27th annual INCOSE international symposium

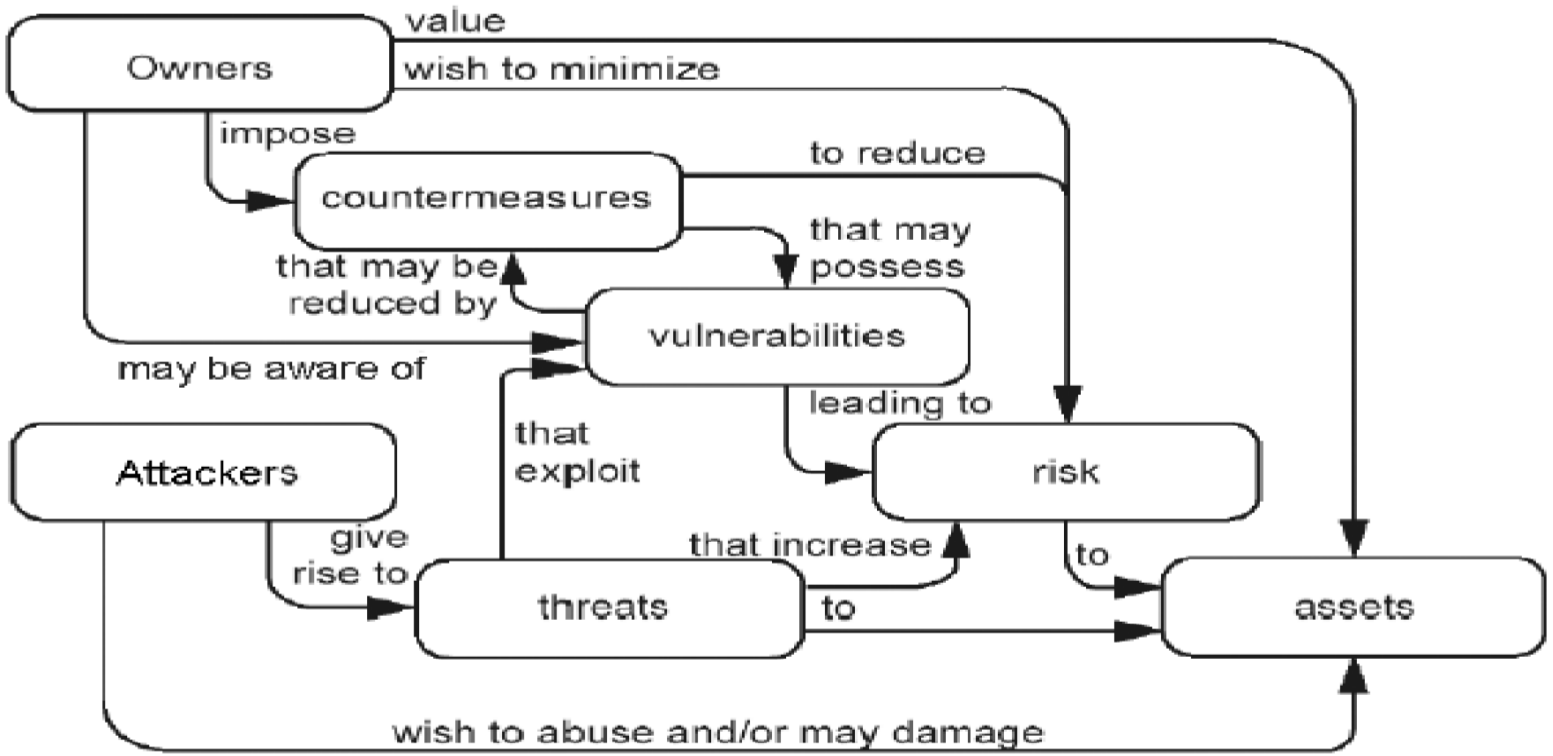
Adelaide, Australia

July 15 - 20, 2017

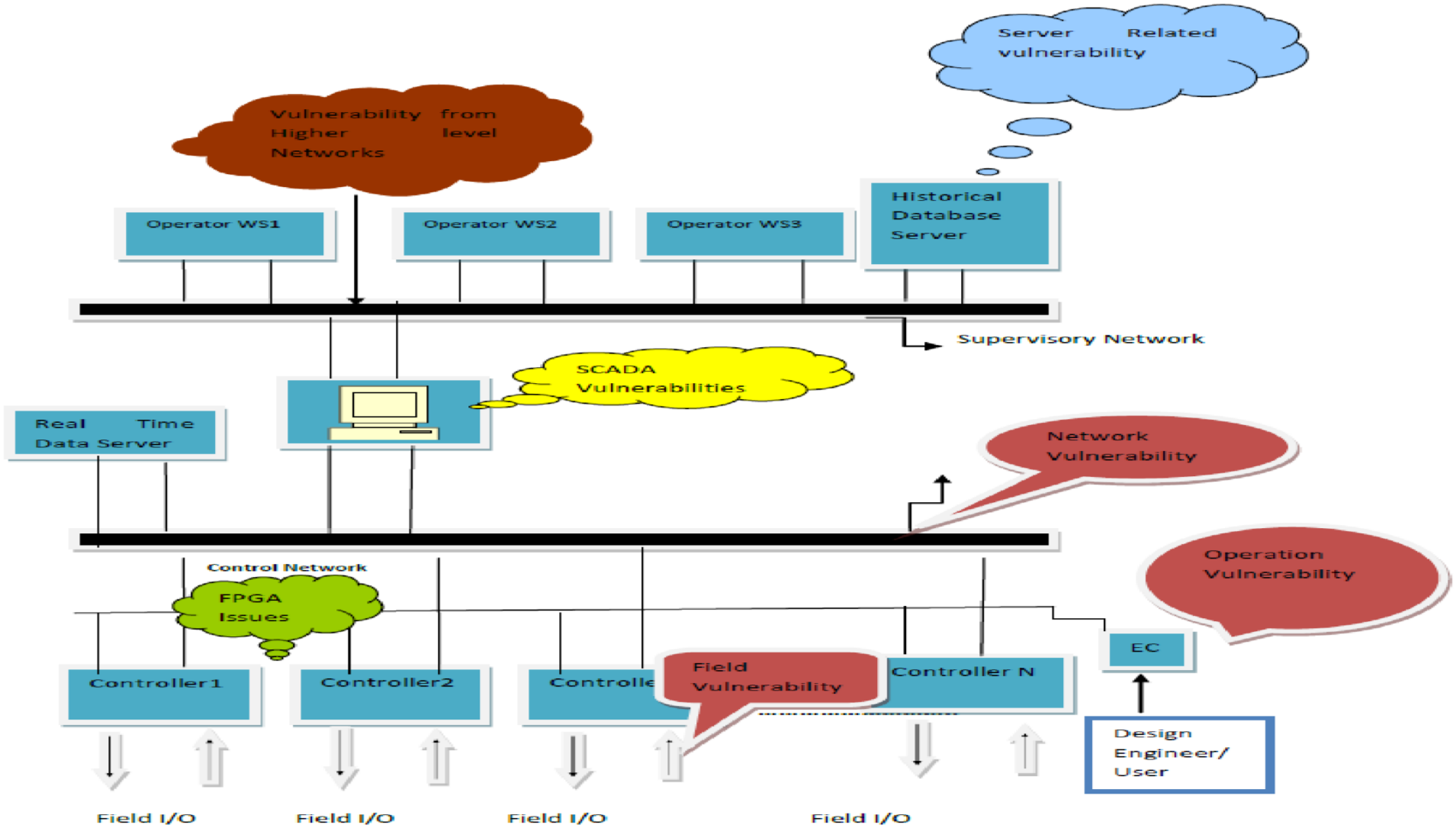
Design of Security Aware Safety Critical Embedded System

By Raka Mitra

Security Concepts and Relationships (adapted from IAEA Nuclear Security Series No.17)



