Systems-of-Systems Assurance

Taz Daughtrey

Cyber Security and Information Systems
Information Analysis Center

10 June 2014 webinar
System of Systems Engineering Collaborators
Information Exchange

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

CSIAC
Cyber Security & Information Systems
Information Analysis Center

Let’s consider ….

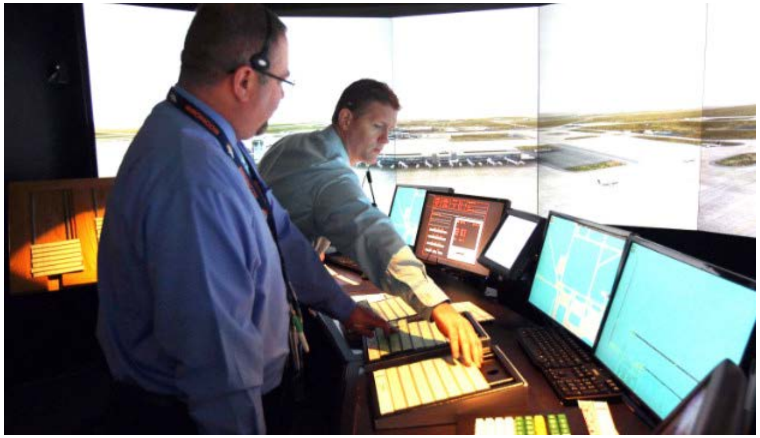
What systems? What assurance?

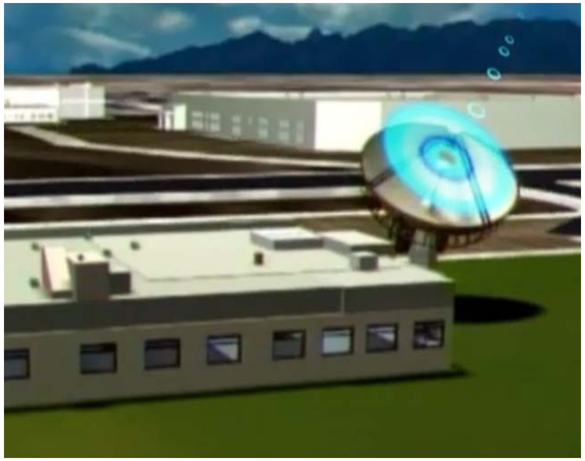
Challenges

Responses

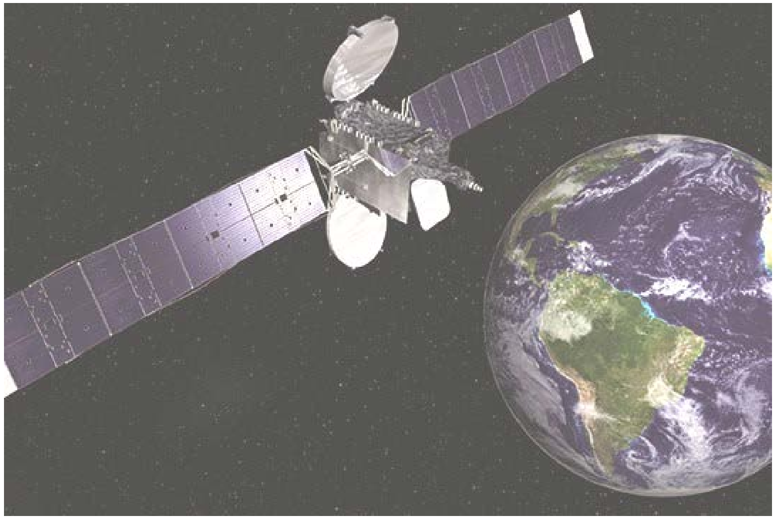
The Way Forward

Air Traffic Control System





Satellite Communication System



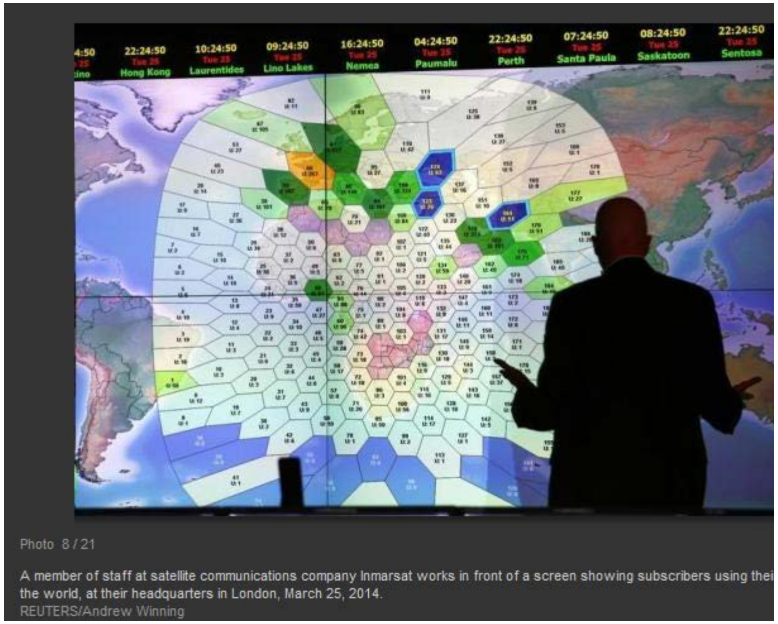
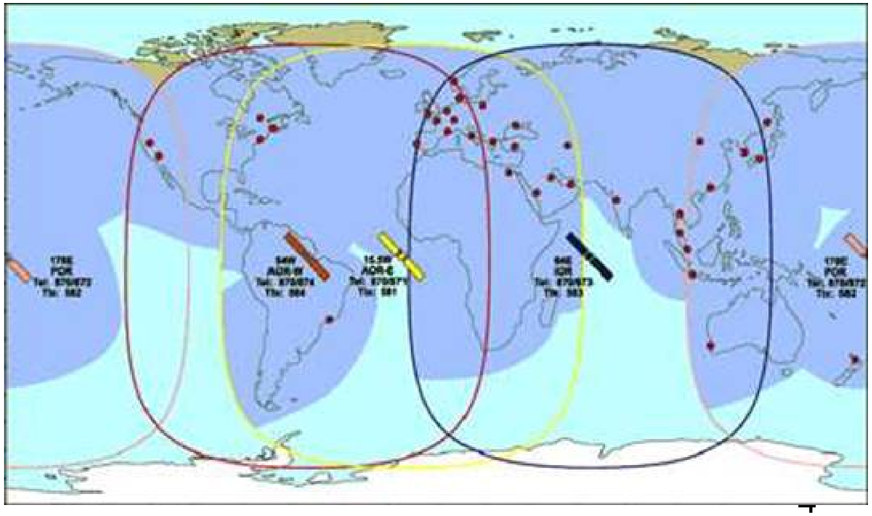
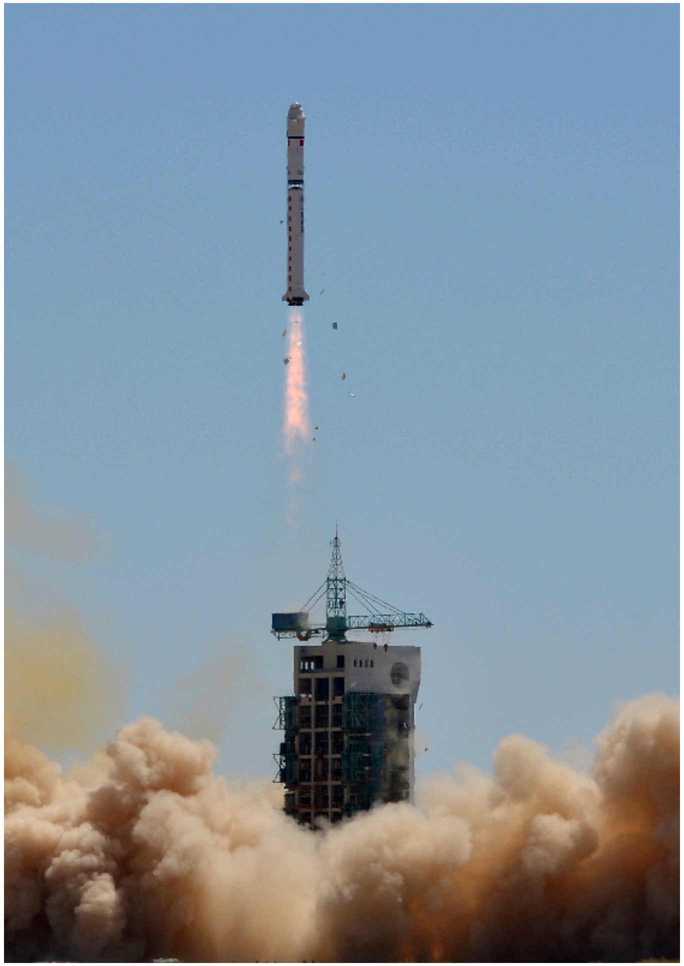


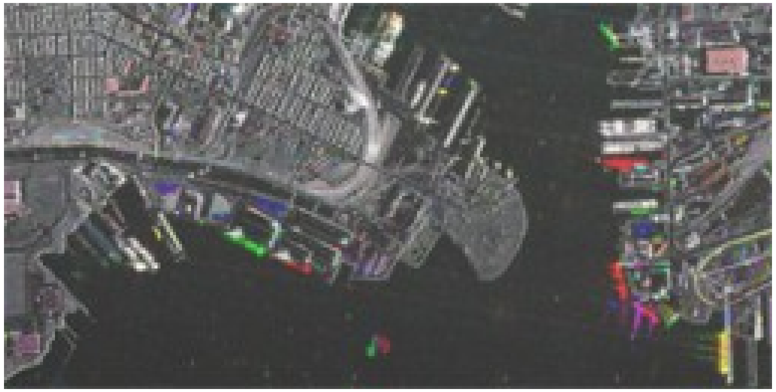
Photo 8 / 21

A member of staff at satellite communications company Inmarsat works in front of a screen showing subscribers using thei
the world, at their headquarters in London, March 25, 2014.
REUTERS/Andrew Winning



