Asset	Vengono elencati gli asset che potrebbero essere di interesse per un potenziale avversario. Questi possono essere di tipo fisico o logico. Possibili esempi di asset sono: le credenziali di accesso, i dettagli di una carta di credito, le chiavi di crittografia o i dettagli dell'utente.
Punti di Ingresso/Uscita	I punti di ingresso/uscita sono quei punti del sistema dove i dati entrano o escono. Questi vengono talvolta indicati come "punti di attacco" poiché soggetti ad uno o più potenziali attacchi. Ciascuno di questi, corrisponde ad una parte del sistema per la quale dovrebbero essere implementate opportune misure di sicurezza.
Livelli di Fiducia o di Trust	Un livello di trust viene utilizzato per definire i privilegi che un'entità esterna deve avere per accedere al sistema. Questi possono essere classificati in base ai privilegi assegnati o alle credenziali fornite e fanno riferimento a punti di ingresso/uscita di risorse protette. Possibili esempi sono l'utente anonimo del sistema, l'utente autenticato del sistema e l'amministratore. I livelli di trust vengono applicati ad ogni punto di entrata/uscita.

5.2 Secure by Design

Le applicazioni la cui architettura non viene valutata dal punto di vista della sicurezza sono applicazioni 'fragili'. L'analisi, fatta in concerto sia sull'architettura dell'applicazione che sulle interazioni, accresce la visibilità dei team IT circa gli ambiti della sicurezza e del risk management. Gli architetti delle applicazioni software sono responsabili della realizzazione del progetto per garantire l'adeguata copertura ai rischi derivanti sia da un uso standard del sistema, sia da un attacco dannoso.
Nella fase di design di una nuova applicazione o di re-ingegnerizzazione di un'applicazione esistente, per ciascuna caratteristica funzionale, è necessario analizzare aspetti aggiuntivi quali:

- Gli aspetti di sicurezza nel processo riguardante tale funzione sono stati massimizzati?
- Premeditatamente, come si potrebbe abusare di tale funzione?
- La funzione deve essere attivata per impostazione predefinita? In caso affermativo, esistono limiti o alternative che potrebbero contribuire a ridurre il rischio derivante da tale funzione?

Andrew van der Stock chiama il suddetto processo "Thinking Evil", e raccomanda di mettersi nei panni dell'attaccante e di pensare a tutte le possibili alternative per abusare di ogni singola funzione, considerando i tre pillar fondamentali (Riservatezza, Integrità, Disponibilità) e utilizzando a sua volta il modello STRIDE.
Utilizzando il modello di rischio di minaccia STRIDE/DREAD discusso nel presente documento, è possibile intraprendere la giusta strada per adottare formalmente un'architettura sicura nello sviluppo applicativo del software.
Il concetto di sicurezza nell'architettura inizia ad esistere nel momento in cui vengono modellati i requisiti di business e prosegue fino a quando l'ultima istanza dell'applicazione viene dismessa.

5.2.1 Principi base del secure design

"Security by design" è un concetto base dell'ingegneria del software e definisce un software progettato espressamente per essere sicuro (anticipando e minimizzando a priori gli impatti delle vulnerabilità che potrà manifestare in produzione) capace di garantire i seguenti caposaldi della sicurezza dell'informazione:

- **R**iservatezza: consentire l'accesso solo ai dati per i quali l'utente è autorizzato.
- **I**ntegrità: garantire che i dati non vengano manomessi o alterati da utenti non autorizzati.