Typical I&C architecture and Possible Vulnerabilities (adapted from System Requirement



Risk Assessment Matrix

Likelihood of Occurence	Severity				
		Catastrophic (4)	Critical (3)	Marginal (2)	Negligible (1)
	Frequent (4)	16 (H)	12 (H)	8 (H)	4 (M)
	Probable (3)	12 (H)	9 (H)	6 (M)	3 (M)
	Occasional (2)	8 (H)	6 (M)	4 (M)	2 (L)
	Remote (1)	4 (M)	3 (L)	2 (L)	1 (L)

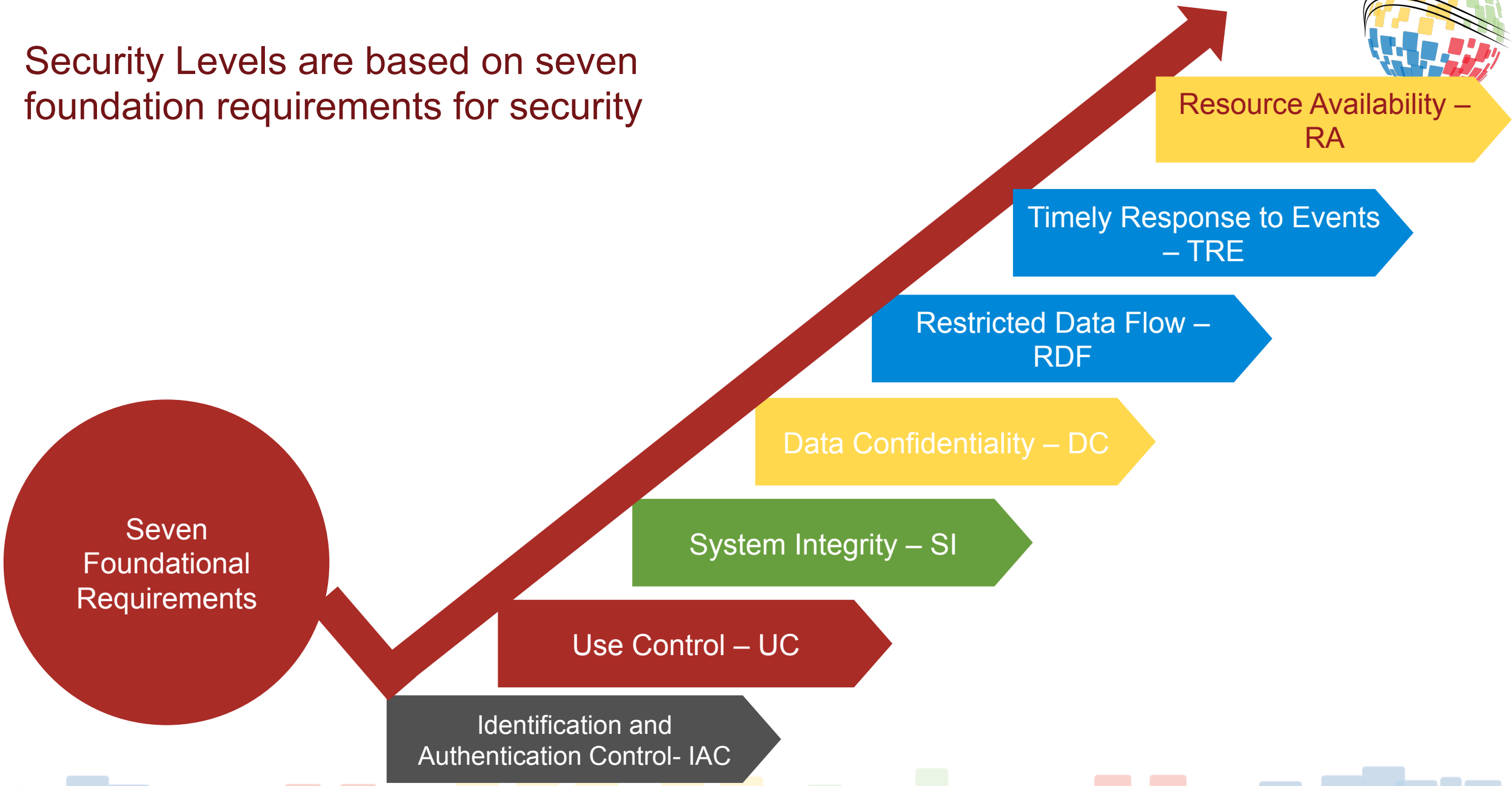
Security Levels

Target Security Levels: These are the desired level of security for a particular system. This is determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation.