Satellite Imaging System



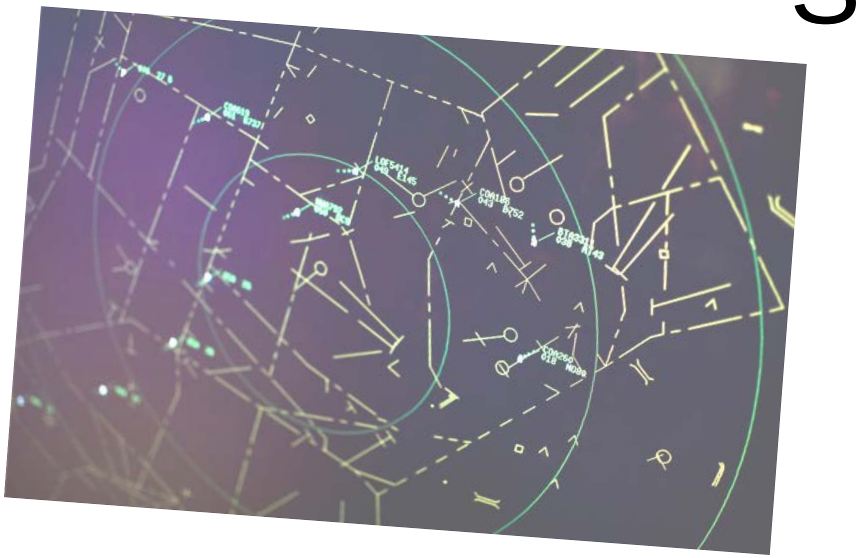


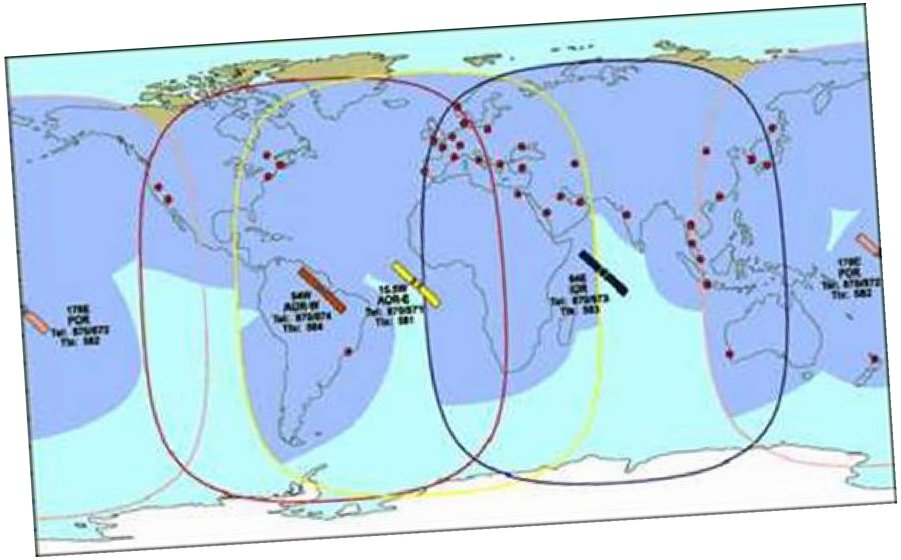
Military Transportation System

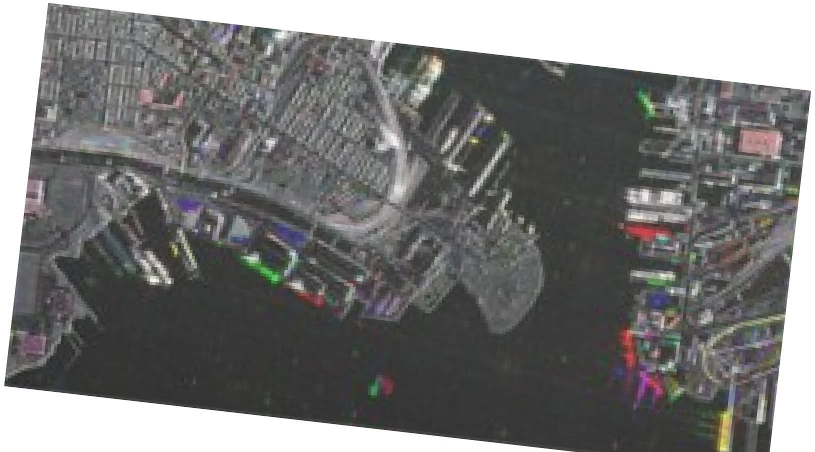
Need to “stitch” these systems together

➔ ad-hoc *system of systems*

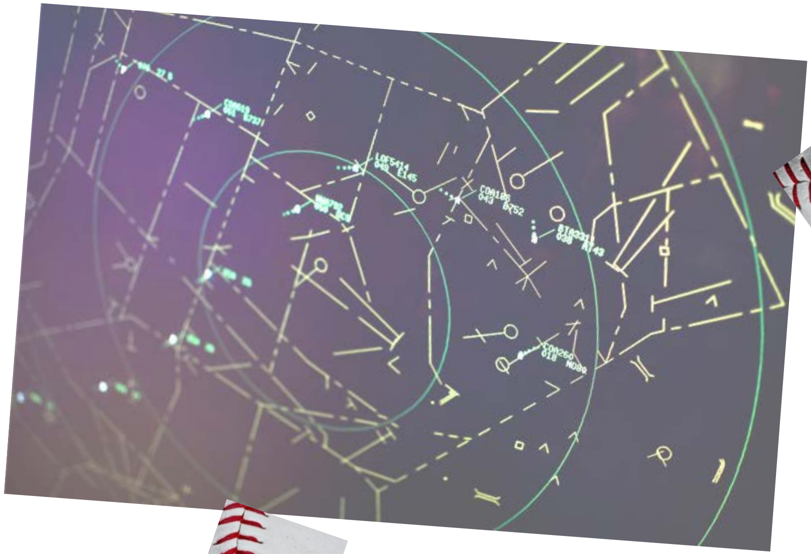
Search-and-Recovery System

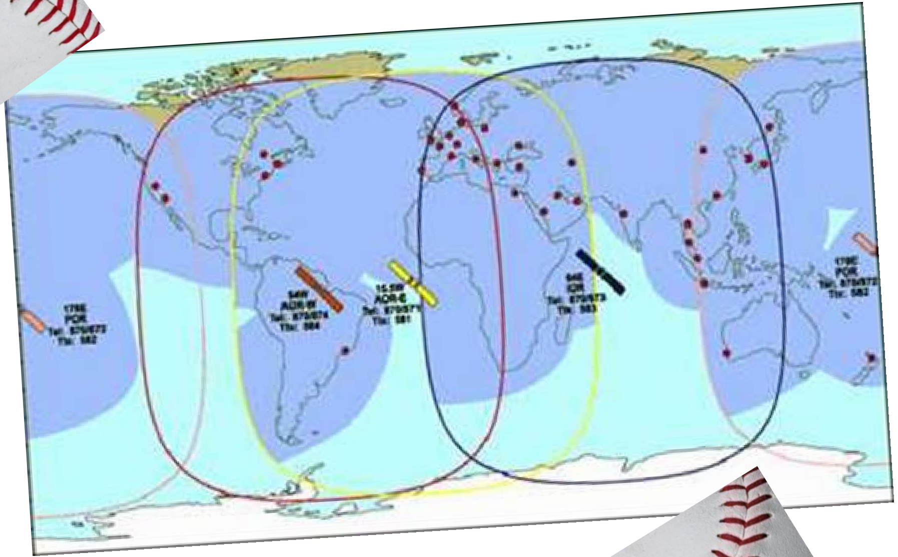


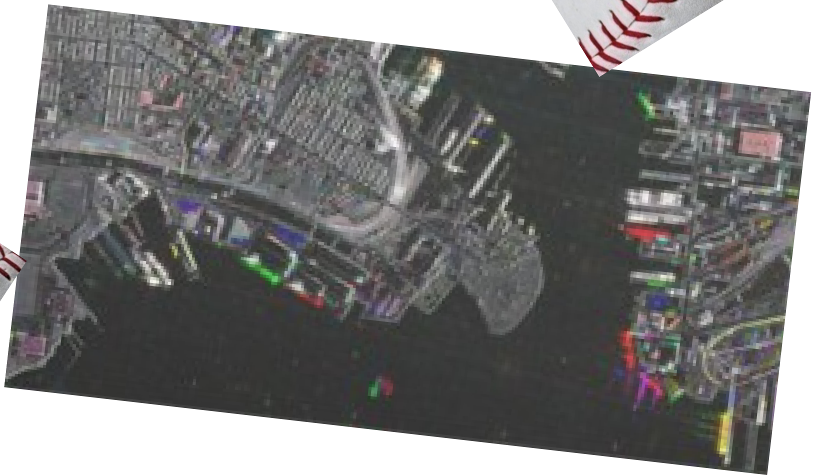




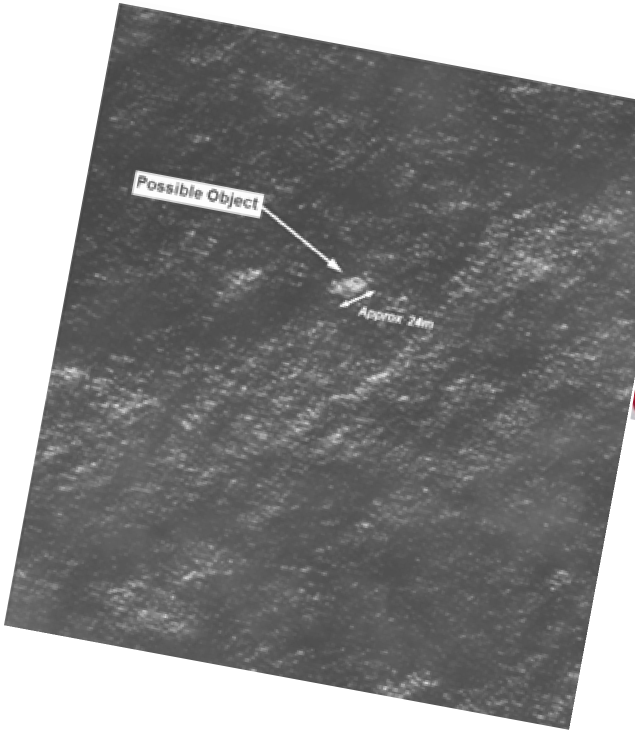
Beware of the "stitches"





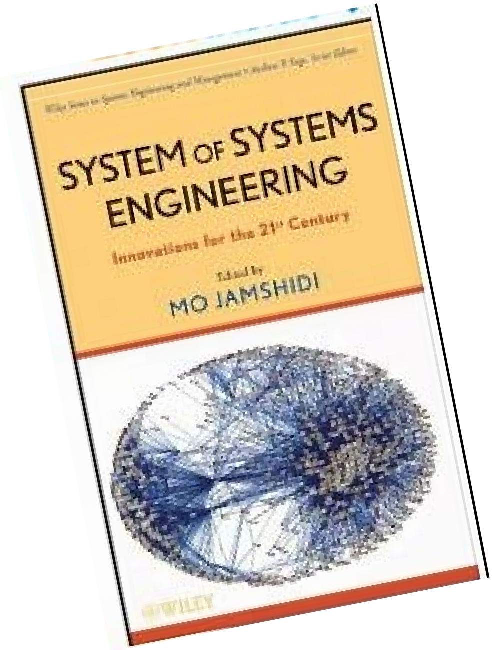


Beware of those doing the “stitching”



Communication and
Decision Making
are the “stitches”

