INFORMATION SECURITY

14

La Rivista dell'ICT per la Sicurezza

Organo ufficiale di Associazione Italiana esperti in Infrastrutture Critiche

PRIMO PIANO
L'importanza della prevenzione nella lotta alle frodi

PRIMO PIANO
Volando nella Nebbia delle Nuvole (ovvero Cloud e Sicurezza)

AZIENDA DEL MESE
La progettazione dei Sistemi Complessi mediante Model Based System Engineering

SOTTO LA LENTE
Stonesoft, la minaccia AET e il cavallo di Troia

Edizioni a.r.l. ROC n°17883 ISSN 2037 - 5611
Pubbl. mensile registrata presso il Tribunale di Roma il 7/12/2010 n°372 Poste Italiane S.p.A.
Spedizione in abbonamento postale - 70% Roma Aut. n. C/RM/109/2013

La progettazione dei Sistemi Complessi mediante Model Based System Engineering

L'applicazione dell'MBSE è in grado di fornire sostanziali benefici rispetto al comune approccio documentale, incrementando la produttività e la qualità, riducendo i rischi e migliorando lo scambio di informazioni all'interno dei vari team di sviluppo.

Lucio Tirone
Responsabile Engineering ASTER Spa

L'INCOSE (*International Council on Systems Engineering*) definisce il Systems Engineering come "*… an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs."* (INCOSE)

Lo standard ISO/IEC 15288 identifica quattro gruppi di processi a supporto del Systems Engineering: *Enterprise Processes*, che riguardano i processi che l'impresa deve attivare a supporto dello sviluppo di qualunque sistema; gli *Agreement Processes*, relativi ai rapporti con clienti e fornitori che l'impresa deve regolare per lo sviluppo del sistema; i *Project Processes*, che includono i processi di pianificazione, gestione e controllo dello stato dello sviluppo del sistema rispetto alle esigenze operative; ed infine i *Technical Processes*, che includono tutti i processi tipici dello sviluppo tecnico e tecnologico del sistema, dall'analisi dei requisiti operativi alla progettazione, allo sviluppo, verifica e validazione del sistema, e fino alle fasi di operazione, manutenzione e dismissione del sistema stesso.