Achieved Security Levels: These are the actual level of security for a particular system. These are measured after a system design is available or when a system is in place. They are used to establish that a security system is meeting the goals that were originally set out in the target Security Levels.

Capability Security Levels: These are the security levels that a component or systems can provide when properly configured.

Security Levels are based on seven foundation requirements for security

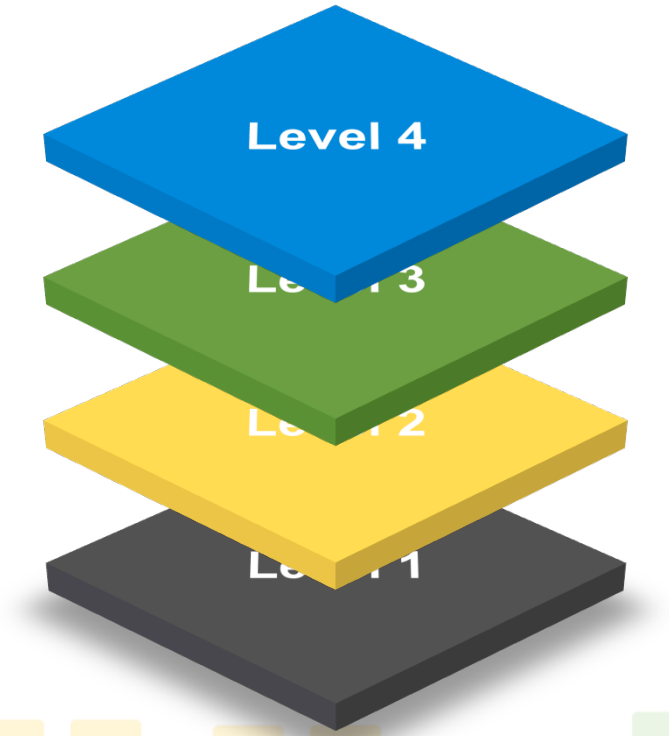


Security Levels

Level Definitions

Security Level 3: Protection against intentional violation using sophisticated means with moderate resources, system skills and moderate motivation