**“Take the red pill …
See how deep the
rabbit hole goes”**



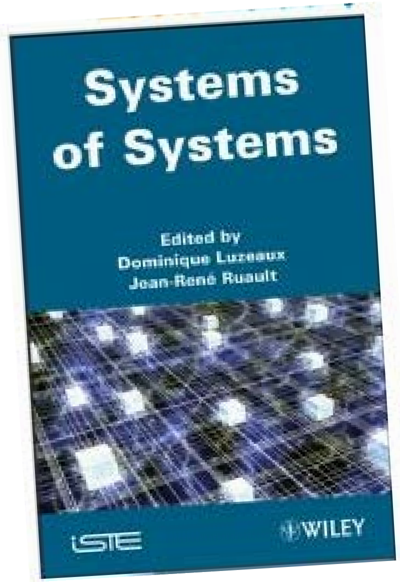
SYSTEM OF SYSTEMS ENGINEERING

Innovations for the 21st Century

Edited by

MO JAMSHIDI

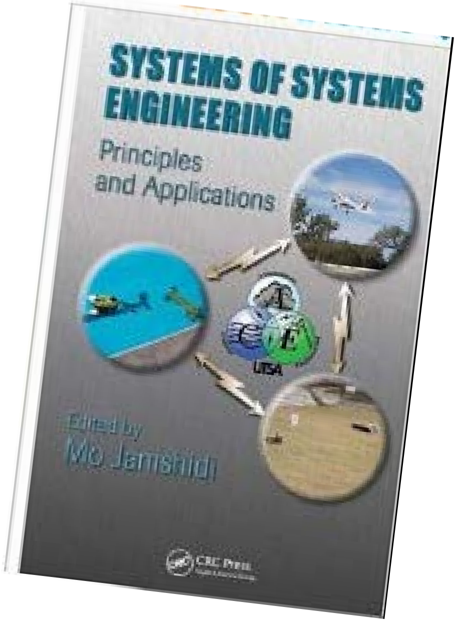
WILEY



Systems of Systems

Edited by
Dominique Luzeaux
Jean-René Ruault

ISTE WILEY

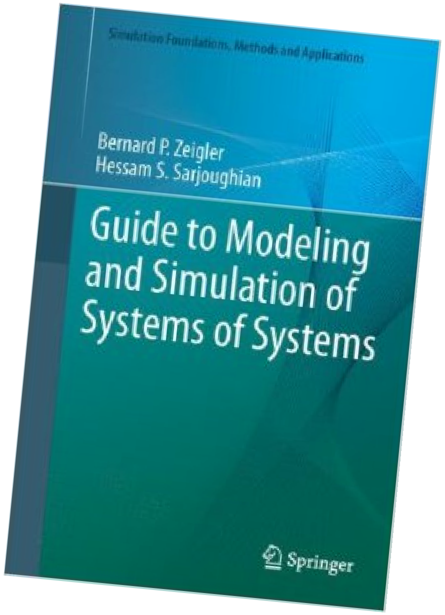


SYSTEMS OF SYSTEMS ENGINEERING

Principles and Applications

Edited by
Mo Jamshidi

CRC Press

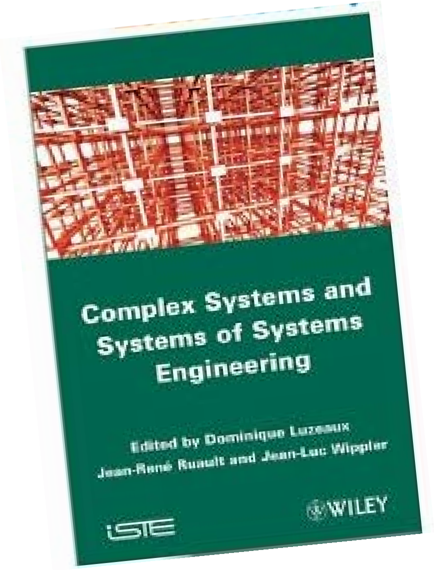


Simulation Foundations, Methods and Applications

Bernard P. Zeigler
Hessam S. Sarjoughian

Guide to Modeling and Simulation of Systems of Systems

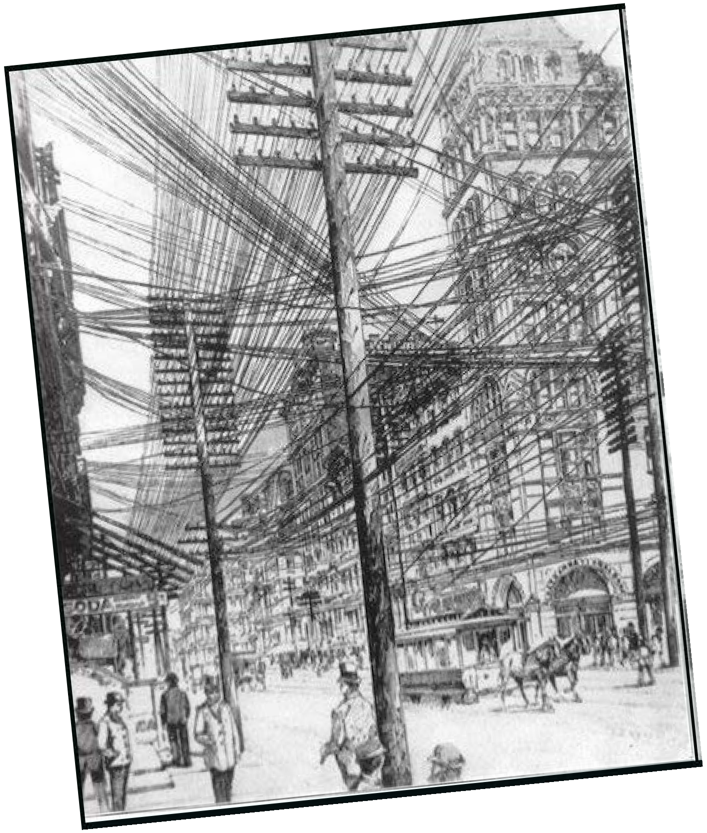
Springer



Complex Systems and Systems of Systems Engineering

Edited by Dominique Luzeaux
Jean-René Ruault and Jean-Luc Wippler

ISTE WILEY



virtual

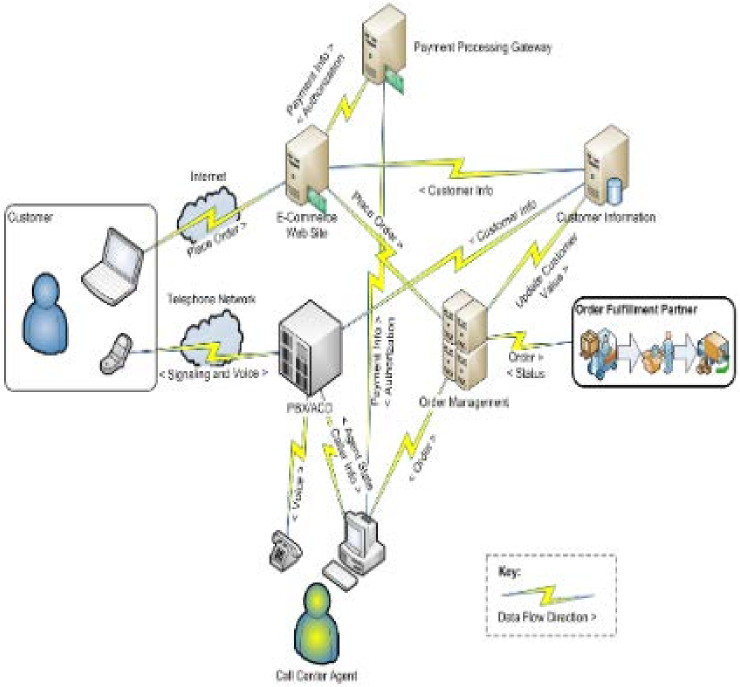
acknowledged

collaborative

directed

Software Engineering Institute:

“Mission Threads”



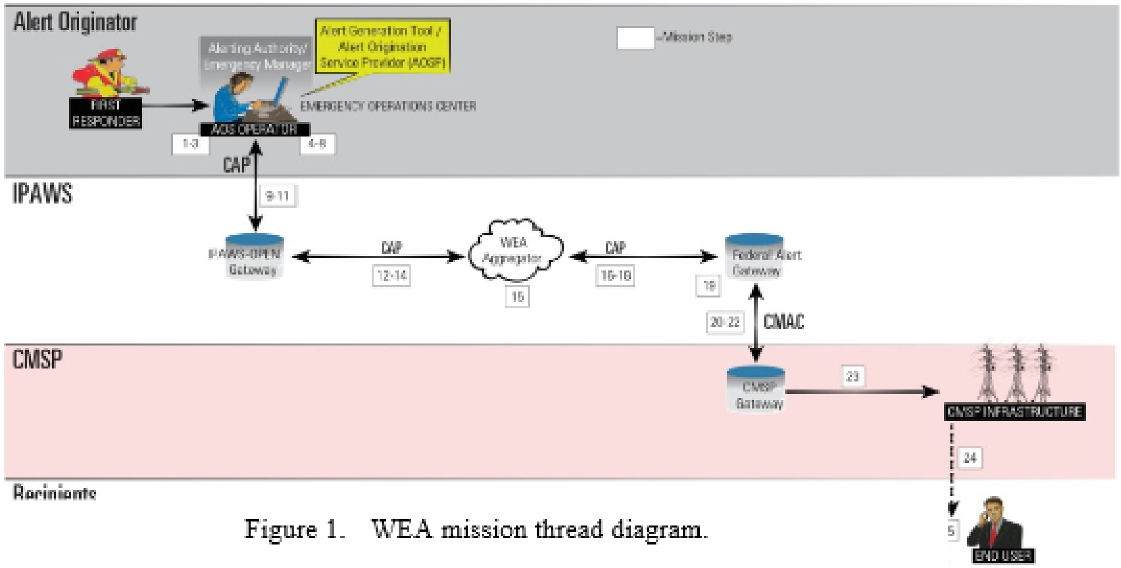
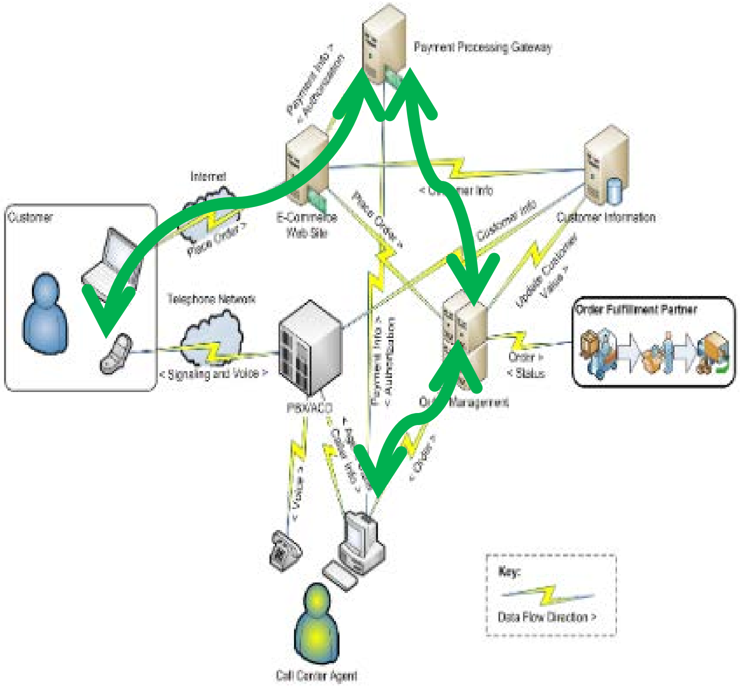


Figure 1. WEA mission thread diagram.



Also need:

“Assurance Threads”

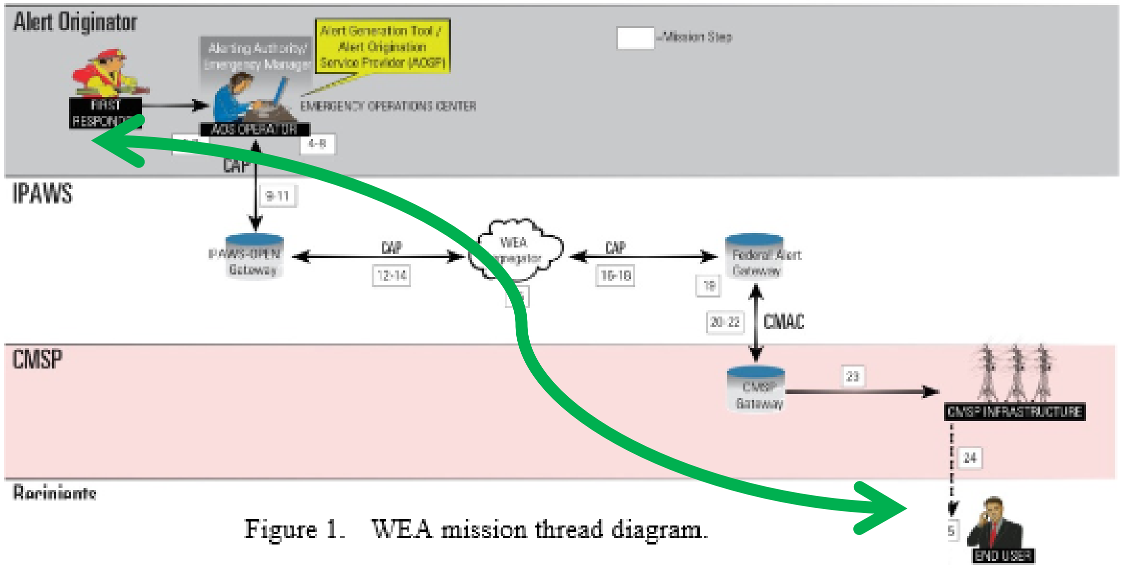
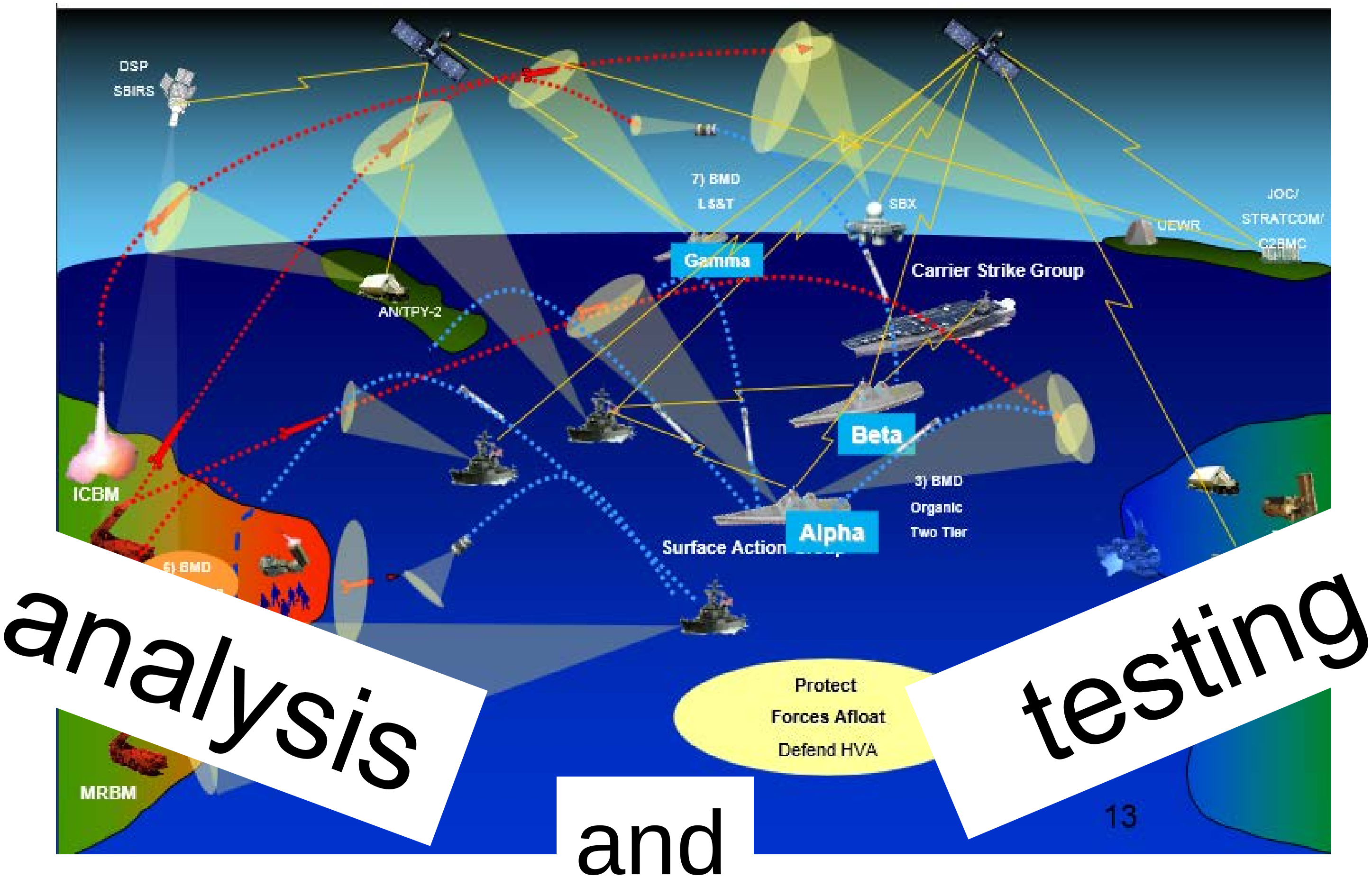


Figure 1. WEA mission thread diagram.