L'implementazione di tali processi attraverso un approccio formale e standar-

dizzato di modellazione applicabile fin dal livello di progettazione concettuale del sistema è la base della metodologia MBSE (*Model Based Systems Engineering*), che consiste nell'applicazione formale della modellazione per supportare le attività di progettazione, di gestione dei requisiti, di analisi e di verifica e validazione dei sistemi, a partire dalla fase di concezione, attraverso lo sviluppo e le altre fasi del ciclo di vita.
L'applicazione dell'MBSE è in grado di fornire sostanziali benefici rispetto al comune approccio documentale (document-centric), incrementando la produttività e la qualità, riducendo i rischi e migliorando lo scambio di informazioni all'interno dei vari teams di sviluppo. In particolare, si ritiene che l'MBSE rimpiazzerà l'approccio documentale che è stato adottato dagli ingegneri sistemisti nel passato e che influenzerà le future pratiche di ingegnerizzazione dei sistemi complessi attraverso una piena integrazione nella definizione dei processi di Systems Engineering (INCOSE SE Vision 2020).
Gli approcci metodologici basati sulla modellazione sono stati storicamente adottati con successo per lo sviluppo delle *componenti safety-critical* dei sistemi aeronautici, spaziali, di difesa, di controllo industriale, ecc. ed in particolar modo le parti meccaniche critiche, gli apparati elettronici ed il software di processo.
Con l'MBSE, si rilancia tale tendenza estendendola al dominio della progettazione del sistema complesso nel suo insieme, riconoscendo attraverso un approccio basato sul *pensiero sistemico* (systems thinking), o equivalentemente sull'*approccio olistico* alla progettazione, il primato del *tutto* (cioè del sistema) rispetto alle parti che lo compongono. Nell'analisi del comportamento di un sistema complesso, si studia il *tutto* con lo scopo di acquisire maggiore comprensione sulle sue *parti*, e non viceversa, in quanto il comportamento del tutto *emerge* dalle interazioni tra le parti, e non può essere dedotto dall'analisi delle parti prese singolarmente.
Se da un lato tale esigenza è ormai consolidata in settori tecnologici quali l'elettronica per la Difesa, le Centrali Nucleari, i Sistemi Aeronautici e Spaziali, in relazione all'elevata complessità e dimensioni dei sistemi coinvolti, al quadro di cooperazione multinazionale spesso presente, all'interazione ed integrazione di diversi domini multidisciplinari, alla presenza di tecnologie e soluzioni rapidamente varianti nel tempo ed al generale elevato "costo del fallimento", dall'altro è ormai sempre più evidente come, con l'emergere delle tematiche dell'Homeland Security e della Protezione delle Infrastrutture Critiche, non si possa prescindere dall'applicazione pervasiva di tali processi evoluti di progettazione anche in settori tradizionalmente considerati "civili" e non strettamente *safety-critical,* quali per esempio quello dei sistemi di acquisizione, controllo e monitoraggio per le reti ed infrastrutture energetiche, idriche, di trasporto e di monitoraggio del territorio e dell'ambiente.
D'altra parte con il progresso tecnologico che ha portato ad una sempre maggiore pervasività delle tecnologie ICT e ad una sempre maggiore interoperabilità ed interdipendenza delle reti ed infrastrutture critiche e dei sistemi che tali reti governano, l'applicazione di metodologie formali di systems engineering a tutti i livelli della filiera, dai gestori alle autorità di controllo, ai produttori, agli enti certificatori ed alla comunità accademica e scientifica, costituisce un presupposto fondamentale per garantire il controllo (e in prospettiva la certificazione) dei livelli di vulnerabilità e resilienza delle reti e dei sistemi lungo tutto il loro ciclo di vita.

La Metodologia MBSE ed il linguaggio SysML

La metodologia MBSE riconduce la progettazione di un sistema complesso a 5 fasi principali che ne coprono tutti gli aspetti essenziali:
1. L'analisi di contesto
2. L'analisi del Concetto Operativo (ConOps)
3. La definizione delle architetture HW/SW
4. L'analisi del comportamento del sistema
5. La gestione delle interfacce

Tali fasi convergono nella definizione e caratterizzazione di un modello formale del sistema che ne rappresenta in maniera univoca ed esaustiva i comportamenti del sistema come definiti dai requisiti operativi o dai framework architetturali che lo specificano.
Il modello formale è generalmente descritto mediante il linguaggio SysML, concepito e sponsorizzato da INCOSE e OMG, con una larga partecipazione dell'industria, che è stato adottato a partire dal 2006 come un linguaggio di modellazione *general purpose*, per supportare l'MBSE applicata alla progettazione di sistemi complessi, che includano hardware, software, dati, operatori, procedure ed infrastrutture. Il SysML (attualmente è in uso la versione 1.2, rilasciata nel 2010) definisce una serie standardizzata di dia-

L'AIIC AL SERVIZIO DELLA CONTINUITÀ OPERATIVA DEL PAESE

L'AIIC Associazione Italiana Esperti in Infrastrutture Critiche promuove la cultura interdisciplinare per lo sviluppo di strategie, metodologie, tecnologie e formazione capaci di gestire la sicurezza delle infrastrutture critiche assicurandone la continuità operativa. Promuove la conoscenza e la condivisione delle esperienze maturate e favorisce un approccio interdisciplinare, intersettoriale e svolge un'attività divulgativa con eventi tecnico-scientifici, studi e ricerche tematiche.
http://www.infrastrutturecritiche.it/.

grammi che consentono analisi e sintesi statiche (diagrammi di architettura) e dinamiche (diagrammi di comportamento) di sistemi complessi.
Nella fase di analisi di contesto, si definiscono formalmente e gestiscono in modo sistematico e controllato:

- gli Stakeholders del sistema, ed i loro needs (user requirements)
- il boundary del sistema
- le interfacce esterne

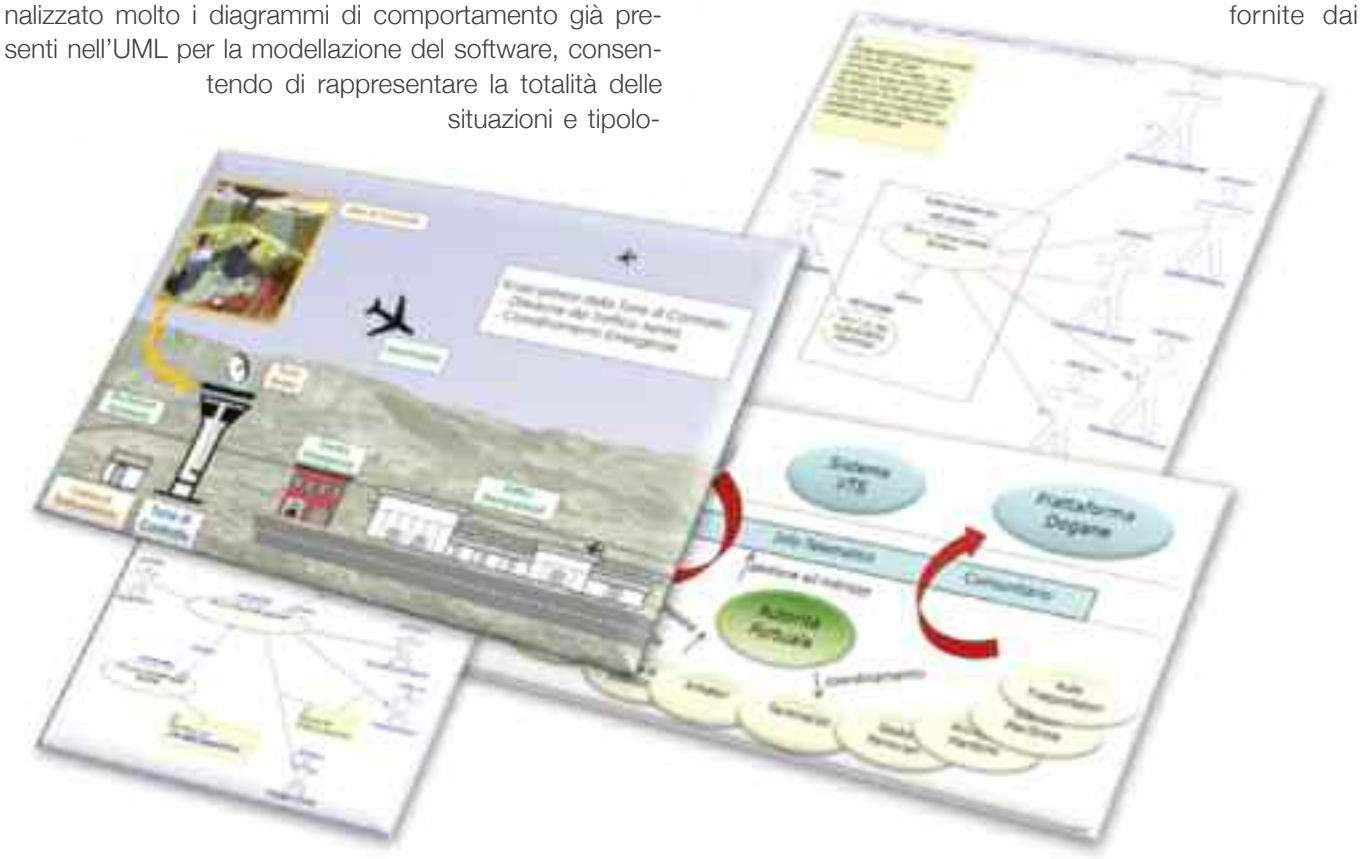
Successivamente nella fase di Analisi del Concetto Operativo, si introduce nel modello l'analisi delle capabilities offerte dal sistema, fornendo delle viste di alto livello che definiscono il suo ruolo (operational views) o comportamento (use case views) nell'ambito dello scenario operativo previsto.
Nella successiva fase di definizione delle architetture HW/SW, qualunque tipo di sistema (hardware, software, misto) e qualunque componente del sistema (sottosistemi, algoritmi, personale operativo, procedure…) può essere rappresentato nel modello mediante dei Block Definition Diagrams, fornendo in tal modo una base formale alla progettazione di architetture complesse
Analogamente, nella fase di analisi dei comportamenti del sistema, vengono definite e rappresentate nel modello tutte le interazioni tra le diverse componenti definite, siano esse statiche, a stati o dinamiche. Il linguaggio SysML ha razionalizzato molto i diagrammi di comportamento già presenti nell'UML per la modellazione del software, consentendo di rappresentare la totalità delle situazioni e tipologie di interazioni mediante:

- Sequence diagrams: comportamenti del sistema rappresentati da scambio di informazioni e dati tra elementi, sincronizzato in modo predefinito nel tempo
- Activity diagrams: comportamenti del sistema rappresentati da sequenze funzionale di azioni da svolgere
- State diagrams: comportamenti del sistema rappresentati come evoluzioni dello stato del sistema o di un suo componente al verificarsi di determinati eventi o stimoli

Infine, nella fase di gestione delle interfacce, vengono analizzati e rappresentati nel modello tutti i tipi di interazione tra entità diverse, attraverso strumenti chiamate convenzionalmente "porte":

- Flow Ports, per rappresentare scambi continui di dati o entità fisiche (ad esempio valori di temperatura acquisiti da un sensore, o il carburante in ingresso ad un motore, o la tensione di alimentazione di un apparato)
- Standard Ports, per rappresentare scambi di servizi e messaggi (ad esempio l'invocazione di funzioni e metodi da componenti software, l'invio e la ricezione di messaggi strutturati, o la segnalazione di allarmi)

Il modello formale del sistema definito in tal modo consente di implementare un controllo rigoroso sulla tracciabilità e l'evoluzione dei requisiti (di utente, sistema o sottosistema), nel corso dell'intero ciclo di vita del sistema. Mediante le capability di export fornite dai



Esempi di analisi di ConOps e Use Case

principali tools commerciali di modellazione, è possibile generare l'intera documentazione di progetto (SRD, SSS, SSDD, IRS, ICD, …) in automatico, realizzando appositi templates basati su qualunque standard di riferimento.
Inoltre il modello del sistema è impiegato per automatizzare completamente i piani di verifica e validazione del sistema fino alla sua certificazione e collaudo.

