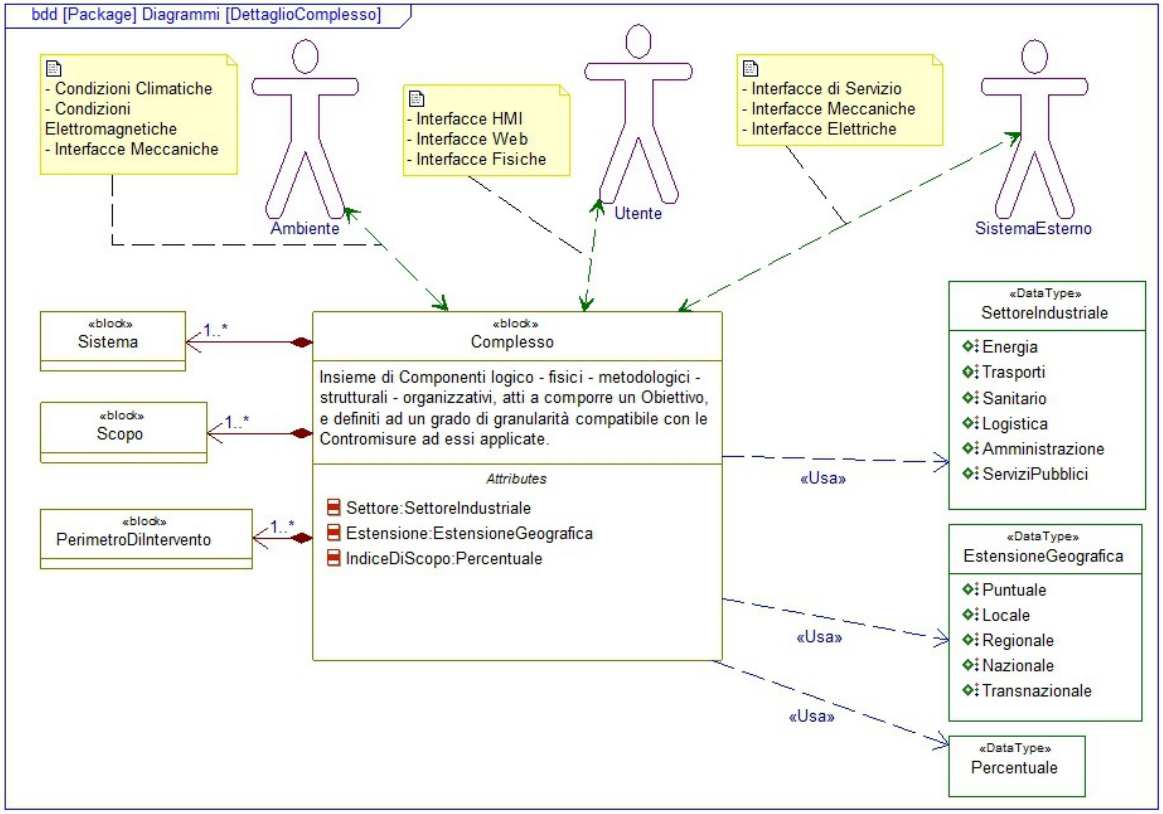
ASTER TECHNOLOGY & ENGINEERING

Elementi del Data Model: Dimensione Componenti

Il Complesso

- **Descrizione**: Insieme di Componenti logico - fisici - metodologici - strutturali - organizzativi, atti a comporre un obiettivo, e definiti ad un grado di granularità compatibile con le contromisure ad essi applicate.

- **Elenco degli Attributi**
  - **Settore Industriale**: [Energia, Trasporti, Sanitario, Logistica, Amministrazione, Servizi Pubblici, …]
  - **Estensione Geografica**: [Puntuale, Locale, Regionale, Nazionale]
  - **Indice di Scopo**: il valore medio degli Indici di Funzionalità dei suoi Componenti riconducibili ad un determinato Scopo, che attesta il grado di attuazione dello Scopo medesimo, espresso come percentuale



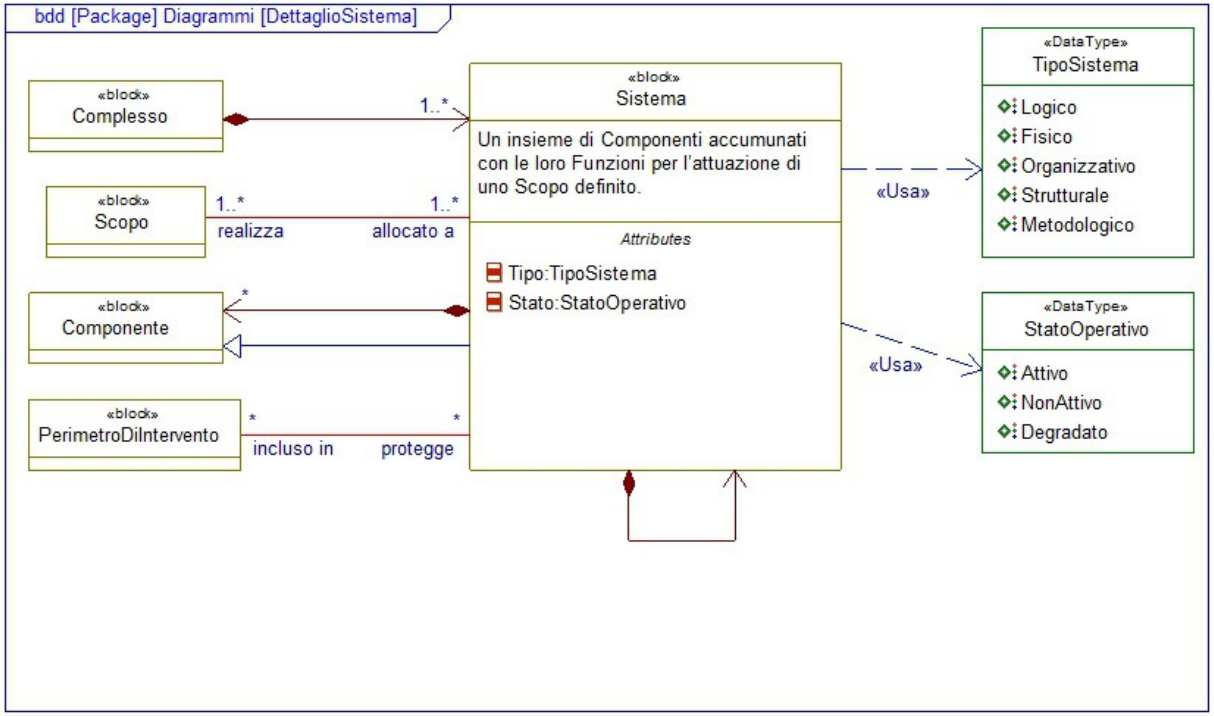
ASTER TECHNOLOGY & ENGINEERING

Elementi del Data Model: Dimensione Componenti

Il Sistema

- **Descrizione**: Un insieme di Componenti accomunati alle loro Funzioni per l'attuazione di uno Scopo definito.

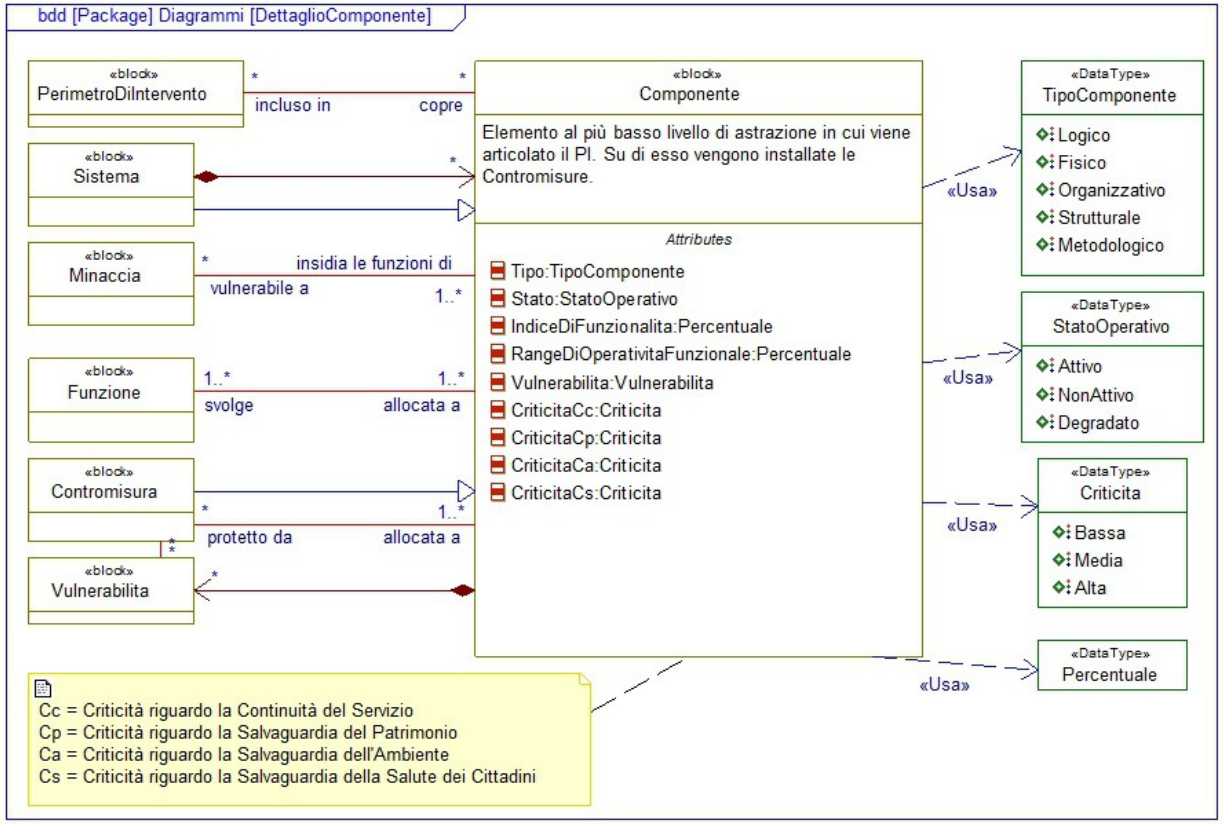
- **Elenco degli Attributi**
  - **Tipo Sistema**: [Logico, Fisico, Organizzativo, Strutturale, Metodologico]
  - **Stato Operativo**: [Attivo, Non Attivo, Degradato]