Scenario-based



analysis and testing

Assurance

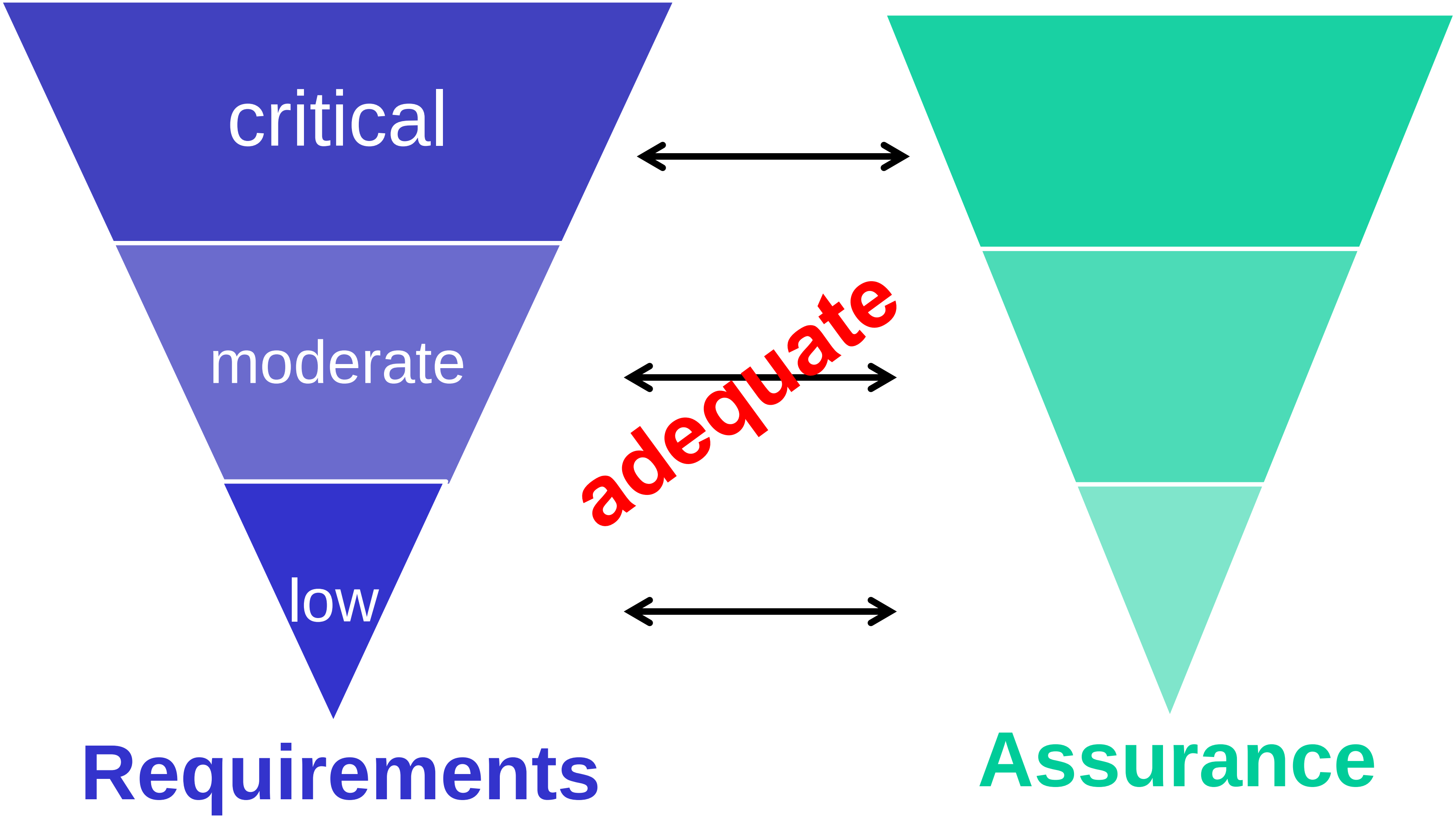
It’s all a “confidence” game.

Providing adequate confidence that …

… product requirements are being satisfied.

… project plans are being actualized.

… stakeholders’ interests are being honored.


critical
moderate
low
adequate
Requirements
Assurance

Let’s consider ….

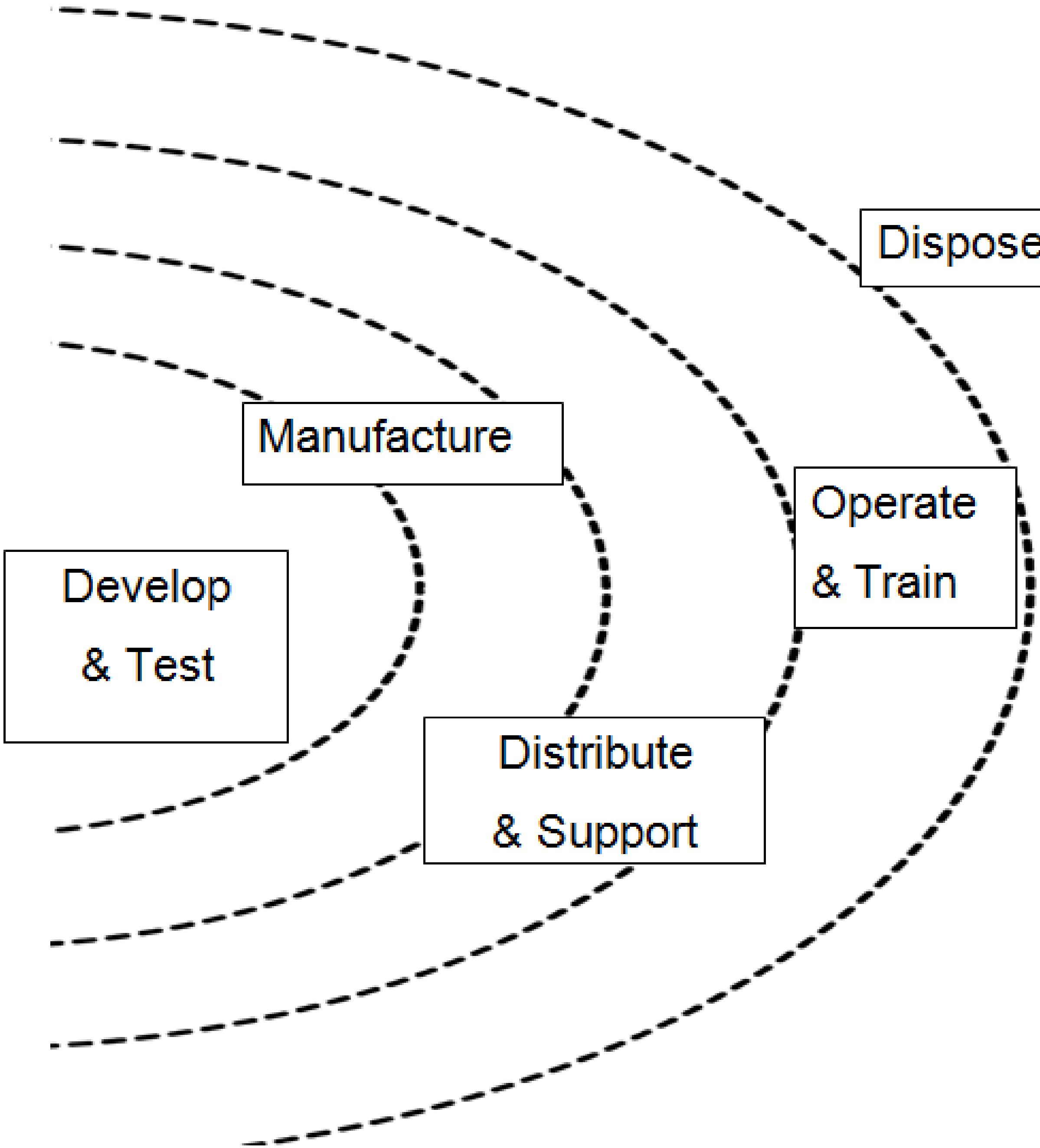
What systems? What assurance?

