Systems Engineering Fundamentals Risk Management

by *Gerrit Muller*   University of South-Eastern Norway-NISE

e-mail: `gaudisite@gmail.com`

`www.gaudisite.nl`

Abstract

Systems Engineering offers many methods and techniques to detect and mitigate risks. This presentaion touches upon methods like Failure Mode Effect Analysis, Hazard Analysis, etc. addressing related concerns such as reliability, safety, and security.

September 1, 2020
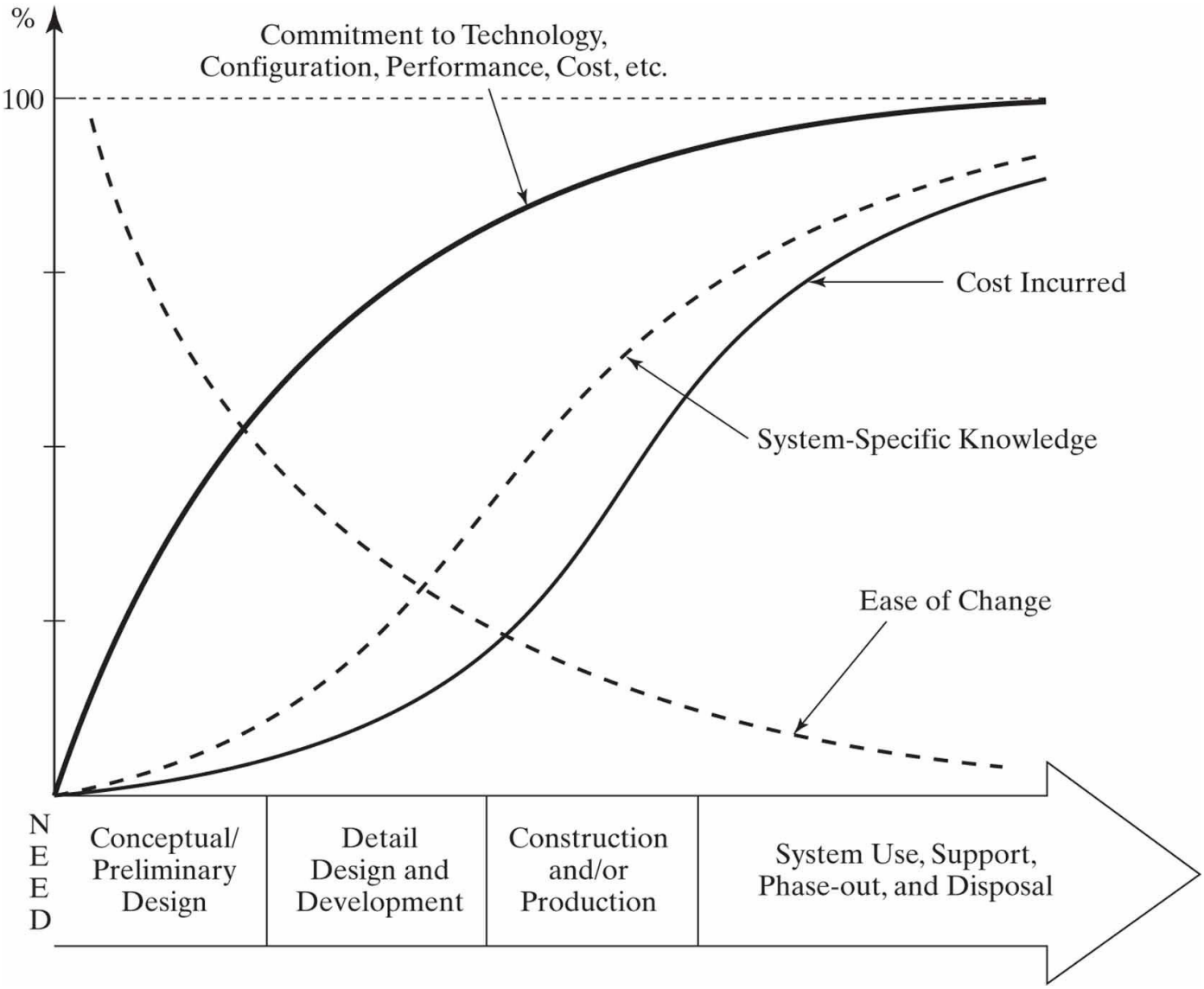status: planned
version: 0