Elementi del Data Model: Dimensione Componenti

Il Componente

- **Descrizione**: Elemento al più basso livello di astrazione in cui viene articolato il Complesso. Su di esso vengono installate le Contromisure.
- **Elenco degli Attributi**
  - **Tipo Componente**: [Logico, Fisico, Organizzativo, Strutturale, Metodologico]
  - **Stato Operativo**: [Attivo, Non Attivo, Degradato]
  - **Indice Di Funzionalità**: Valore che attesta l'operatività del Componente per quanto riguarda una specifica Funzione, espresso in Percentuale
  - **Range Di Operatività Funzionale**: I valori minimo e massimo dell'Indice di Funzionalità del Componente per quanto riguarda una specifica Funzione
  - **Vulnerabilità**: Misura della incapacità del Componente di contrastare il realizzarsi degli Effetti Dannosi di una specifica Minaccia



- **Criticità Cc, Cp, Ca, Cs**: [Bassa, Media, Alta], rappresenta la criticità del Componente relativamente ad uno specifico tipo di Danno

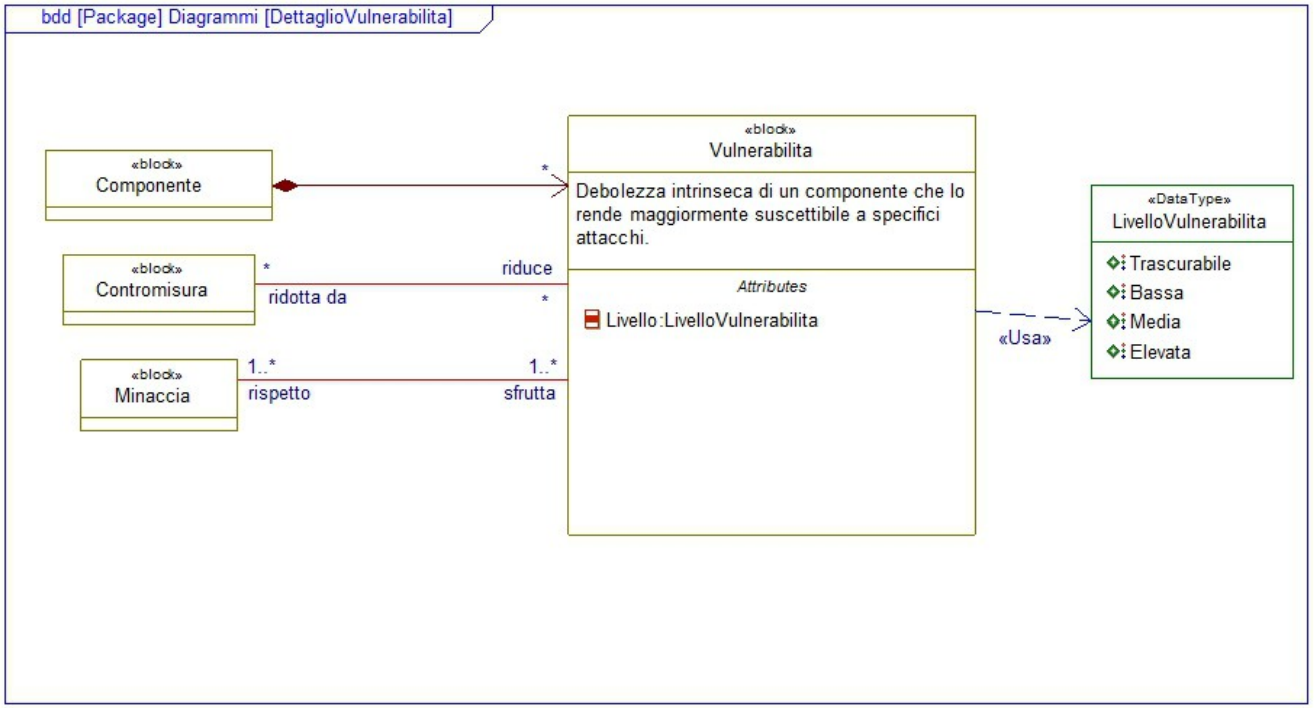
ASTER TECHNOLOGY & ENGINEERING

Elementi del Data Model: Dimensione Componenti

La Vulnerabilità

- **Descrizione**: Debolezza intrinseca di un componente che lo rende maggiormente suscettibile a specifici attacchi.

- **Elenco degli Attributi**
  - **Livello**: [Trascurabile, Bassa, Media, Elevata]

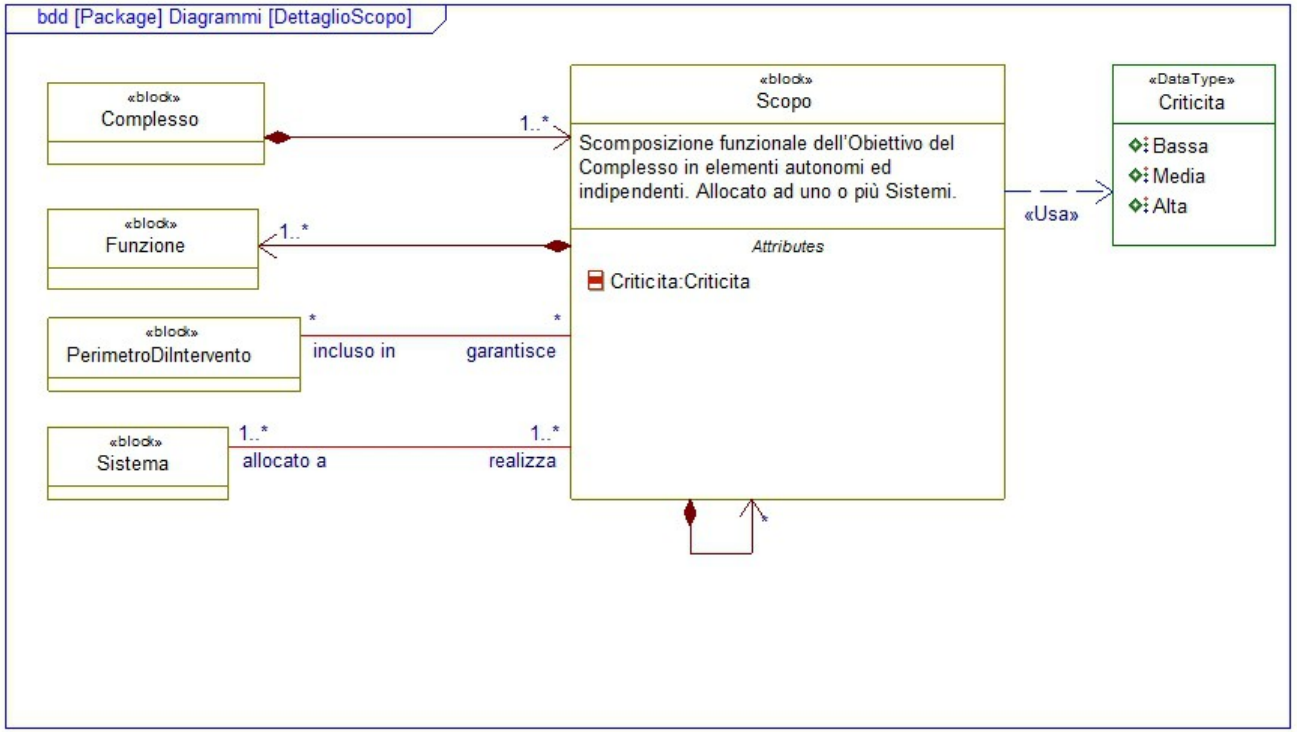


Elementi del Data Model: Dimensione Componenti

Lo Scopo

- **Descrizione**: Scomposizione funzionale dell'Obiettivo del Complesso in elementi autonomi ed indipendenti. Allocato ad uno o più Sistemi.