Challenges

Responses

The Way Forward

Meeting stakeholders' expectations



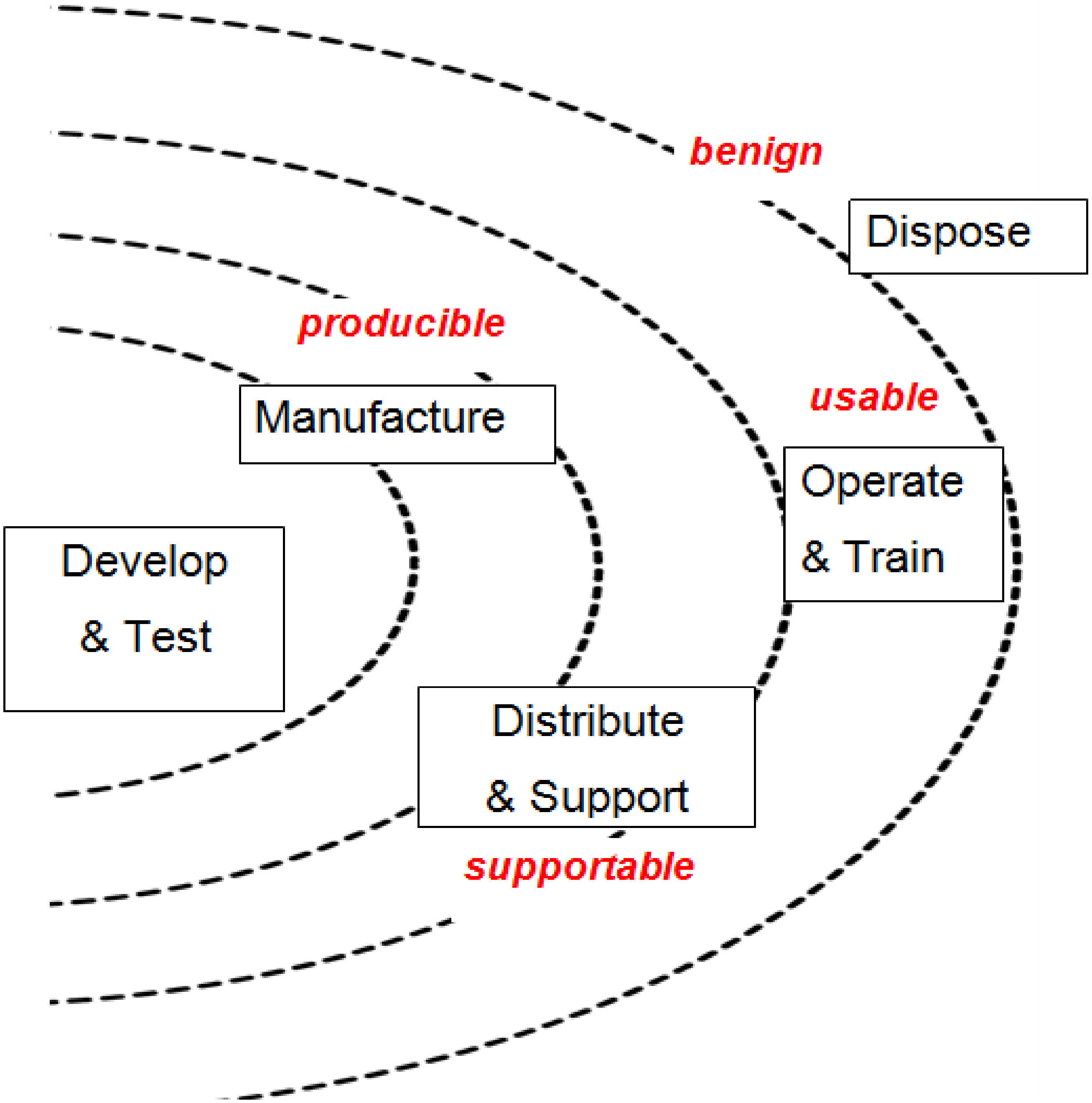
Develop & Test

Manufacture

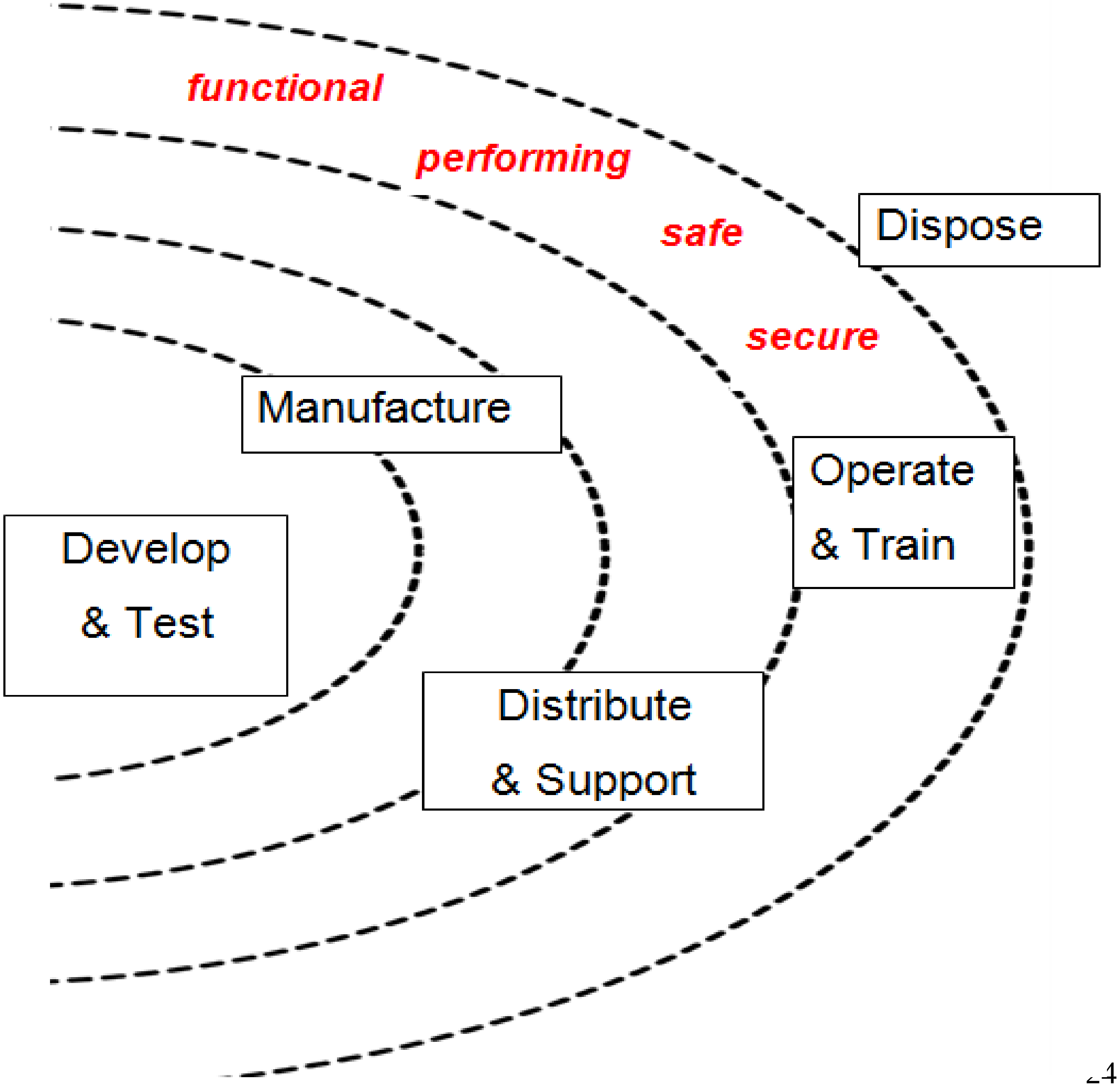
Distribute & Support

Operate & Train

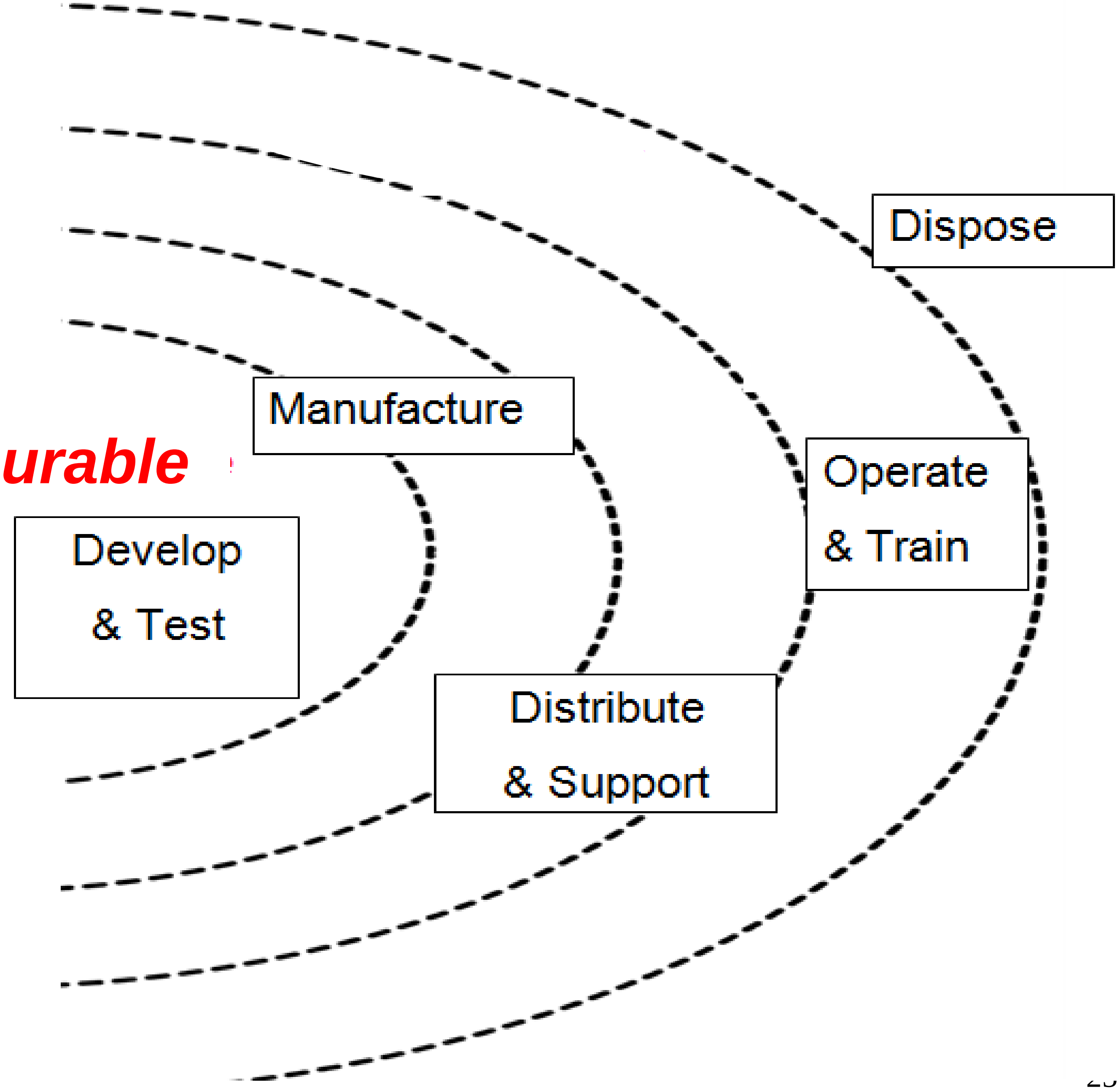
Dispose



benign
Dispose
producible
Manufacture
usable
Operate & Train
Develop & Test
Distribute & Support
supportable

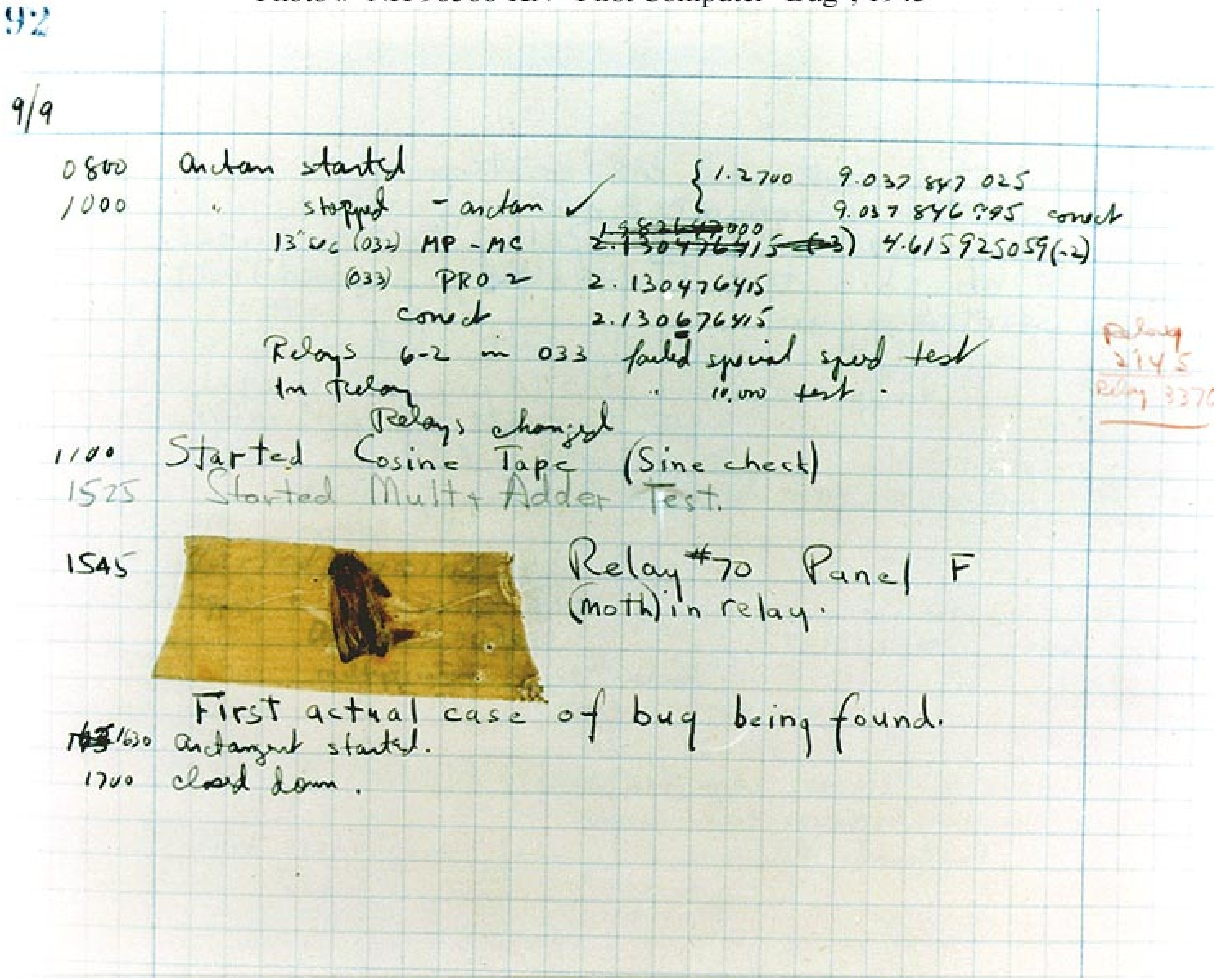

functional
performing
safe
secure
Dispose
Manufacture
Operate
& Train
Develop
& Test
Distribute
& Support

assurable


Dispose
Manufacture
Operate
& Train
Develop
& Test
Distribute
& Support

Success criteria

Photo # NH 96566-KN First Computer "Bug", 1945



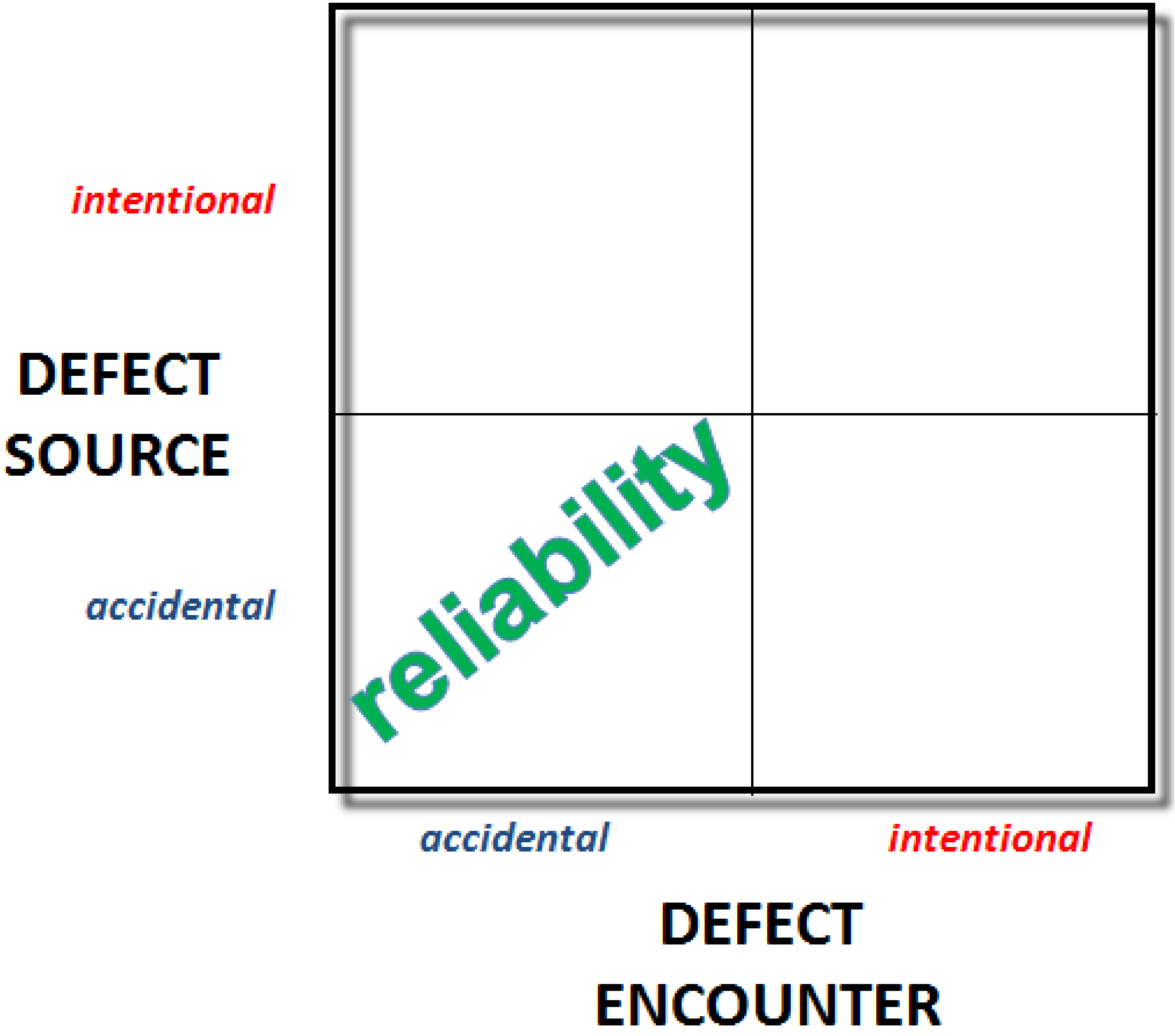
9/9

0800 Arctan started
1000 " stopped - arctan ✓ {1.2700 9.037 847 025
9.037 846 995 correct
13" UC (032) MP - MC ~~1.982647000~~ ~~2.130476415~~ ~~(-3)~~) 4.615925059(-2)
(033) PRO 2 2.130476415
correct 2.130676415
Relays 6-2 in 033 failed special speed test
In relay " 10,000 test.
Relays changed