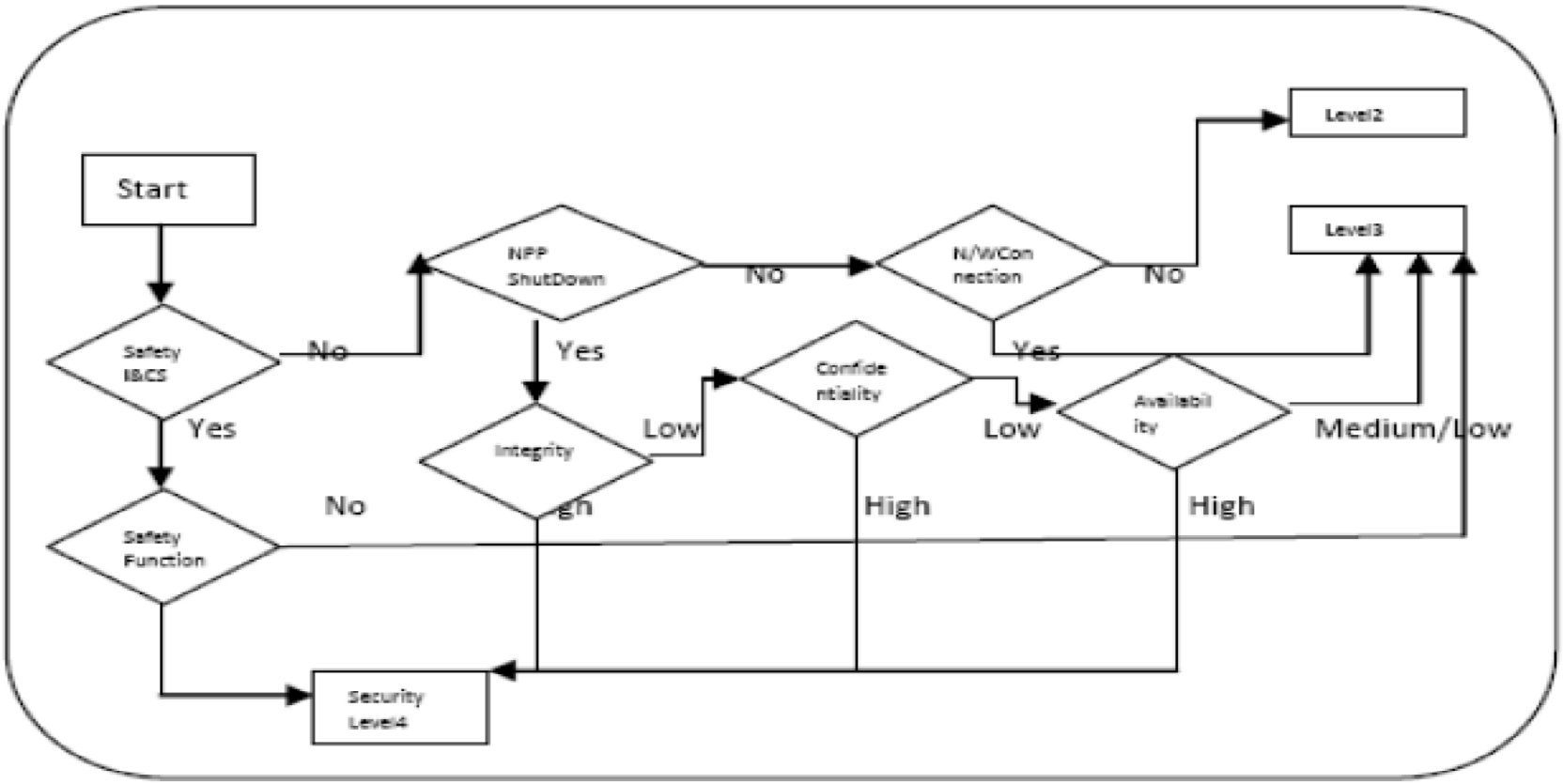
Security Level 1: Protection against casual or coincidental violation