- **Elenco degli Attributi**
  - **Criticità**: [Bassa, Media, Alta], rappresenta la criticità dello Scopo relativamente al conseguimento dell'Obiettivo del Complesso di cui fa parte



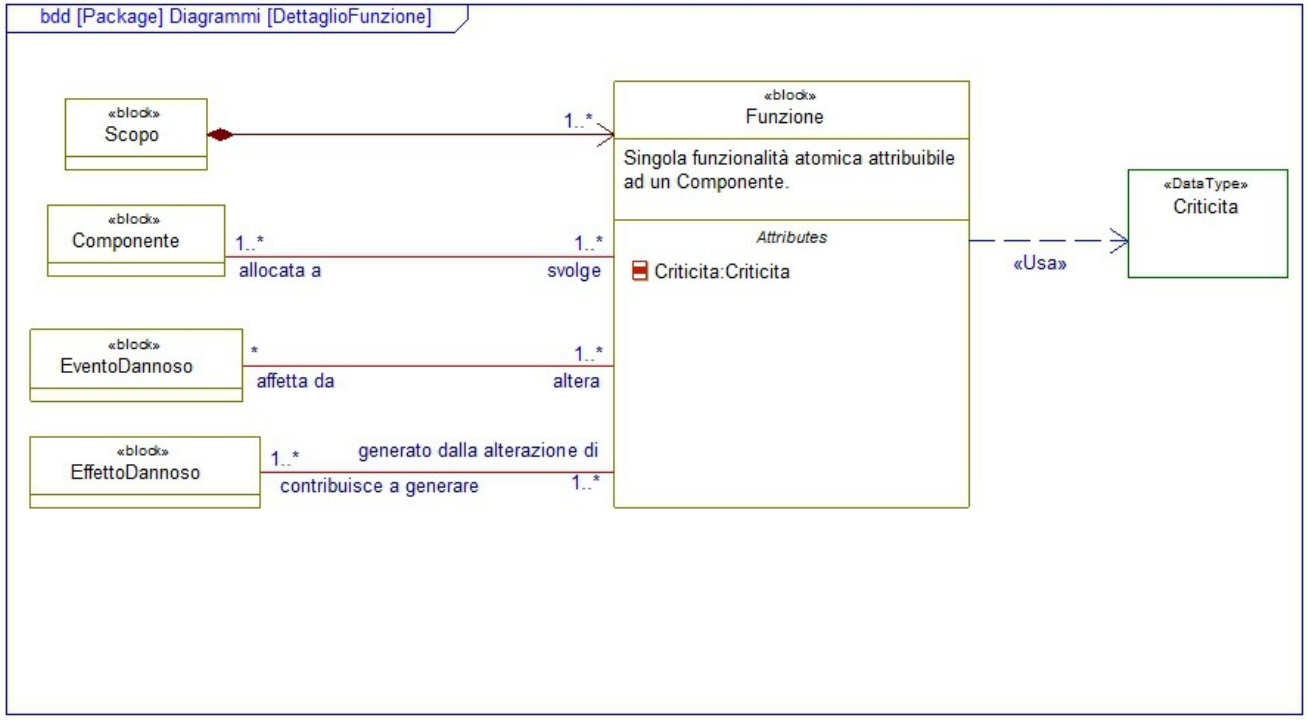
ASTER TECHNOLOGY & ENGINEERING

Elementi del Data Model: Dimensione Componenti

La Funzione

- **Descrizione**: Singola funzionalità atomica attribuibile ad un Componente.

- **Elenco degli Attributi**
  - **Criticità**: [Bassa, Media, Alta], rappresenta la criticità della Funzione relativamente al conseguimento dello Scopo cui fa parte

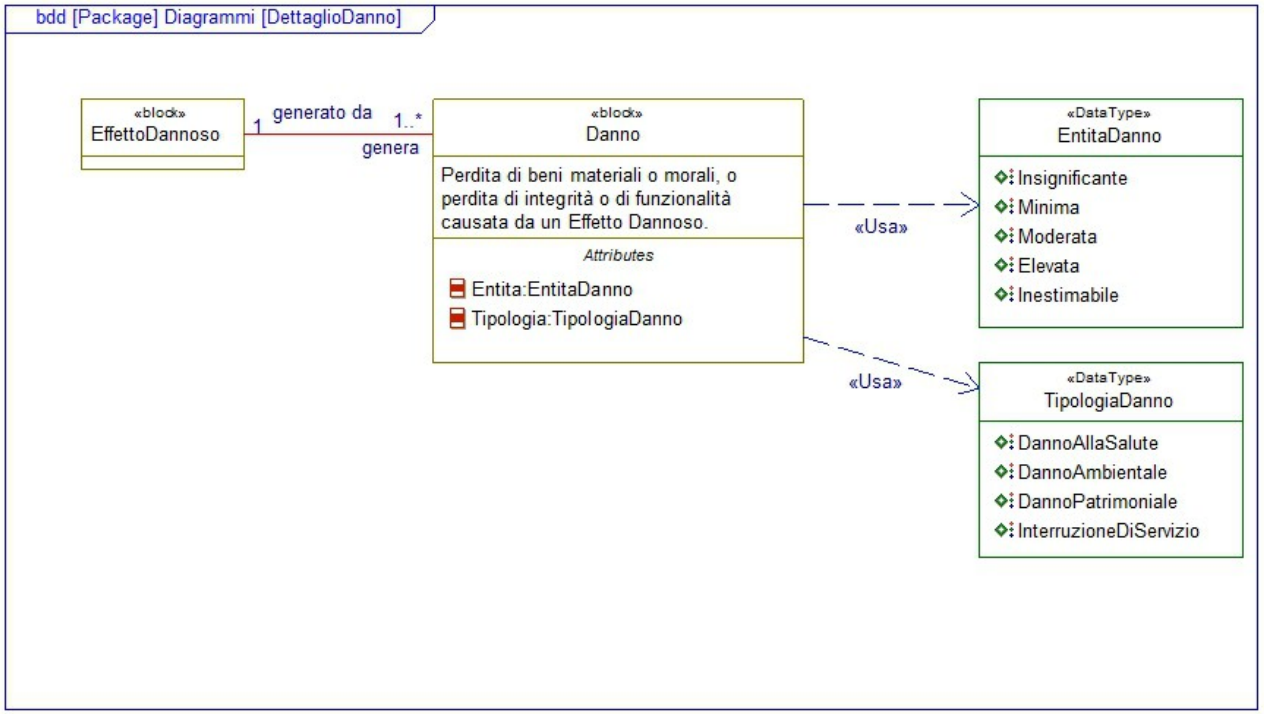


Elementi del Data Model: Dimensione Viste

Il Danno

- **Descrizione**: Perdita di beni materiali o morali, o perdita di integrità o di funzionalità causata da un Effetto Dannoso.

- **Elenco degli Attributi**
  - **Entità**: [Insignificante, Minima, Moderata, Elevata, Inestimabile]
  - **Tipologia**: [Danno Alla Salute, Danno Ambientale, Danno Patrimoniale, Interruzione Di Servizio]

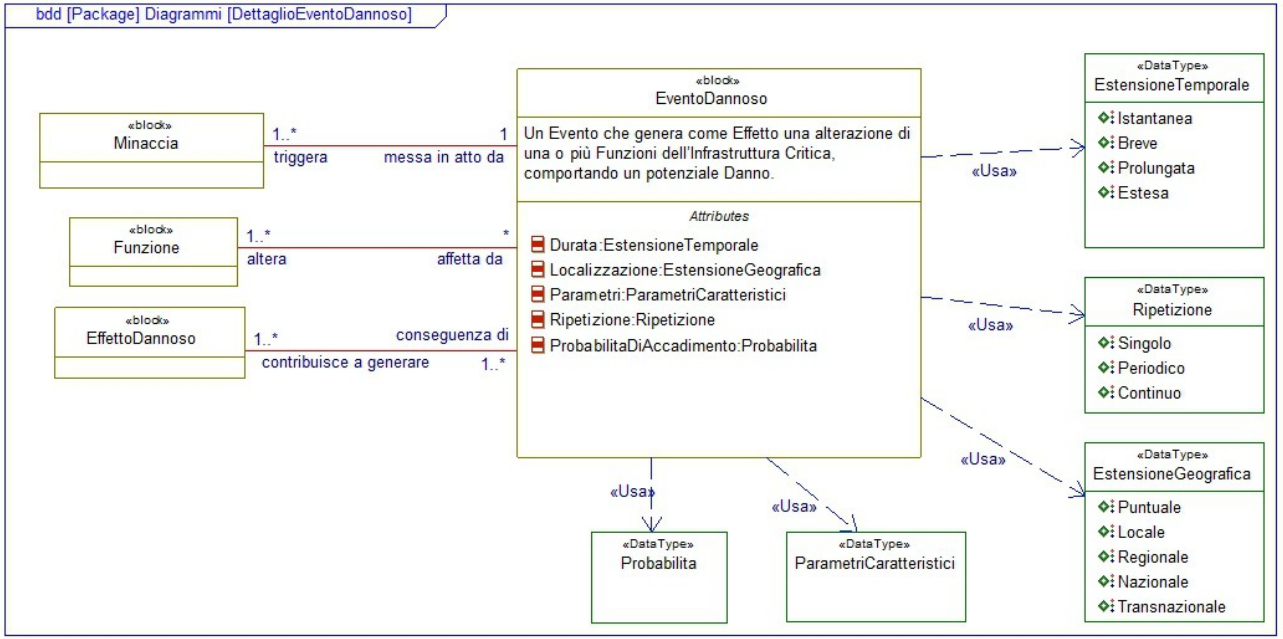


Elementi del Data Model: Dimensione Viste

L'Evento Dannoso (o Attacco, la causa)

- **Descrizione**: Un Evento che genera come Effetto una alterazione di una o più Funzioni dell'Infrastruttura Critica, comportando un potenziale Danno.