Relay 2145
Relay 3376

1100 Started Cosine Tape (Sine check)
1525 Started Mult + Adder Test.
1545 Relay #70 Panel F
(moth) in relay.

First actual case of bug being found.
~~1600~~ 1630 Arctangent started.
1700 closed down.



intentional

DEFECT
SOURCE

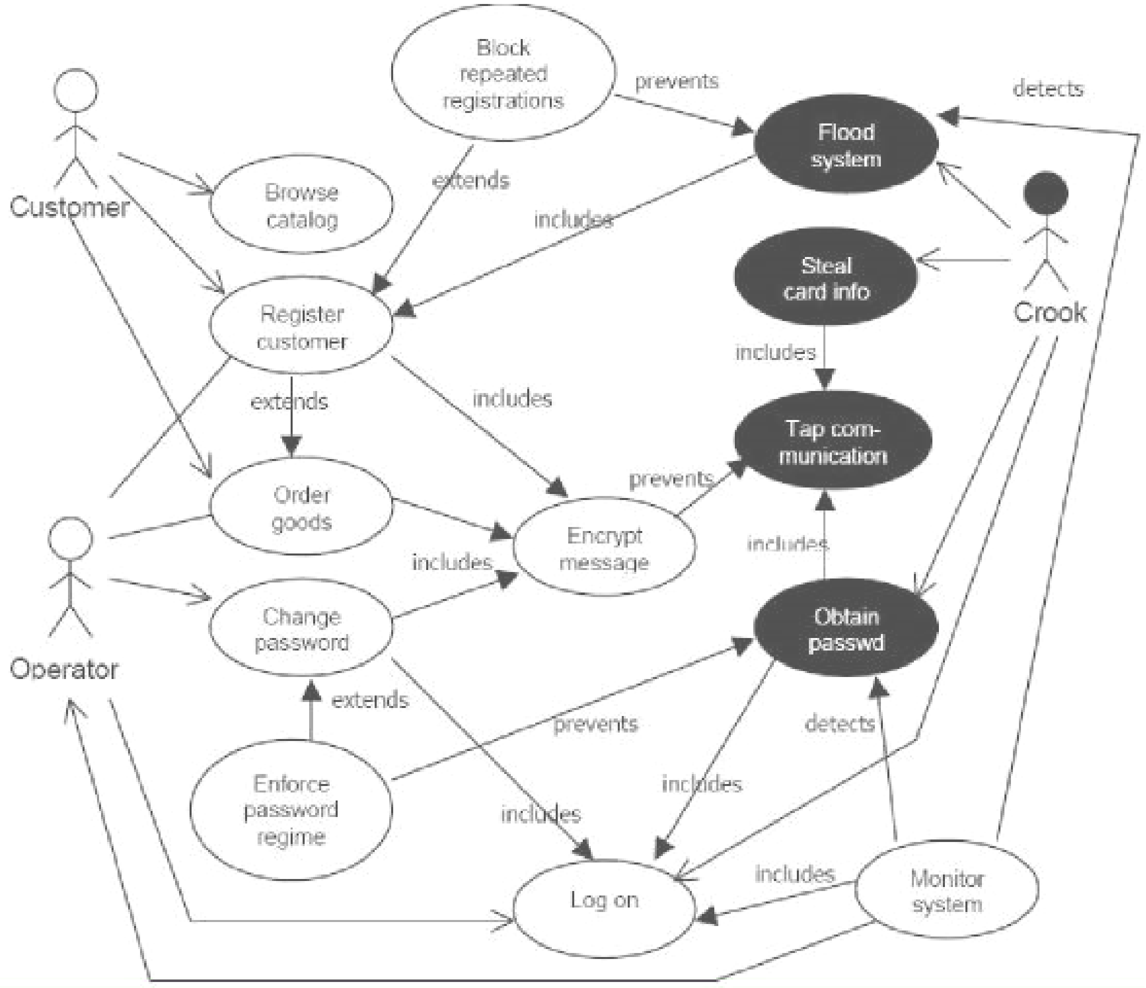
accidental

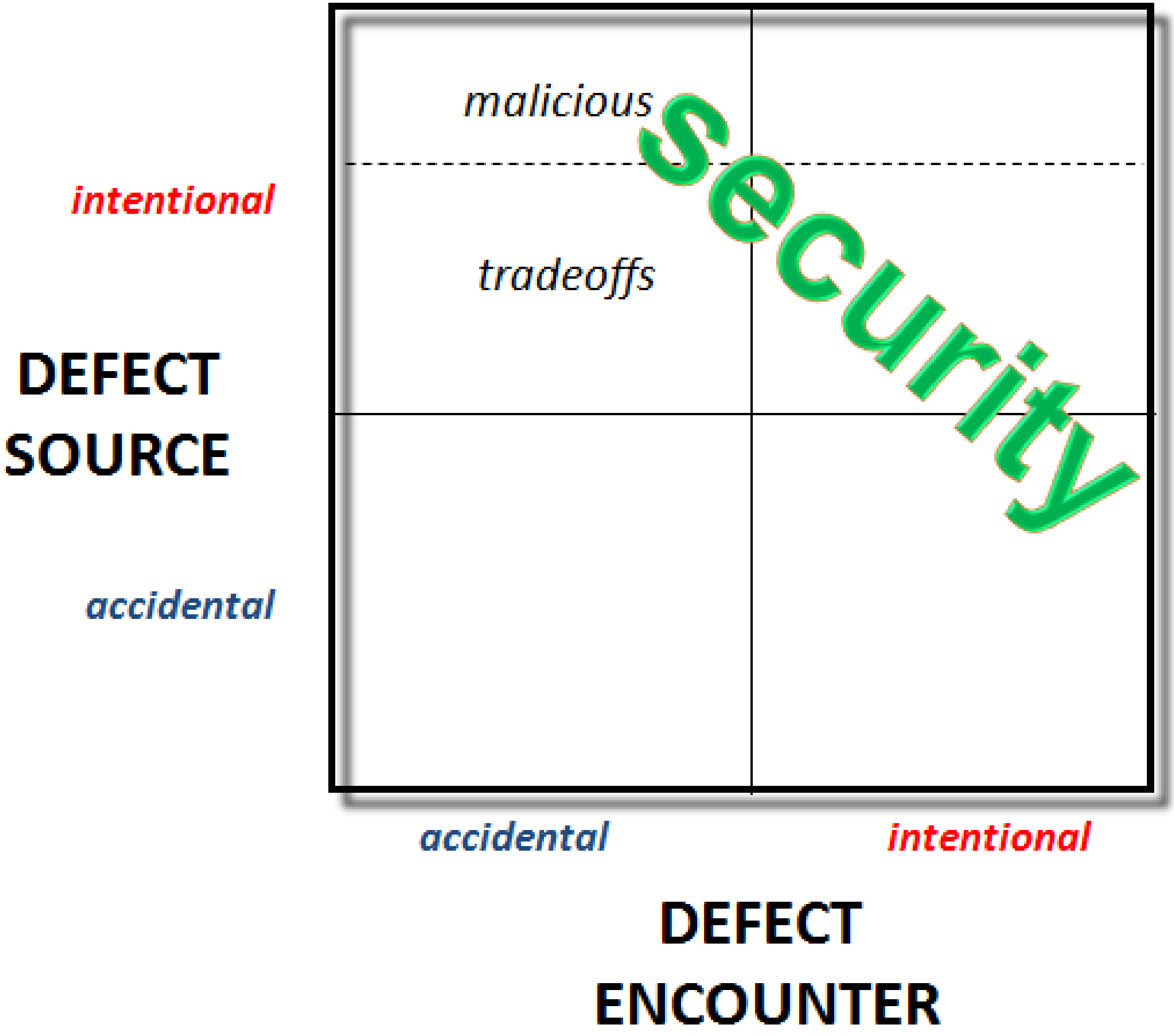
reliability

accidental

intentional

DEFECT
ENCOUNTER


Block repeated registrations
prevents
detects
Flood system
Customer
Browse catalog
extends
includes
Crook
Steal card info
Register customer
includes
extends
includes
Tap com-munication
prevents
Order goods
Encrypt message
includes
includes
Change password
Obtain passwd
Operator
extends
prevents
detects
includes
Enforce password regime
includes
includes
Log on
Monitor system



malicious

tradeoffs

security

intentional

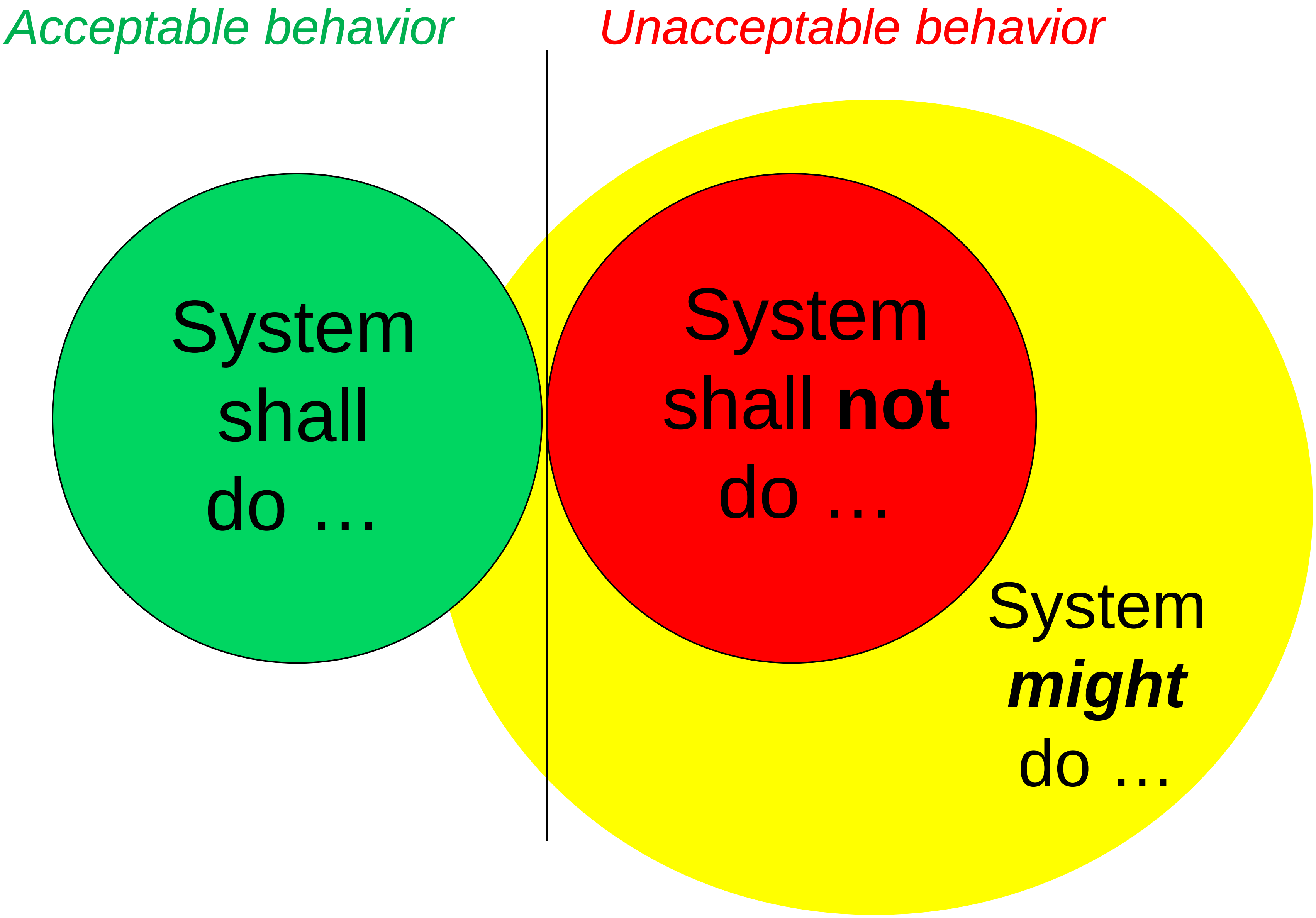
DEFECT SOURCE

accidental

accidental

intentional

DEFECT ENCOUNTER


Acceptable behavior
Unacceptable behavior
System shall do …
System shall **not** do …
System ***might*** do …