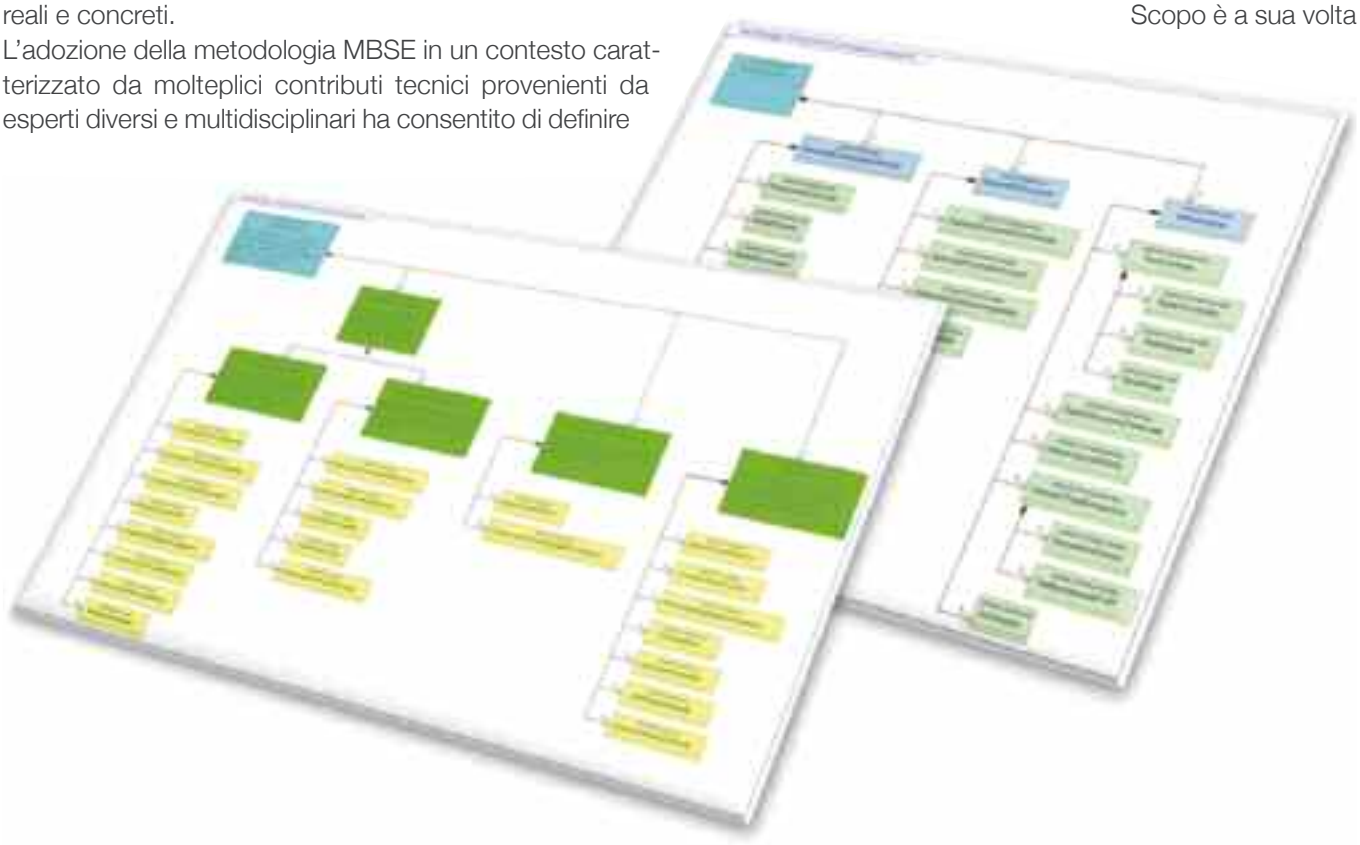
L'applicazione del MBSE al settore della Protezione delle Infrastrutture Critiche: il Gruppo di Lavoro Data Model di AIIC

L'applicazione del MBSE al settore della protezione delle infrastrutture critiche è stata recentemente discussa in ambito AIIC, dal gruppo di lavoro GdL Data Model che l'ha adottata 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*" in ambito Europeo.
In particolare, sulla base dei modelli e "viste" già prodotte dal GdL PSO di AIIC, "*Infrastrutture Critiche Europee - Piano di Sicurezza dell'Operatore: Proposta di linee guida operative*", il GdL intende effettuare una razionalizzazione e raffinamento delle entità e delle relazioni già ipotizzate (perimetro di intervento, componenti, minacce, contromisure) nell'ambito delle relative viste, secondo l'approccio MBSE, fino ad un livello di progettazione adeguato ad assicurare la identificazione degli elementi del Data Model in contesti reali e concreti.
L'adozione della metodologia MBSE in un contesto caratterizzato da molteplici contributi tecnici provenienti da esperti diversi e multidisciplinari ha consentito di definire formalmente:

- il Glossario dei Termini
- il Piano di Lavoro
- l'Architettura e le componenti fisiche e logiche dell'Infrastruttura Critica di riferimento
- il Data Model vero e proprio

Il primo compito è stato quello di stabilire un Glossario comune dei Termini, orientato a definire il significato dei termini più ricorrenti e di rilievo, allo scopo di evitare ambiguità ed incomprensioni. Questo è forse il più sottostimato dei compiti del Systems Engineer, ma la sua importanza è cruciale nello stabilire una base di conoscenza condivisa. Le domande comuni sono: "come si definisce un sistema?"; oppure "a cosa si applica una minaccia?", o ancora "qual è la differenza tra minaccia ed attacco?". A queste domande occorre rispondere in modo univoco e condiviso. Alcuni esempi rilevanti dell'attività di definizione del Glossario dei Termini sono:

- L'Infrastruttura Critica è assimilata nell'ambito dell'analisi ad un Complesso, definito come un 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.
- Il Complesso per realizzare il suo Obiettivo si articola in una serie di uno o più Sistemi e Scopi, che possono essere anche organizzati in più livelli. Ogni Scopo è a sua volta



Esempi di progettazione dell'architettura fisica e funzionale

ASTER

ASTER è una società d'ingegneria indipendente, specializzata nei settori dei Sistemi Complessi e delle Infrastrutture ad alto contenuto tecnologico, nei quali opera a supporto di Clienti Industriali ed Istituzionali per lo sviluppo di grandi progetti tecnologici nelle principali aree di business della Elettronica per la Difesa, Sicurezza e Trasporti, Energia ed Utilities.

Originariamente operante come Business Unit del Gruppo Multinazionale Francese ASSYSTEM, ASTER è oggi qualificata come fornitore di servizi di ingegneria integrata per l'Industria e come consulente indipendente per Enti Pubblici ed Istituzioni, sia a livello nazionale che internazionale, per la progettazione, la supervisione, i servizi di collaudo e prove, nell'ambito di programmi per la realizzazione di impianti ed infrastrutture tecnologiche safety-critical (aeroporti, porti, impianti industriali, …), sulla base delle competenze specialistiche chiave in sistemi di supporto decisionale e situation awareness, sistemi di monitoraggio e sorveglianza integrata e sistemi C4I. Inoltre, nelle nostre aree di business, promuoviamo costantemente progetti di ricerca ed innovazione auto-finanziati e co-finanziati per lo sviluppo del portafoglio di prodotti tecnologici aziendali.

Aster collabora da anni con le principali industrie nazionali attive nei settori della difesa e della sicurezza (SELEX Sistemi Integrati, MBDA Italia, Telespazio) nonché con Enti pubblici e di ricerca (Ministero Difesa, Assoporti, CNR) e gestori di reti ed infrastrutture (ARIN, INGV) per conto delle quali ha svolto numerose attività di progettazione e supporto specialistico negli ambiti del Systems Engineering.

Aster è inoltre membro dell'AFCEA (Armed Forces Communications & Electronics Association) ed è la prima Società d'Ingegneria Italiana ad aver aderito al programma dell'INCOSE (International Council on Systems Engineering) di certificazione professionale sul Systems Engineering (SEP-Systems Engineering Professional).

Nell'ambito del Systems Engineering, ASTER è Business Partner certificato di IBM, per la fornitura di ambienti e soluzioni integrate per la gestione del ciclo di vita dei sistemi complessi. Inoltre, in collaborazione con la società spagnola VISURE, ASTER fornisce soluzioni integrate di requirement engineering, basate sulle più recenti tecnologie di gestione avanzata dei requisiti. Infine abbiamo recentemente siglato un accordo di partnership con la società francese Eiris Conseil per la fornitura di corsi di training specializzato in Systems Engineering, MBSE e SysML alle Industrie e alla Pubblica Amministrazione.