- **Elenco degli Attributi**
  - **Durata**: [Istantanea, Breve, Prolungata, Estesa]
  - **Ripetizione**: [Singolo, Periodico, Continuo]
  - **Localizzazione**: [Puntuale, Locale, Regionale, Nazionale, Transnazionale]
  - **Parametri Caratteristici**: i parametri che definiscono nel dettaglio l'Evento
  - **Probabilità di Accadimento**: probabilità che l'Evento abbia luogo

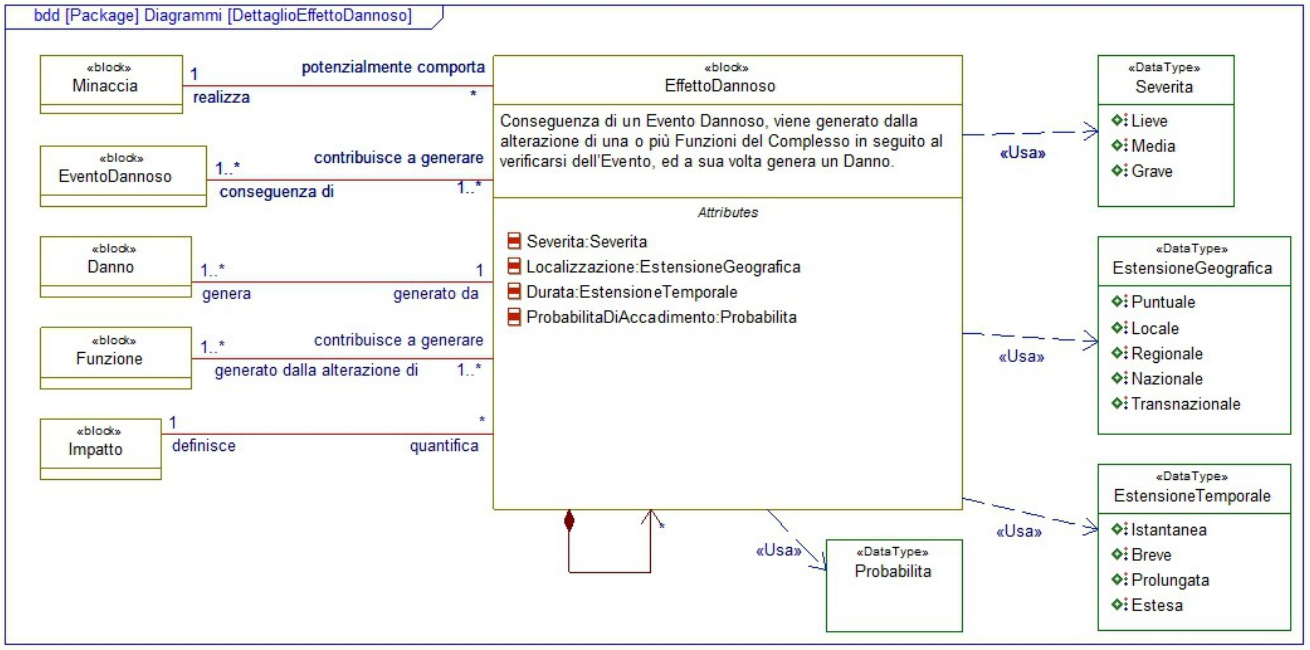


Elementi del Data Model: Dimensione Viste

L'Effetto Dannoso (la conseguenza)

- **Descrizione**: Conseguenza di un Evento Dannoso; viene generato dalla alterazione di una o più Funzioni del Complesso in seguito al verificarsi dell'Evento Dannoso, ed a sua volta genera un Danno.

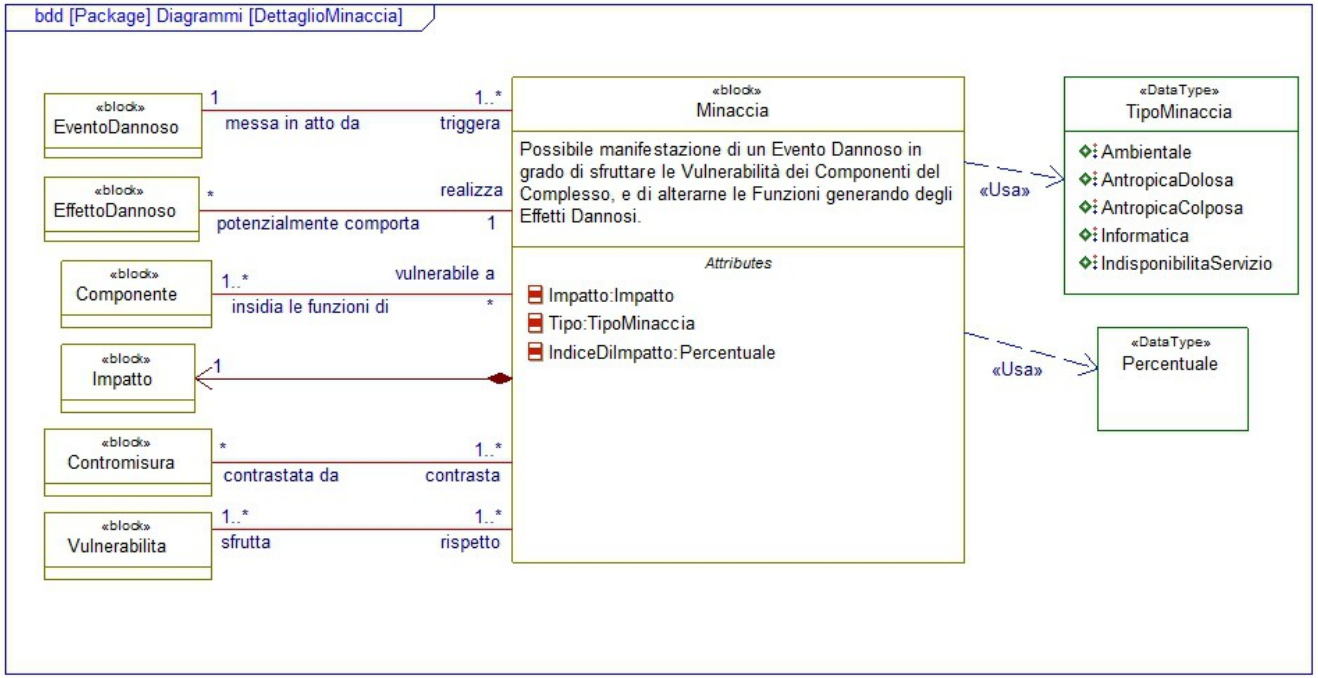
- **Elenco degli Attributi**
  - **Severità**: [Lieve, Media, Grave], in ragione dell'entità dei Danni associati
  - **Durata**: [Istantanea, Breve, Prolungata, Estesa]
  - **Localizzazione**: [Puntuale, Locale, Regionale, Nazionale, Transnazionale]
  - **Probabilità di Accadimento**: probabilità che l'Effetto abbia luogo



Elementi del Data Model: Dimensione Viste

La Minaccia

- **Descrizione**: Possibile manifestazione di un Evento Dannoso in grado di sfruttare le Vulnerabilità dei Componenti del Complesso, e di alterarne le Funzioni generando degli Effetti Dannosi.



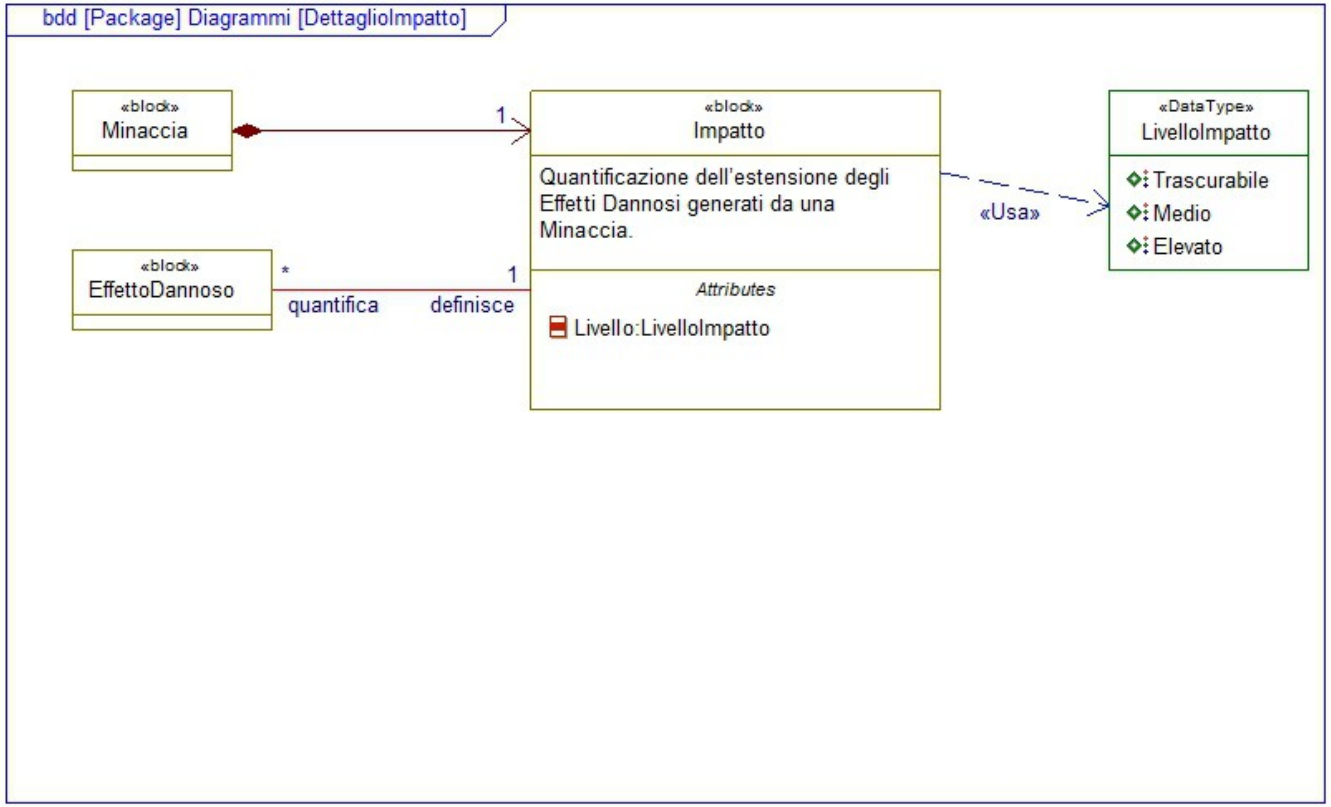
- **Elenco degli Attributi**
  - **Impatto**: una quantificazione dell'estensione degli Effetti Dannosi causati dalla Minaccia
  - **Tipo**: [Ambientale, Antropica Dolosa, Antropica Colposa, Informatica, Indisponibilità di Servizio]
  - **Indice di Impatto**: in relazione ad uno specifico Componente, rappresenta il valore che la Minaccia oppone alla realizzazione dell'Indice di Funzionalità del Componente, espresso in percentuale

Elementi del Data Model: Dimensione Viste

L'Impatto

- **Descrizione**: Quantificazione dell'estensione degli Effetti Dannosi generati da una Minaccia.