Security Requirements

confidentiality

integrity

accessibility

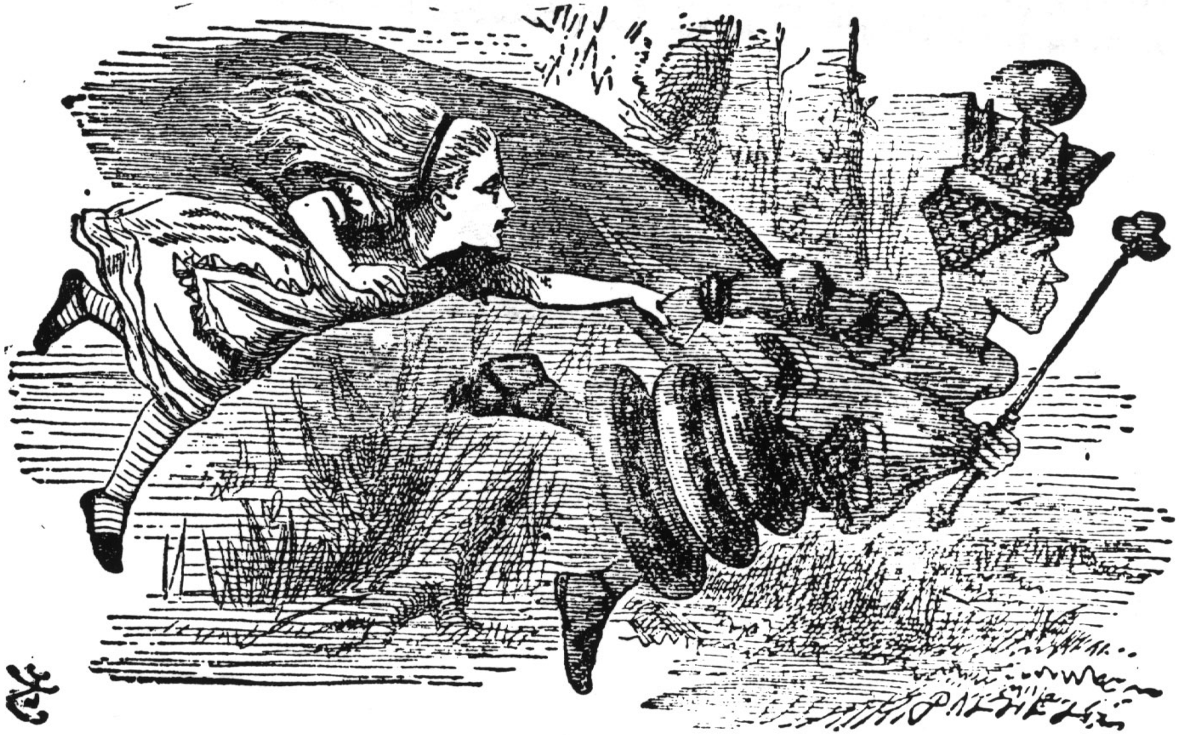
Let’s consider ….

What systems? What assurance?

Challenges

Responses

The Way Forward



“We must run as fast as we can,
just to stay in place.

And if you wish to go anywhere,
you must run twice as fast as that.”

static

assessments

inspections

walkthroughs

audits

reviews

prototyping

simulation

unit testing

integration testing

system testing

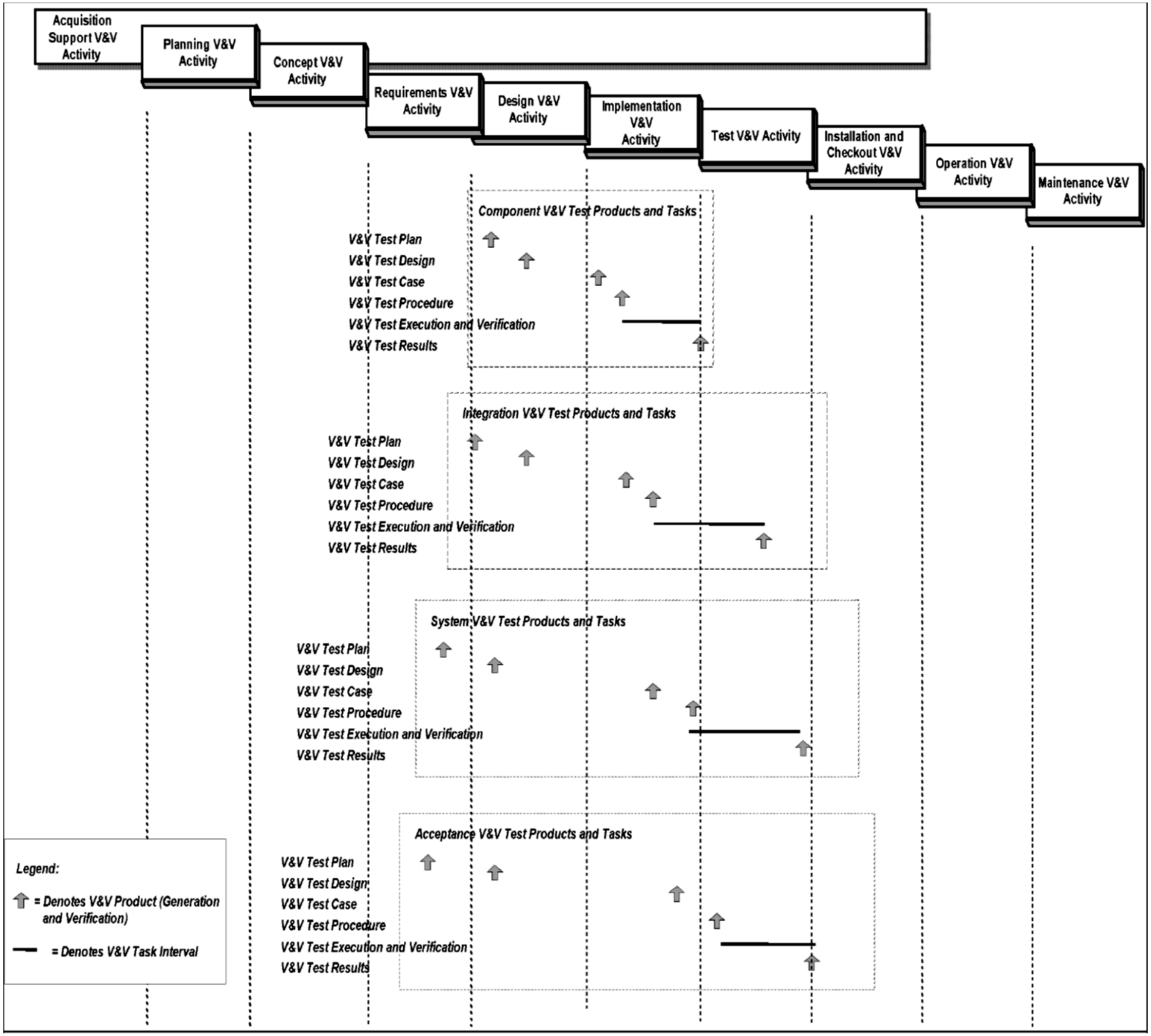
acceptance testing

dynamic assessments

	Process: Acquisition (5.2)	Process: Supply (5.3)	Process: Development (5.4)						Process: Operation (5.5)	Process: Maintenance (5.6)
V&V Inputs	(1) Prel System Description (2) Statement of Need (3) Draft RFP or Tender (4) System Integrity Level Scheme (5) SVVP (6) Contract (7) Supplier Development Plans & Schedules (8) User Needs (9) Concept Documentation (10) SDD, IDD, SRS, IRS (11) Source Code (12) Executable Code (13) Test Plans, Designs, Cases, Procedures, Results (14) Acceptance Test Plan (15) V&V Task Results	(1) SVVP (2) Contract (3) Supplier Development Plans & Schedules (4) RFP or Tender (5) User Needs	(1) Concept Documentation (2) Supplier Development Plans & Schedules (3) User Needs (4) Acquisition Needs (5) Developer Integrity Level Assignments (6) Preliminary Threat and Risk Assessment (TRA) (7) Hazard Analysis Report (8) Security Analysis (9) V&V Tasks Results	(1) Concept Documentation (2) SRS (3) IRS (4) Criticality Task Report (5) User Documentation (6) System Test Plan (7) Acceptance Test Plan (8) SW Config Management Process Documentation (9) Hazard Analysis Report (10) Preliminary TRA (11) Supplier Development Plans & Schedules (12) Security Analysis (13) V&V Task Results	(1) SRS (2) SDD (3) IRS (4) IDD (5) Design Standards (6) Concept Documentation (7) Criticality Task Report (8) Test Plans & Designs (9) User Documentation (10) Hazard Analysis Report (11) Supplier Development Plans & Schedules (12) Security Analysis (13) V&V Task Results	(1) SRS (2) SDD (3) IRS (4) IDD (5) Source & Executable Code (6) Coding Stds (7) User Documentation (8) Concept Documentation (9) Criticality Task Report (10) Test Plans/Designs/Cases (11) Test Procedures (12) Component Test Results (13) Hazard Analysis Report (14) Supplier Development Plans & Schedules (15) Security Analysis (16) V&V Task Results	(1) Test Plans, Designs, and Procedures (2) SDD (3) IDD (4) Source and Executable Code (5) User Documentation (6) Test Results (7) Hazard Analysis Report (8) Supplier Development Plans & Schedules (9) Security Analysis (10) V&V Task Results	(1) Installation Package (2) User Documentation (3) Hazard Analysis Report (4) Supplier Development Plans & Schedules (5) Security Analysis (6) V&V Task Results (7) V&V Activity Summary Reports	(1) SVVP (2) New Constraints (3) Proposed Changes (4) Installation Package (5) Operating Procedures (6) User Documentation (7) Concept Documentation (8) Hazard Analysis Report (9) Environmental Changes (10) Security Analysis (11) Supplier Development Plans & Schedules (12) Operational Problem Reports (13) V&V Task Results	(1) SVVP (2) Approved Changes (3) Installation Package (4) Supplier Development Plans & Schedules (5) Proposed Changes (6) Anomaly Reports (7) Maintainer Integrity Levels (8) Hazard Analysis Report (9) Security Analysis (10) Supplier Development Plans & Schedule (11) Operation Problem Reports (12) V&V Task Results
	Activity: Acquisition Support V&V (5.2.1)	Activity: Planning V&V (5.3.1)	Activity: Concept V&V (5.4.1)	Activity: Requirements V&V (5.4.2)	Activity: Design V&V (5.4.3)	Activity: Implementation V&V (5.4.4)	Activity: Test V&V (5.4.5)	Activity: Installation and Checkout V&V (5.4.6)	Activity: Operation V&V (5.5.1)	Activity: Maintenance V&V (5.6.1)
V&V Tasks	(1) Scoping the V&V Effort (2) Planning the Interface Between V&V Effort and Supplier (3) System Requirements Review (4) Acceptance Support	(1) Planning the Interface Between V&V Effort and Supplier (2) Contract Verification	(1) Concept Documentation Evaluation (2) Criticality Analysis (3) Hardware/Software/User Requirements Allocation Analysis (4) Traceability Analysis (5) Hazard Analysis (6) Security Analysis (7) Risk Analysis	(1) Traceability Analysis (2) Software Requirements Evaluation (3) Interface Analysis (4) Criticality Analysis (5) System V&V Test Plan Generation (6) Acceptance V&V Test Plan Generation (7) Configuration Management Assessment (8) Hazard Analysis (9) Security Analysis (10) Risk Analysis	(1) Traceability Analysis (2) Software Design Evaluation (3) Interface Analysis (4) Criticality Analysis (5) Component V&V Test Plan Generation (6) Integration V&V Test Plan Generation (7) Component V&V Test Design Generation (8) Integration V&V Test Design Generation (9) System V&V Test Design Generation (10) Acceptance V&V Test Design Generation (11) Hazard Analysis (12) Security Analysis (13) Risk Analysis	(1) Traceability Analysis (2) Source Code and Source Code Documentation Evaluation (3) Interface Analysis (4) Criticality Analysis (5) Component V&V Test Case Generation (6) Integration V&V Test Case Generation (7) System V&V Test Case Generation (8) Acceptance V&V Test Case Generation (9) Component V&V Test Procedure Generation (10) Integration V&V Test Procedure Generation (11) System V&V Test Procedure Generation (12) Component V&V Test Execution (13) Hazard Analysis (14) Security Analysis (15) Risk Analysis	(1) Traceability Analysis (2) Acceptance V&V Test Procedure Generation (3) Integration V&V Test Execution (4) System V&V Test Execution (5) Acceptance V&V Test Execution (6) Hazard Analysis (7) Security Analysis (8) Risk Analysis	(1) Installation Configuration Audit (2) Installation Checkout (3) Hazard Analysis (4) Security Analysis (5) Risk Analysis (6) V&V Final Report Generation	(1) Evaluation of New Constraints (2) Operating Procedures Evaluation (3) Hazard Analysis (4) Security Analysis (5) Risk Analysis	(1) SVVP Revision (2) Anomaly Evaluation (3) Criticality Analysis (4) Migration Assessment (5) Retirement Assessment (6) Hazard Analysis (7) Security Analysis (8) Risk Analysis (9) Task Iteration
Outputs	(1) SVVP and Updates (2) Task Report(s) (3) Anomaly Report(s)	(1) Updated SVVP (2) Task Report(s) (3) Anomaly Report(s)	(1) Task Report(s) (2) Anomaly Report(s)	(1) Task Report(s) (2) Anomaly Report(s) (3) V&V Test Plans • System • Acceptance	(1) Task Report(s) (2) Anomaly Report(s) (3) V&V Test Plans • Component • Integration (4) V&V Test Designs	(1) Task Report(s) (2) Anomaly Report(s) (3) V&V Test Cases • Component • Integration • System	(1) Task Report(s) (2) Anomaly Report(s) (3) V&V Test Procedures • Acceptance	(1) Task Report(s) (2) Anomaly Report(s) (3) V&V Final Report	(1) Task Report(s) (2) Anomaly Report(s)	(1) Updated SVVP (2) Task Report(s) (3) Anomaly Report(s)