logo
TBD

Life-cycle Commitment, Knowledge, and Incurred Cost

%

100

Commitment to Technology,
Configuration, Performance, Cost, etc.

Cost Incurred

System-Specific Knowledge

Ease of Change

N
E
E
D

Conceptual/
Preliminary
Design

Detail
Design and
Development

Construction
and/or
Production

System Use, Support,
Phase-out, and Disposal

Copyright © 2011 Pearson Education, Inc. publishing as Prentice Hall

FMEA-like Analysis Techniques


```
(systematic)  →  analysis and    →  improve
brainstorm       assessment          spec, design,
                 probability         process,
                 severity            procedure, ...
                 propagation
```
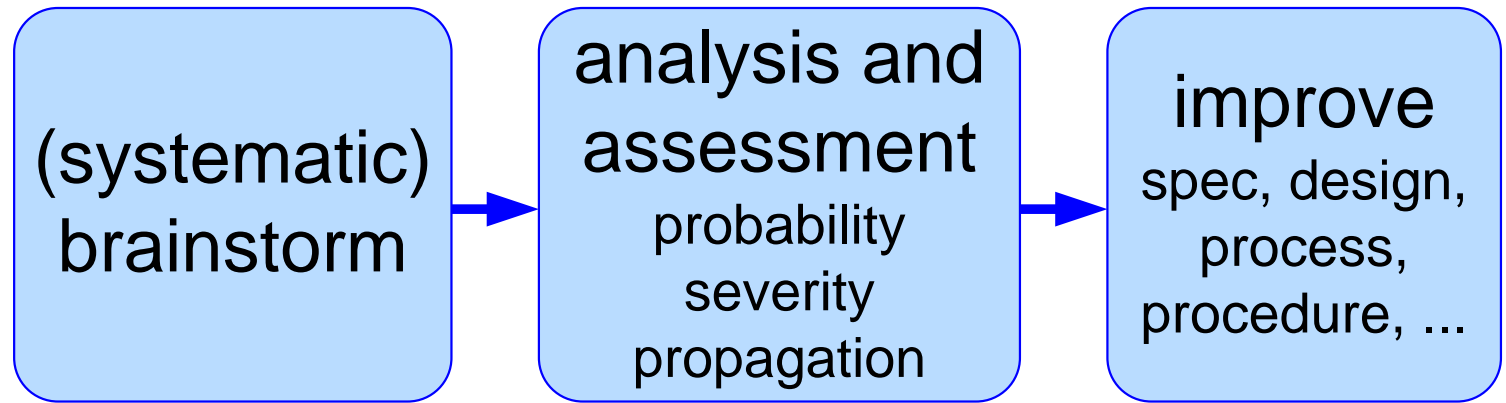
	(systematic) brainstorm	analysis and assessment	improve
safety hazard analysis	potential hazards	damage	measures
reliability FMEA	failure modes exceptional cases	effects	measures
security	vulnerability risks	consequences	measures
maintainability	change cases	impact, effort, time	decisions
performance	worst cases	system behavior	decisions

USN   ESI

Severity-Probability Classification Matrix

	I	II	III	IV	V	VI
E	moderate	moderate	high	unacceptable	unacceptable	unacceptable
D	low	moderate	moderate	high	unacceptable	unacceptable
C	low	low	moderate	moderate	high	unacceptable
B	low	low	low	moderate	high	unacceptable
A	low	low	low	low	moderate	high

probability →

severity →

based on https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis

USN   ESI