- **Elenco degli Attributi**
  - **Livello**: [Trascurabile, Medio, Elevato]

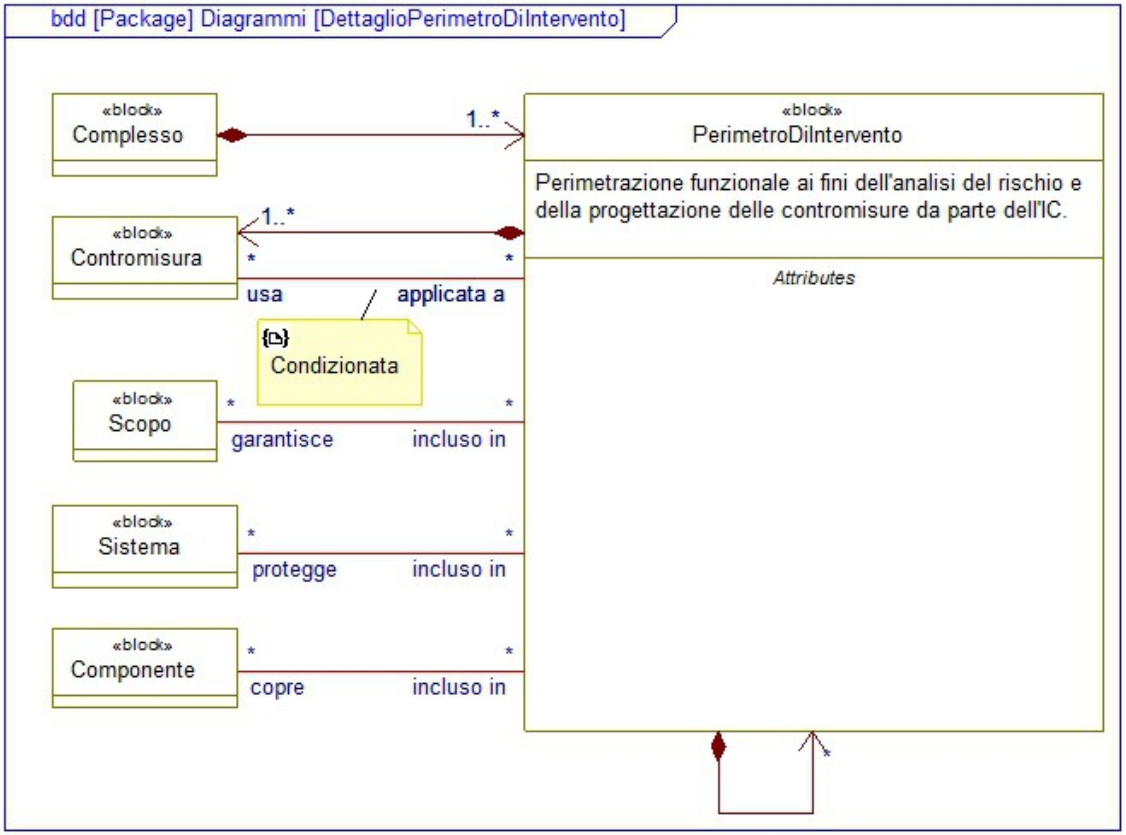


Elementi del Data Model: Dimensione Contromisure

Il Perimetro di Intervento

- **Descrizione**: Perimetrazione funzionale ai fini dell'analisi del rischio e della progettazione delle contromisure da parte dell'Infrastruttura Critica.

- **Elenco degli Attributi**
  - **N/A**

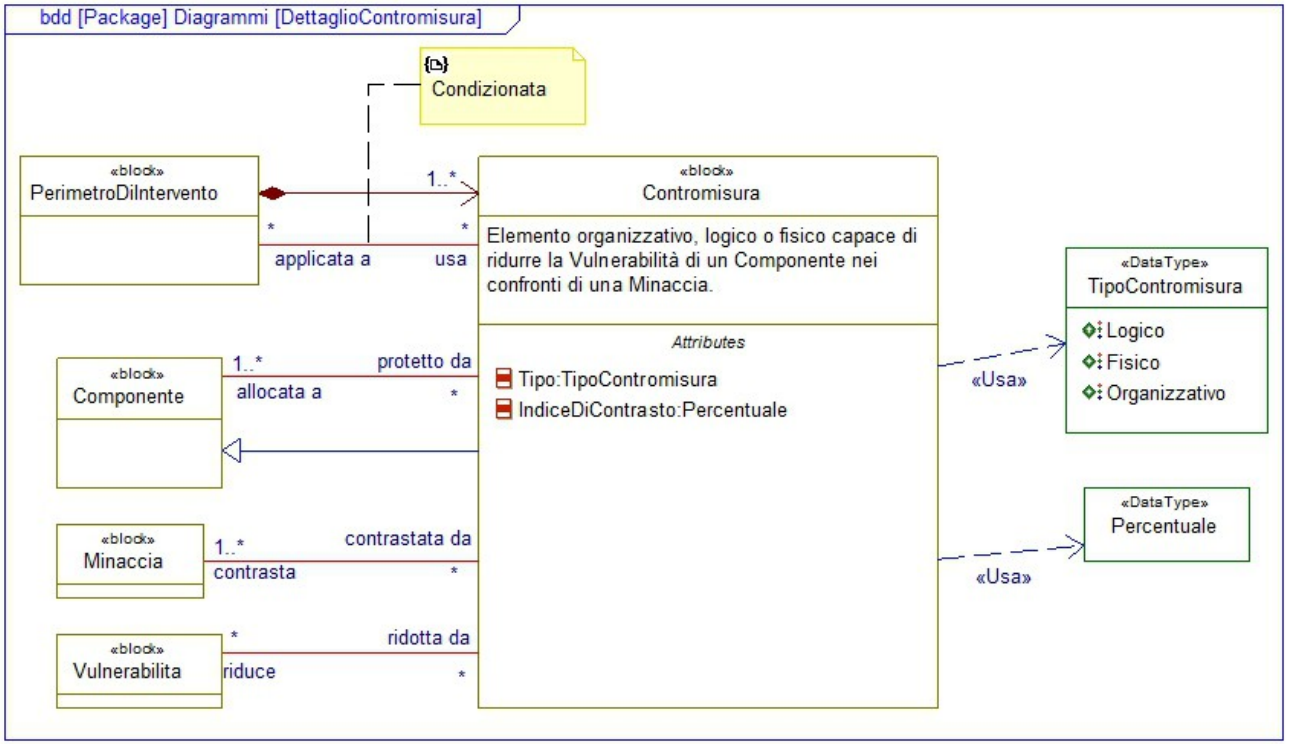


Elementi del Data Model: Dimensione Contromisure

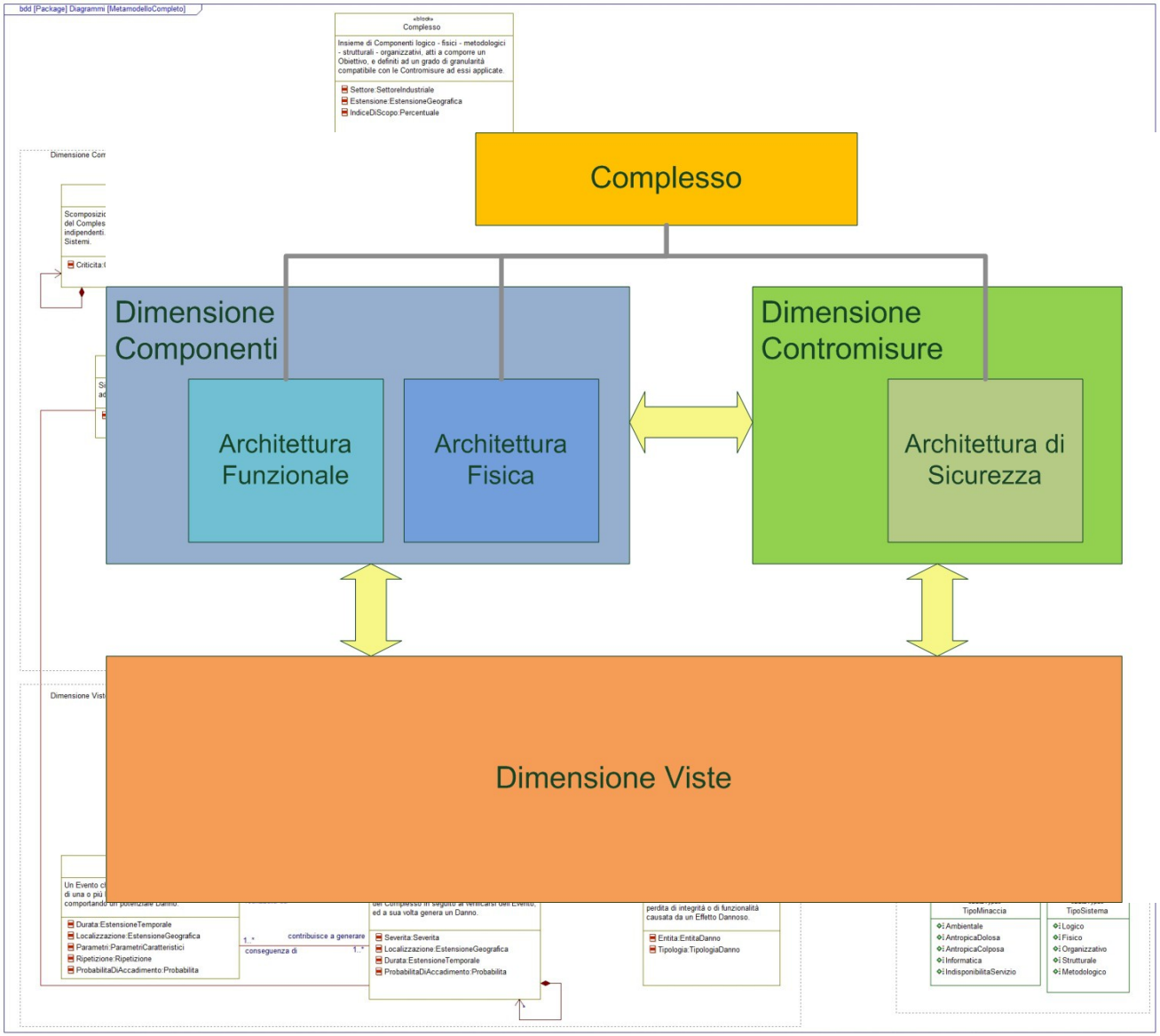
La Contromisura

- **Descrizione**: Elemento organizzativo, logico o fisico capace di ridurre la Vulnerabilità di un Componente nei confronti di una Minaccia.