Dal 2011 Aster è entrata a far parte dell'AIIC con l'obiettivo di contribuire attivamente alle attività dell'Associazione nel settore dell'analisi delle vulnerabilità e del rischio, mettendo a disposizione esperti con competenze specialistiche nelle metodologie di analisi e progettazione di sistemi complessi, nonché nella progettazione e supervisione della messa in sicurezza di infrastrutture critiche.

Ulteriori informazioni e contatti sono disponibili sul sito www.aster-te.it.

scomposto in una serie di una o più Funzioni, mentre ogni Sistema è scomposto in una serie di Componenti.

- Un Sistema è un insieme di Componenti accomunati con le loro Funzioni per l'attuazione di uno Scopo definito.
- Un Componente è l'elemento al più basso livello di astrazione in cui viene articolato il Complesso. Su di esso vengono installate le Contromisure.
- Una Contromisura è un elemento organizzativo, logico o fisico capace di ridurre la Vulnerabilità del Componente a cui è applicata nei confronti di una Minaccia.
- Una Minaccia rappresenta la possibile realizzazione di un Evento Dannoso..
- Un Evento Dannoso è un Evento Rilevante i cui effetti comportano un potenziale Danno appartenente ad una delle categorie di Danno definite (Patrimonio, Ambiente, Salute, Continuità del servizio).
- Un Evento Rilevante è un evento che genera come Effetto una alterazione di una o più Funzioni dell'Infrastruttura Critica.
- Un Danno si può realizzare in quattro modi distinti: Danno alla Salute, Danno Ambientale, Danno Patrimoniale, Interruzione di Servizio.
- Il Perimetro di Intervento è una perimetrazione logica ai fini dell'analisi del rischio e della progettazione delle contromisure. Si può definire un Perimetro di Intervento per specificare le Contromisure necessarie a mettere in sicurezza un determinato Sistema dell'Infrastruttura Critica, oppure un suo Scopo, o un insieme misto di Sistemi e Scopi.

Il secondo passo è consistito nella definizione della logica complessiva dell'attività di messa in sicurezza dell'Infrastruttura Critica. Ciò al fine di elaborare il contesto appropriato di ciascuna fase dell'attività, e di evitare sovrapposizioni ed incongruenze. L'analisi dell'architettura fisica dell'Infrastruttura Critica e delle funzioni dei suoi componenti è un'attività ben distinta dall'analisi delle minacce che incombono su quelle funzioni, e lo è altrettanto dalla progettazione delle contromisure necessarie a contrastare quelle minacce.

È un errore piuttosto comune quello di trarre conclusioni al di fuori del contesto appropriato, e su tali conclusioni basare scelte che esporranno l'Infrastruttura Critica a minacce non opportunamente prese in conto. Ad esempio svolgere l'analisi funzionale avendo già un'idea consolidata delle contromisure che si andranno ad implementare porta facilmente a sottovalutare minacce di tipologie non comuni. Occorre invece svolgere ciascuna fase nell'ambito del proprio perimetro specifico, documentando in modo accurato il razionale di ogni scelta effettuata, e definendo formalmente gli output che vengono forniti alla fase seguente. Il flusso delle attività si compone delle tre fasi seguenti:

- Analisi di Sistema: consiste nell'analisi volta ad individuare le funzionalità implementate dall'Infrastruttura Critica, nel ruolo svolto dai componenti fisici nell'attuazione di quelle funzionalità, e nell'analisi delle interfacce interne ed esterne che mettono in relazione i componenti dell'Infrastruttura Critica tra di loro e con il mondo esterno
- Analisi di Rischio: consiste nell'identificazione delle minacce che insistono sulla Infrastruttura Critica, e nell'analisi delle vulnerabilità che l'Infrastruttura Critica presenta verso di esse

• Analisi di Sicurezza: consiste nella definizione dei Perimetri di Intervento, e nella progettazione delle Contromisure che è necessario adottare per contrastare le minacce individuate nella fase precedente