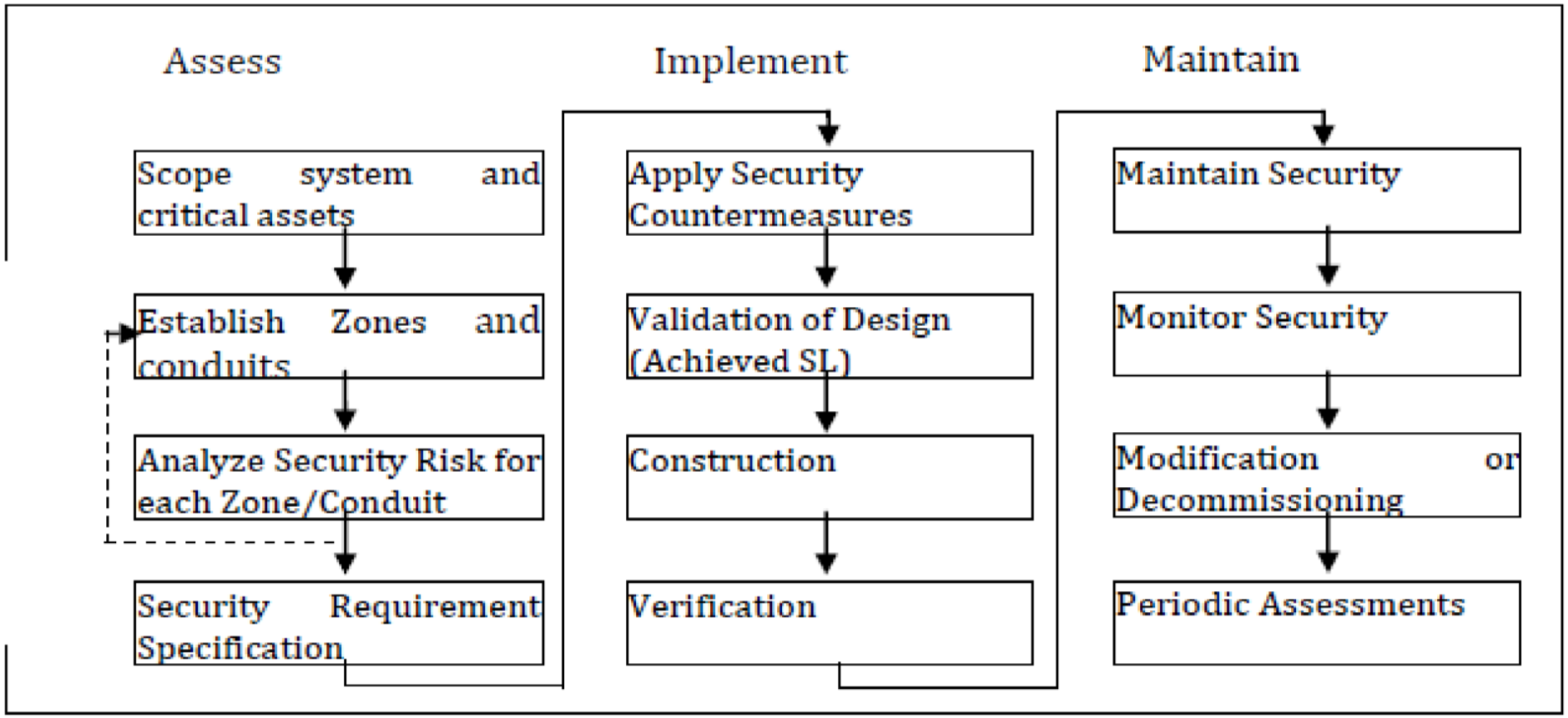
Security Level 4: Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation

Security Level 2: Protection against intentional violation using simple means with low resources, generic skills and low motivation

Procedure for assigning Achieved Security Level (adapted from Security Level Assignment in Korean Nuclear Power Plant)



Schematic of Secure Software Development Life Cycle



Assigning Security Levels – An Example

I&CS Device Asset/Zones	Threat	Consequence Rating	Likelihood Rating	Security Level
	Identification and Authentication Control			
Basic Process Control System	• Another device spoofs the identity of the Process control embedded system	H	M	SL-4
	• Attacker spoofs the identity of clients to the PCS	H	M	

Achieved Security Levels as per SRs and REs

SRs and REs	SL1	SL2	SL3	SL4	Requirement/Rationale
FR 1 – Identification and authentication control (IAC)					Protect the Control System by verifying the identity of any user
SR 1.1 – human user identification and authentication	√	√	√	√	Authentication based on segregation of duties and privilege level.
RE (1) Unique identification and authentication			√	√	The control system shall provide the capability to uniquely identify and authenticate all human users. Provided through passwords, tokens, biometrics, geographic location.

Procedure for Secure Software Design

Procedure for the Secure Software Design and Development of Safety Critical Embedded Systems.

Threat Modeling – Seeks to describe and develop pertinent threats

Secure Design & Architecture – Integrates solutions to all possible potential threats into design

Secure Implementation – Secure Coding Practices- Augment awareness about software security in software development

Software Security Testing –Performs sanity checking before release of code

CM, Operation and Maintenance of a Secure Software

Thank You!