- **Elenco degli Attributi**
  - **Tipo**: [Logico, Fisico, Organizzativo]
  - **Indice di Contrasto**: in relazione ad una specifica Minaccia che insidia una Funzione di un Componente, rappresenta il valore che la Contromisura oppone alla realizzazione della Minaccia, ripristinando l'Indice di Funzionalità del Componente, espresso in percentuale



Data Model Completo

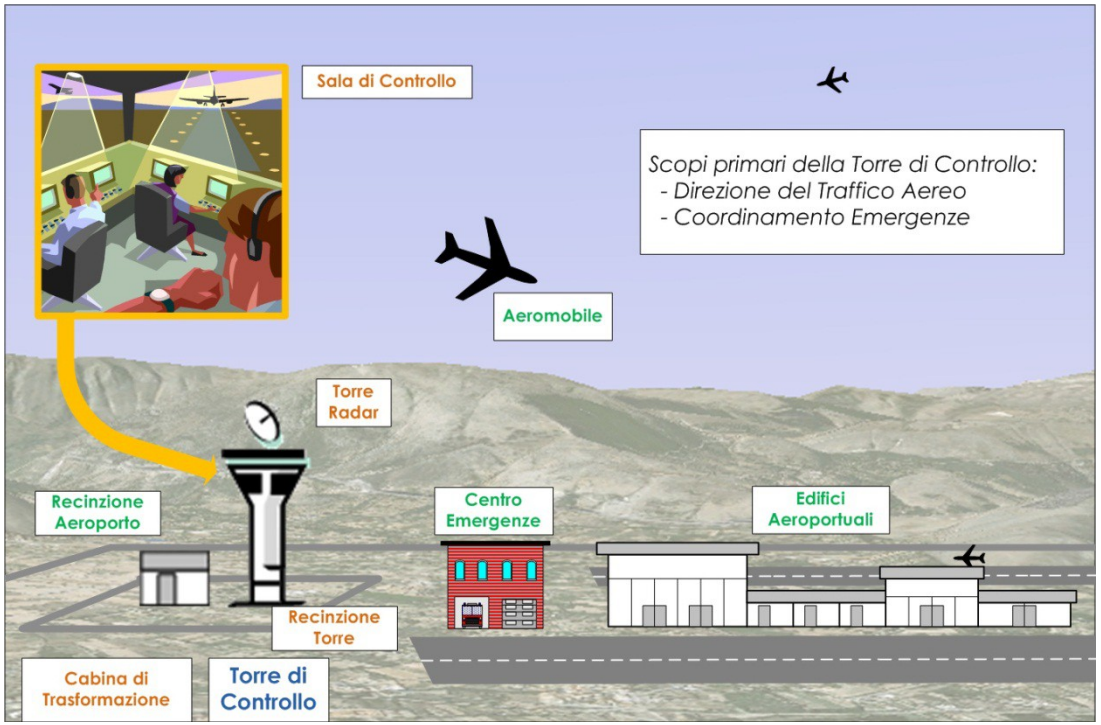


Tipi di Dati

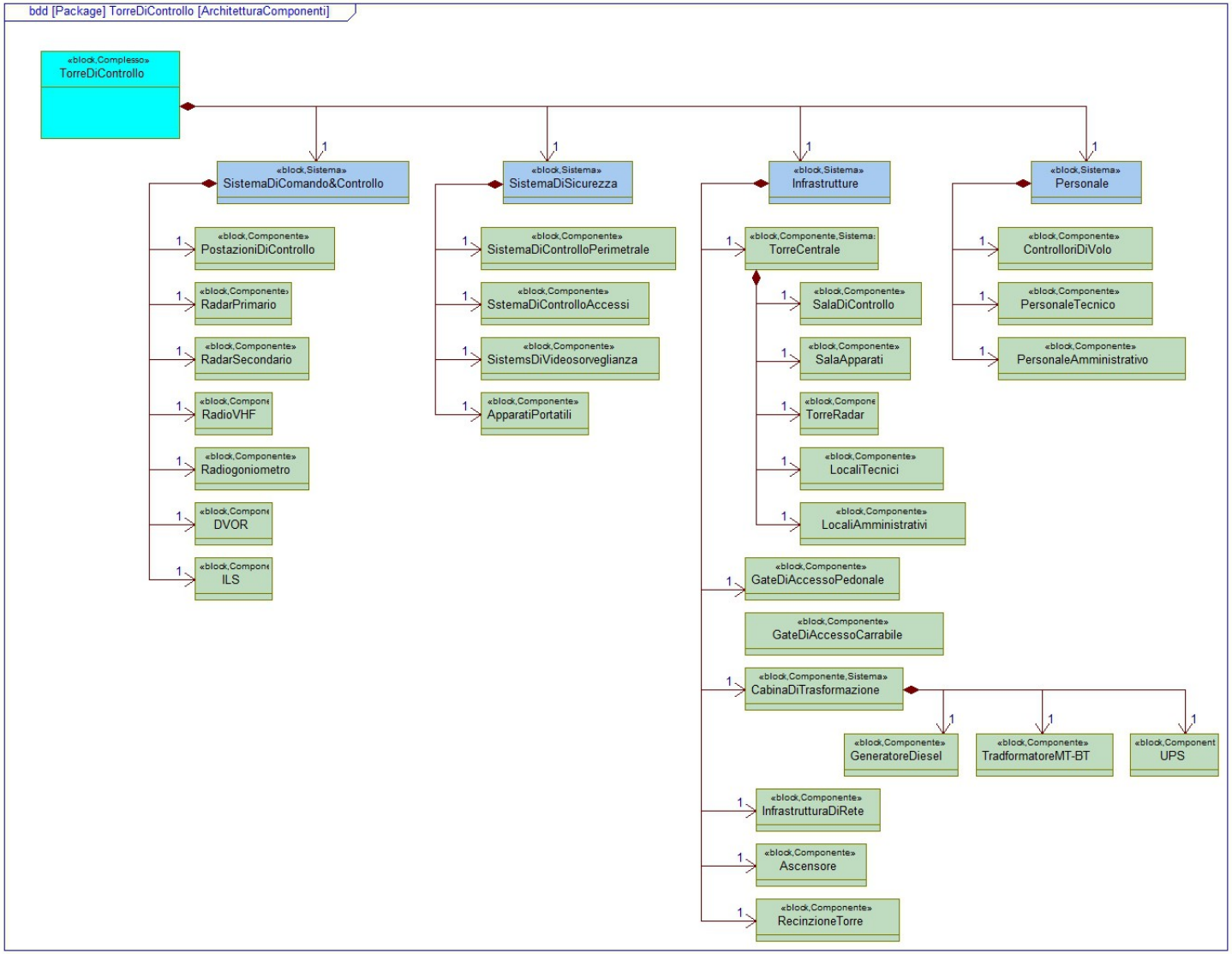
ASTER TECHNOLOGY & ENGINEERING

Applicazioni del Data Model: Torre di Controllo

- Analisi di Rischio su un sistema campione: Torre di Controllo
  - Analisi del Contesto
  - Architettura Fisica
  - Architettura Funzionale
  - Allocazione Funzionale
  - Generazione DB delle entità in SQL
  - Esempio di scheda di progettazione Contromisure