Le tre fasi hanno un andamento che è necessariamente ciclico, in quanto a valle dell'individuazione ed implementazione delle contromisure utili a contrastare le minacce individuate dall'Analisi di Rischio, si saranno aggiunte delle nuove funzionalità e nuovi componenti all'Infrastruttura Critica (le contromisure stesse). Queste, definite formalmente tramite una nuova Analisi di Sistema, ed analizzate in dettaglio da una nuova Analisi di Rischio, porteranno alla definizione di nuove minacce che non potevano essere considerate nel ciclo precedente. Seguirà quindi una nuova Analisi di Sicurezza per contrastare le nuove minacce, ed il ciclo si ripeterà in iterazioni successive. Le iterazioni avranno termine nel momento in cui l'Analisi di Rischio sarà in grado di valutare che l'insieme di tutte le contromisure adottate è in grado di ridurre le vulnerabilità dell'Infrastruttura Critica nei confronti di tutte le minacce considerate nelle varie iterazioni al disotto di una soglia prefissata.

Nel contesto dell'analisi appena definita, si può asserire che l'obiettivo finale del GdL Data Model, è stato quello di generare un Modello dei Dati ed una Terminologia condivisa a supporto di tutte e tre le fasi descritte. Ad esempio, il modello del dato "Contromisura", è stato dotato di una relazione con la "Minaccia" che essa tende a contrastare, di una relazione con il "Componente" sul quale essa è installata, e di un attributo che ne determina la tipologia (logica, fisica, organizzativa). Queste tre caratterizzazioni consentono di posizionare la Contromisura in maniera univoca nello spazio delle contromisure (viste, contromisure, componenti), definito nelle Linee Guida PSO.

Sul piano tecnico, per la definizione formale del Data Model, è possibile adottare varie tecniche come la scomposizione funzionale (FFBD o Functional Flow Break Down), o il SysML (Systems Modeling Language), per rappresentare le architetture sia logiche che fisiche degli elementi del modello, le loro caratteristiche, attributi ed interazioni.

Nel caso del GdL Data Model, si è scelto di rappresentare un Complesso (quindi una Infrastruttura Critica) 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)

Le tre architetture rappresentano diversi "punti di vista" dello stesso Complesso. Le prime due di fatto esistono indipendentemente l'una dall'altra: si possono avere infatti diverse architetture fisiche che implementano le stesse funzioni, e viceversa configurare in modi diversi una stessa architettura fisica per svolgere funzioni diverse. La terza invece fa una sintesi delle prime due dal punto di vista della sicurezza, individuando gli ambiti sui quali verranno progettate le contromisure.

La definizione di ciascuna delle architetture viene svolta mediante la rappresentazione delle relazioni tra gli oggetti definiti precedentemente, costituendo un *metamodello* che consente di stabilire le regole secondo le quali sarà possibile derivare i modelli specifici dei casi reali che saranno analizzati in accordo alla metodologia definita.

La costruzione del metamodello porta ad interrogarsi su tutte le possibili interazioni tra gli elementi definiti, e costituisce di fatto una razionalizzazione delle definizioni ottenute nella fase di generazione del Glossario dei termini. Su questa base, ciascuno degli elementi viene analizzato in modo grafico e semplice da comprendere, e la discussione per definire proprietà e relazioni risulta sensibilmente facilitata.

Il caso di studio descritto rappresenta solo un esempio applicativo, peraltro ancora nella sua fase iniziale di sviluppo, ed è certamente utile sottolineare che soltanto intraprendendo azioni analoghe a tutti i livelli della filiera si potrà pervenire a risultati di rilevanza generale.

Ciò nonostante, esso sta indubbiamente dimostrando come l'applicazione delle metodologie MBSE possa rappresentare un contributo importante nel settore delle infrastrutture critiche, favorendo la creazione di un quadro di riferimento comune, armonizzato e certificato per la valutazione del rischio, l'analisi dei sistemi ed il controllo delle vulnerabilità, della resilienza e delle interdipendenze delle reti e dei sistemi, sia in fase di progettazione/integrazione che in fase di esercizio.