Applicazioni del Data Model: Torre di Controllo

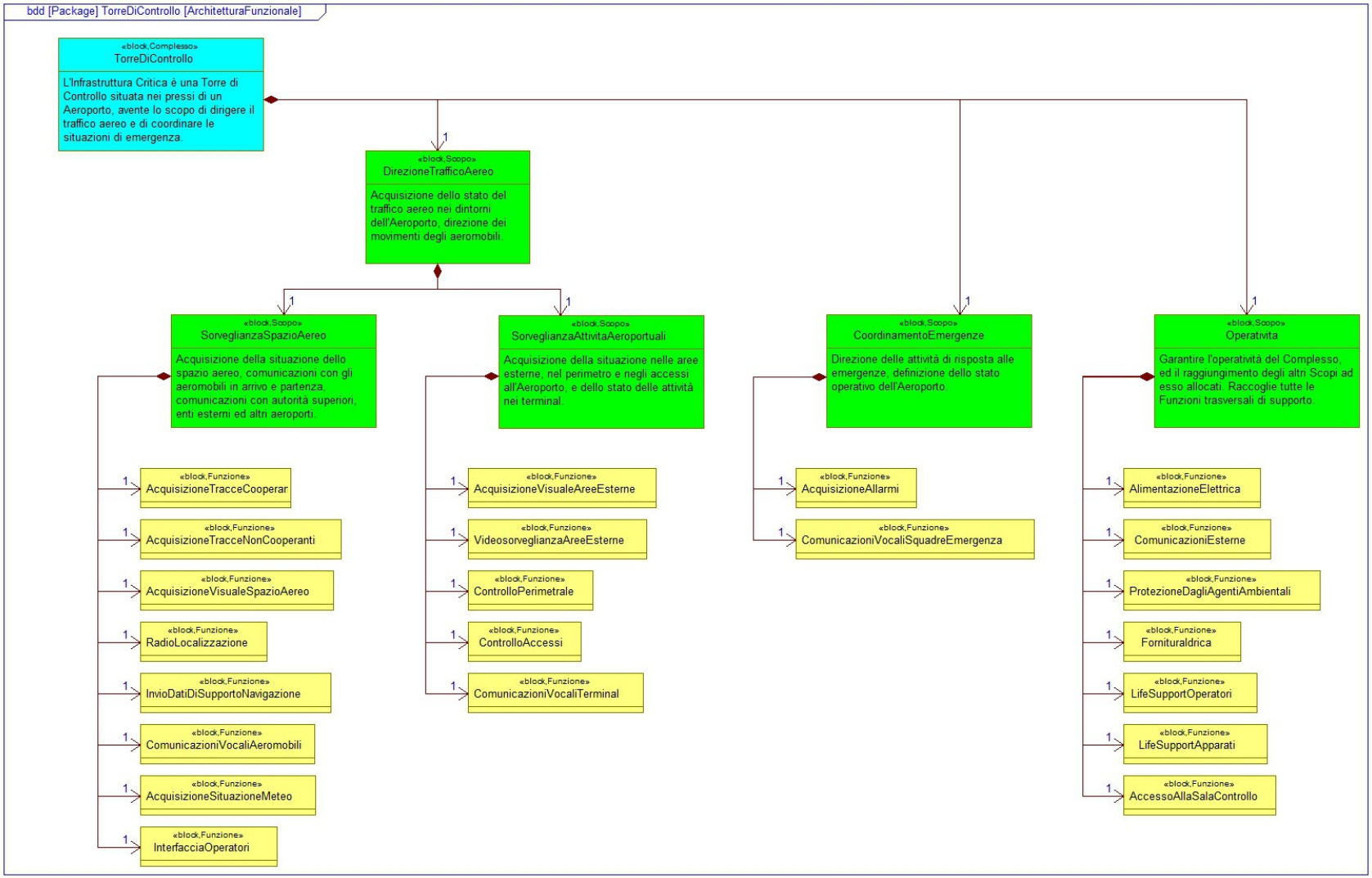


- Architettura Fisica

ASTER
TECHNOLOGY & ENGINEERING

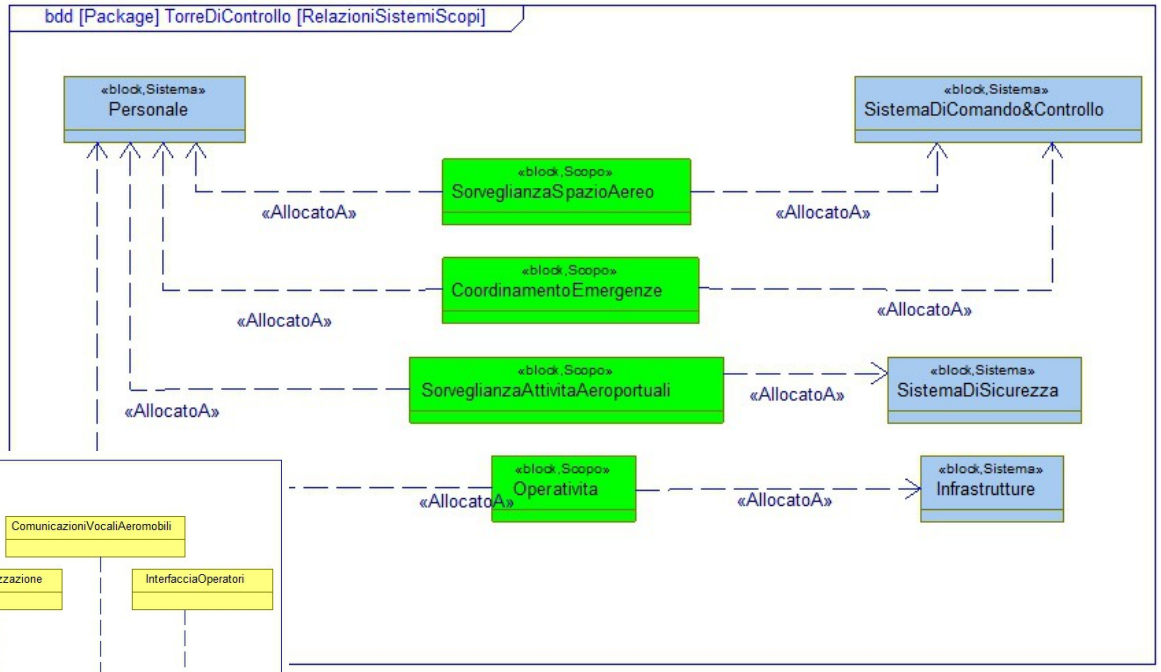
Applicazioni del Data Model: Torre di Controllo

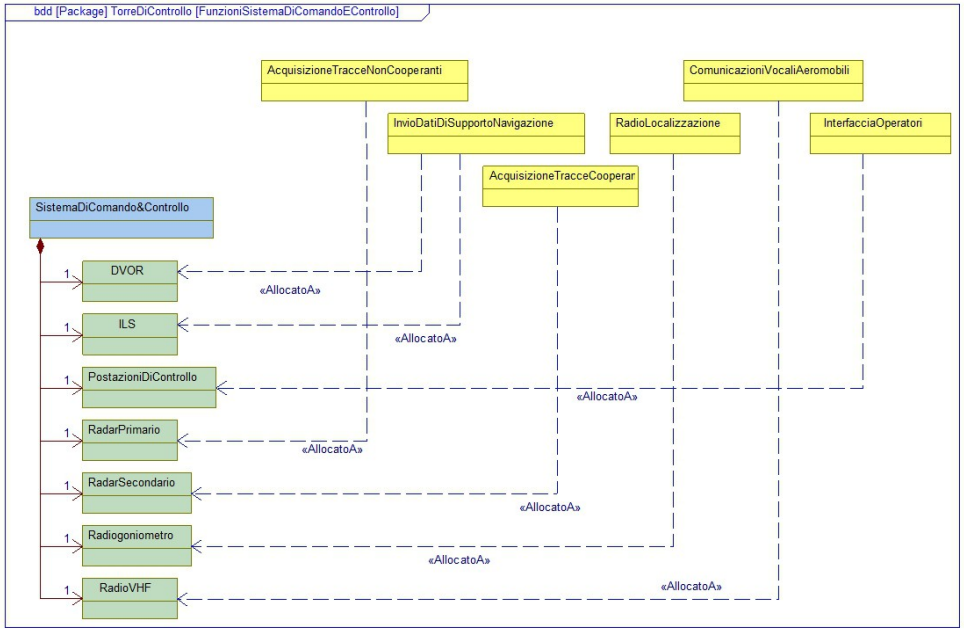
- Architettura Funzionale



Applicazioni del Data Model: Torre di Controllo

- Allocazione Funzionale ai Componenti Fisici





ASTER
TECHNOLOGY & ENGINEERING

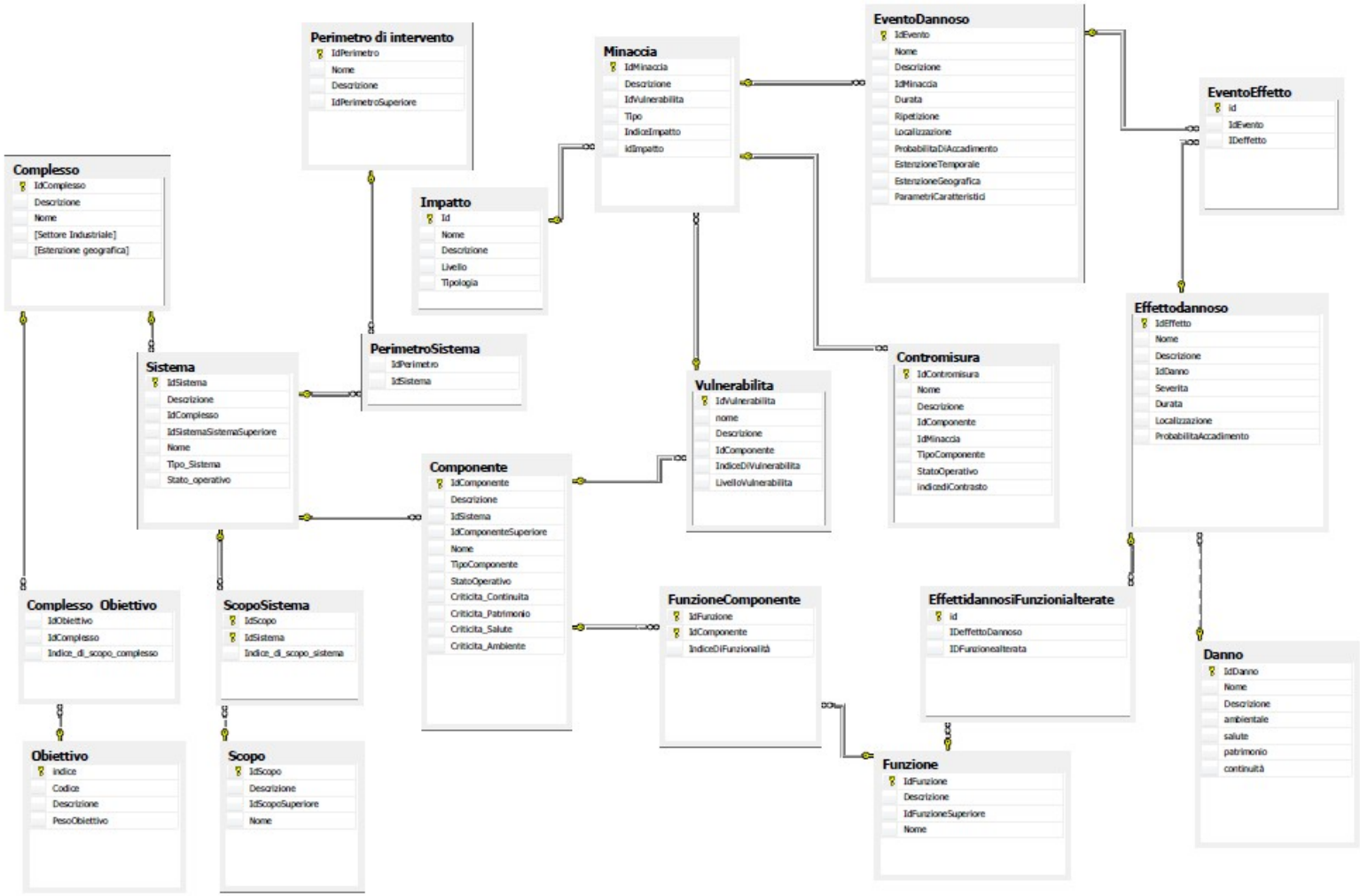
Applicazioni del Data Model: Torre di Controllo

- Allocazione Funzionale ai Componenti Fisici

FUNZIONI \ COMPONENTI	ApparatiPortatili	Ascensore	CabinaDiTrasformazione	DVOR	GateDiAccessoPedonale	GeneratoreDiesel	ILS	InfrastrutturaDiRete	PostazioniDiControllo	RadarPrimario	RadarSecondario	Radiogoniometro	RadioVHF	SalaApparati	SalaDiControllo	SstemaDiControlloAccessi	SistemaDiControlloPerimetrale	SistemsDiVideosorveglianza	TorreCentrale	TorreRadar	TradformatoreMT-BT	RecinzioneTorre	GateDiAccessoCarrabile	UPS	LocaliTecnici	ControlloriDiVolo	PersonaleTecnico	LocaliAmministrativi	PersonaleAmministrativo
AccessoAllaSalaControllo		X			X																		X						
AcquisizioneAllarmi																X	X	X											
AcquisizioneSituazioneMeteo																													
AcquisizioneTracceCooperanti											X																		
AcquisizioneTracceNonCooperanti										X																			
AcquisizioneVisualeAreeEsterne															X				X							X	X		
AcquisizioneVisualeSpazioAereo															X				X							X	X		
AlimentazioneElettrica			X			X															X			X					
ComunicazioniEsterne	X							X					X																X
ComunicazioniVocaliAeromobili													X														X		
ComunicazioniVocaliSquadreEmergenza	X																										X		X
ComunicazioniVocaliTerminal	X																										X		X
ControlloAccessi																X													X
ControlloPerimetrale																	X					X							X
FornituraIdrica																									X				
InterfacciaOperatori									X																				
InvioDatiDiSupportoNavigazione				X			X																						
LifeSupportApparati														X													X		
LifeSupportOperatori		X													X				X									X	
ProtezioneDagliAgentiAmbientali														X	X				X	X									
RadioLocalizzazione												X																	
VideosorveglianzaAreeEsterne																		X											X

Applicazioni del Data Model: Torre di Controllo

- Generazione di un Database in SQL per l'analisi dei rischi



ASTER
TECHNOLOGY & ENGINEERING

Applicazioni del Data Model: Torre di Controllo

- Generazione di un Database in SQL per l'analisi dei rischi

COMPONENTE		SISTEMA		SCOPO	
Cabina di Trasformazione		Infrastrutture		Garantire l'Operatività del Complesso	
EVENTO		VULNERABILITA'		MINACCIA	
E007	Accessi bloccati alla Cabina di Trasformazione	V08	I locali, contenenti il gruppo di continuità, possono essere inagibili per un blocco delle porte motorizzate	M08	Inagibilità locali generatore
FUNZIONE ALTERATA		EFFETTO		DANNO	
Life Support Apparati		EFD007	Impossibilità di eseguire la manutenzione ordinaria e straordinaria sugli apparati di produzione energia ausiliaria	D007	Danneggiamento degli apparati, mancanza energia elettrica ausiliaria
DANNO		TIPOLOGIA			
D007	Mancanza energia elettrica ausiliaria	SALUTE	AMBIENTE	PATRIMONIO	CONTINUITA'
ENTITA' DEL DANNO		Minima	Minima	Moderata	Elevata
CONTROMISURA					
CM07	Prevedere un accesso di emergenza alla Cabina di Trasformazione				

Applicazioni del Data Model: Un nuovo modello per l'analisi del Rischio nelle IC

- Approccio tipico alla definizione di Rischio:
  - ✓ R = PD x IM, dove:
  - ✓ PD è la probabilità che si verifichi il Danno associato alla Minaccia M
  - ✓ IM, l'Impatto, è una quantificazione dell'entità del Danno

RISCHIO		PROBABILITÀ DI ACCADIMENTO DEGLI EFFETTI DANNOSI		
		RARO	POSSIBILE	PROBABILE
IMPATTO DELLA MINACCIA	ELEVATO	Rischio medio	Rischio alto	Rischio alto
	MEDIO	Rischio basso	Rischio medio	Rischio alto
	TRASCURABILE	Rischio basso	Rischio basso	Rischio medio

Applicazioni del Data Model: Un nuovo modello per l'analisi del Rischio nelle IC

- Comunemente si esegue una sintesi basata sul Componente, cioè si cerca di esprimere il valore di RC, facendo la sommatoria su tutte le Minacce Mi che insistono su di esso:
  - ✓ $RC = \sum i (PDi \times IMi) = \sum i (VCMi \times PMi \times IMi)$

- Nella formula si è fatto uso della relazione che collega la **Probabilità di Accadimento del Danno** (PDi, legata agli Effetti Dannosi) alla **Probabilità di Accadimento della Minaccia** (PMi, legata agli Eventi Dannosi), e che passa attraverso l'espressione della Vulnerabilità del Componente i nei confronti della Minaccia Mi, VCMi:
  - ✓ $PDi = VCMi \times PMi$

- Questo perché si vogliono categorizzare tutti i Componenti facenti parte del nostro Perimetro di Intervento, e capire quale presenta il **livello di Rischio maggiore**, in modo da implementare per prime le Contromisure che lo riguardano. In questo caso, è necessario definire le PMi, ed eseguire la sommatoria su i.

Applicazioni del Data Model: Un nuovo modello per l'analisi del Rischio nelle IC

- Limiti dell'approccio:
  - ✓ Quando la Probabilità di Accadimento della Minaccia è estremamente bassa, il valore di Rischio viene abbattuto indipendentemente dal **valore del Danno**, il quale oltretutto risulta particolarmente **difficile da quantificare**, quando in gioco ci sono fattori Ambientali, di Salute del Cittadino, o di Continuità dei Servizi erogati da Infrastrutture Critiche
  - ✓ Nel mondo reale Eventi Dannosi con probabilità **«estremamente bassa»** avvengono piuttosto di frequente

- Il suggerimento che è stato delineato durante l'attività del GdL Data Model, **non ancora completamente formalizzato ed in corso di elaborazione**, consiste nell'individuazione di una grandezza rappresentante il Rischio aggregata in base alla Minaccia e non al Componente, definita Rischio Intrinseco della Minaccia:
  - ✓ RIM = VCMi x IMi

Applicazioni del Data Model: Un nuovo modello per l'analisi del Rischio nelle IC

- Utilizzando questa formula, ed eseguendo la sommatoria non più rispetto al Componente i ma alla Minaccia j:
  - $RM = \sum_j (VCM_j \times PM \times IM_j) = [\sum_j (VCM_j \times IM_j)] \times PM = RIM \times PM$

- Nella formula, si è considerato il fatto che essendo la sommatoria svolta nei confronti della Minaccia, il valore di PMj è **costante**, e può essere estratto dalla sommatoria
- In definitiva, si è definito un Rischio Intrinseco della Minaccia, che può consentire di valutare nell'Analisi dei Rischi anche quelle Minacce **i cui valori di Probabilità di Accadimento siano infinitesimali**, e che risulta basata sul livello di Vulnerabilità esposto dall'Infrastruttura Critica nei confronti della Minaccia

RISCHIO		VULNERABILITÀ ALLA MINACCIA		
		BASSA	MEDIA	ALTA
IMPATTO DELLA MINACCIA	ELEVATO	Rischio medio	Rischio alto	Rischio alto
	MEDIO	Rischio basso	Rischio medio	Rischio alto
	TRASCURABILE	Rischio basso	Rischio basso	Rischio medio

Grazie per la vostra attenzione!

Partecipanti al Gruppo di Lavoro PSO Data Model:

Bruno Carbone

Stefania Caporalini-Ajello

Roberto Ciampoli

Lucilla Mancini

Marcello Pistilli

Orsio Romagnoli

Lucio Tirone

ASTER S.p.A.

Rome Headquarters & Operational Office
Via Tiburtina 1166, 00156 Rome, Italy
Phone: +39 06 94533950/1
Fax: + 39 06 94533959

Naples Operational Office
Via A. Depretis 88, 80133 Naples, Italy
C.F. / P.IVA 11002491006

Email: info@aster-te.it

Partner of Assystem Group

ASTER
TECHNOLOGY & ENGINEERING