Testing Lifecycles

-- IEEE 1012



Acquisition Support V&V Activity

Planning V&V Activity

Concept V&V Activity

Requirements V&V Activity

Design V&V Activity

Implementation V&V Activity

Test V&V Activity

Installation and Checkout V&V Activity

Operation V&V Activity

Maintenance V&V Activity

Component V&V Test Products and Tasks

- *V&V Test Plan*
- *V&V Test Design*
- *V&V Test Case*
- *V&V Test Procedure*
- *V&V Test Execution and Verification*
- *V&V Test Results*

Integration V&V Test Products and Tasks

- *V&V Test Plan*
- *V&V Test Design*
- *V&V Test Case*
- *V&V Test Procedure*
- *V&V Test Execution and Verification*
- *V&V Test Results*

System V&V Test Products and Tasks

- *V&V Test Plan*
- *V&V Test Design*
- *V&V Test Case*
- *V&V Test Procedure*
- *V&V Test Execution and Verification*
- *V&V Test Results*

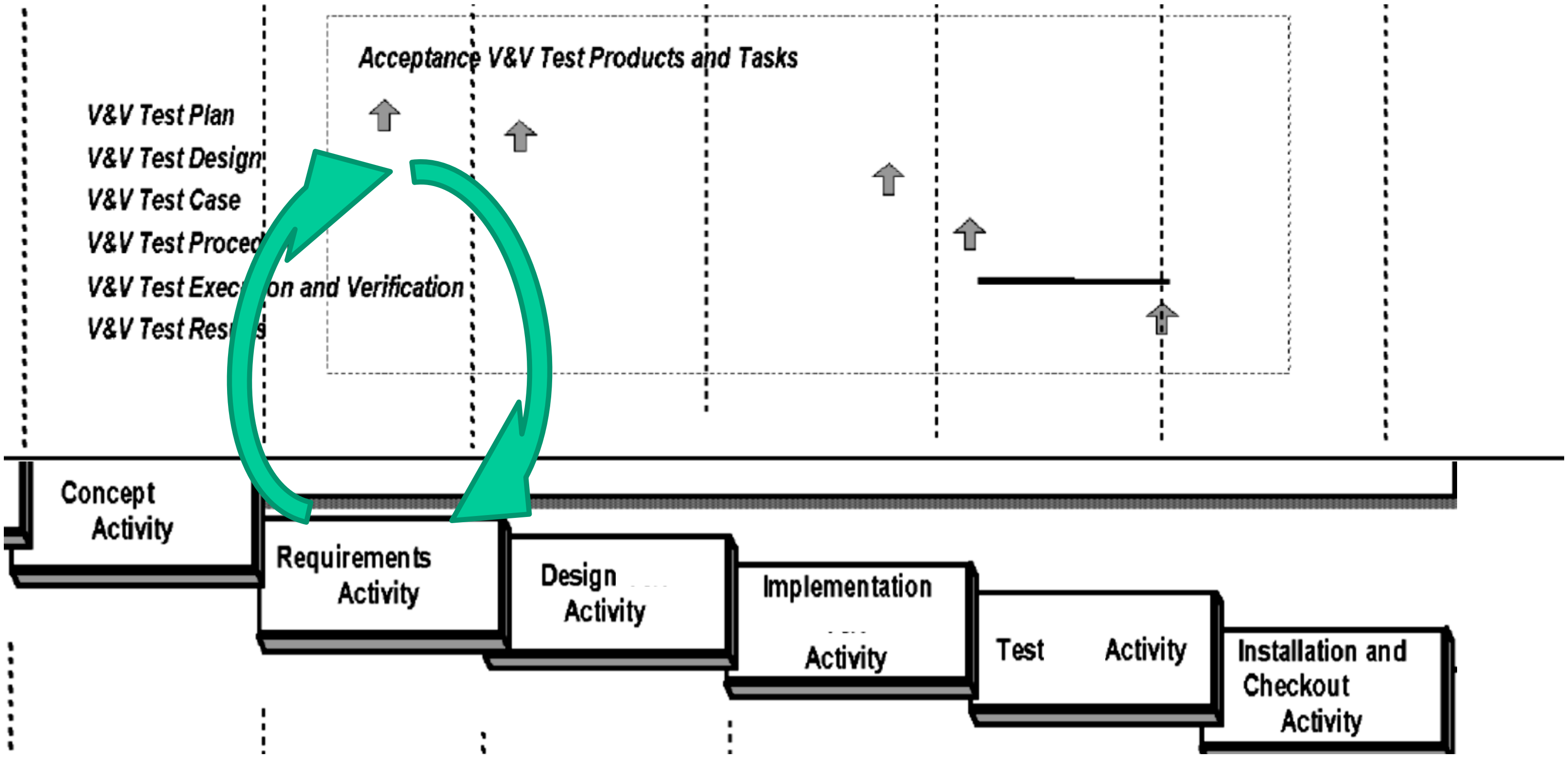
Acceptance V&V Test Products and Tasks

- *V&V Test Plan*
- *V&V Test Design*
- *V&V Test Case*
- *V&V Test Procedure*
- *V&V Test Execution and Verification*
- *V&V Test Results*

Legend:

⇧ = Denotes V&V Product (Generation and Verification)

▬ = Denotes V&V Task Interval



Acceptance V&V Test Products and Tasks

V&V Test Plan

V&V Test Design

V&V Test Case

V&V Test Proced

V&V Test Exec on and Verification

V&V Test Res s

Concept Activity

Requirements Activity

Design Activity

Implementation Activity

Test Activity

Installation and Checkout Activity

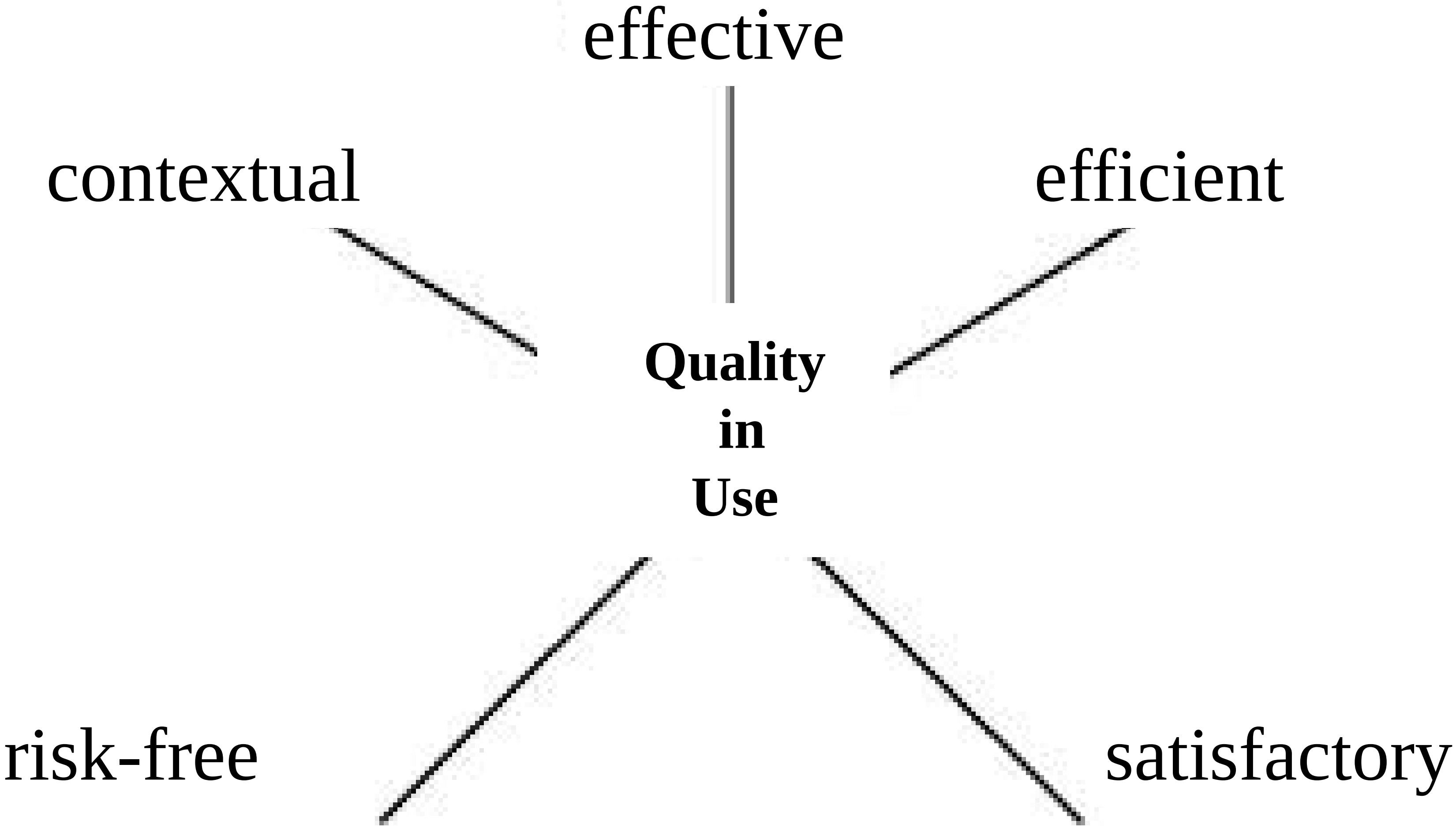
Let’s consider ….

What systems? What assurance?

Challenges

Responses

The Way Forward



effective

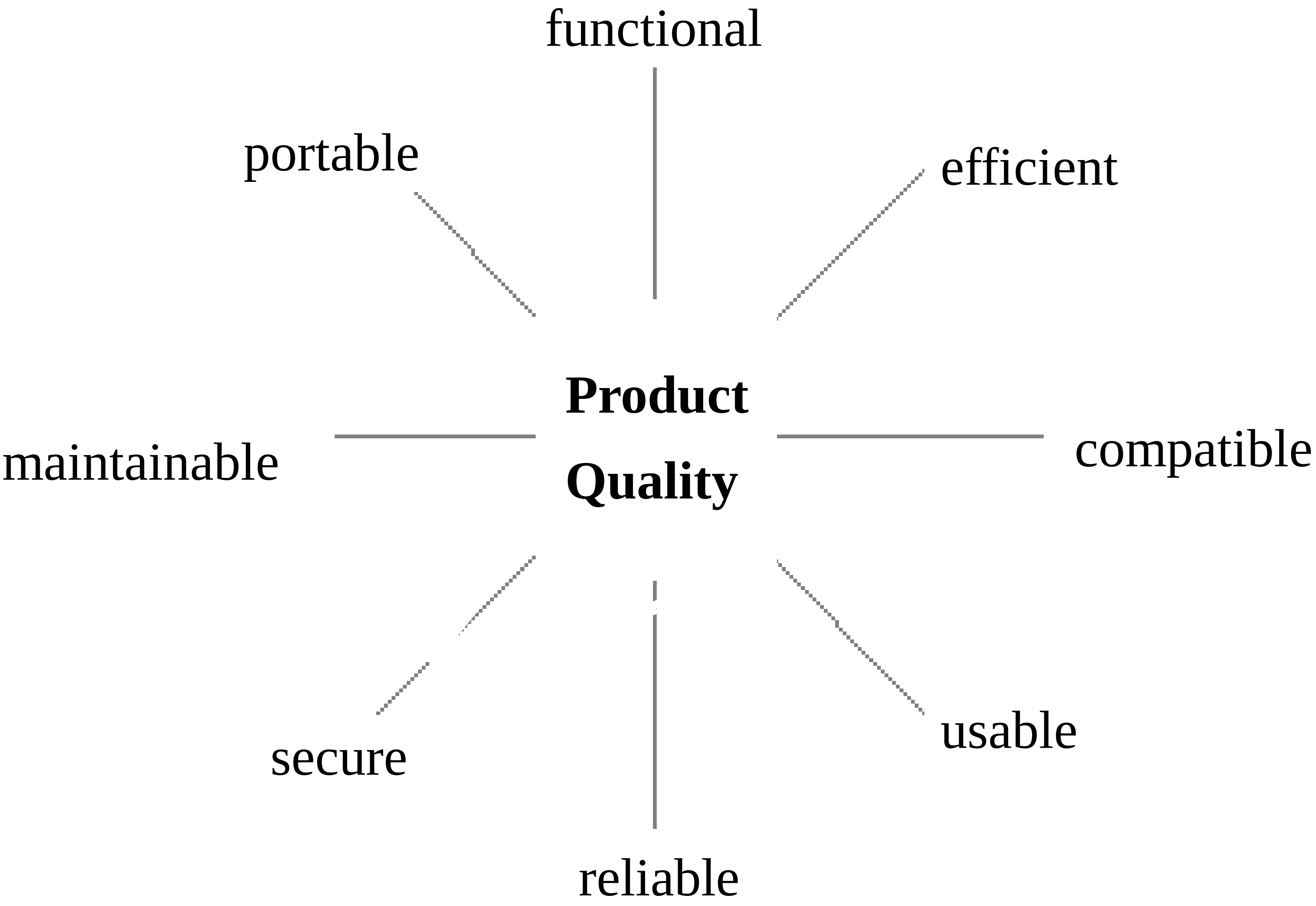
contextual

efficient

Quality in Use

risk-free

satisfactory



functional

portable

efficient

Product Quality

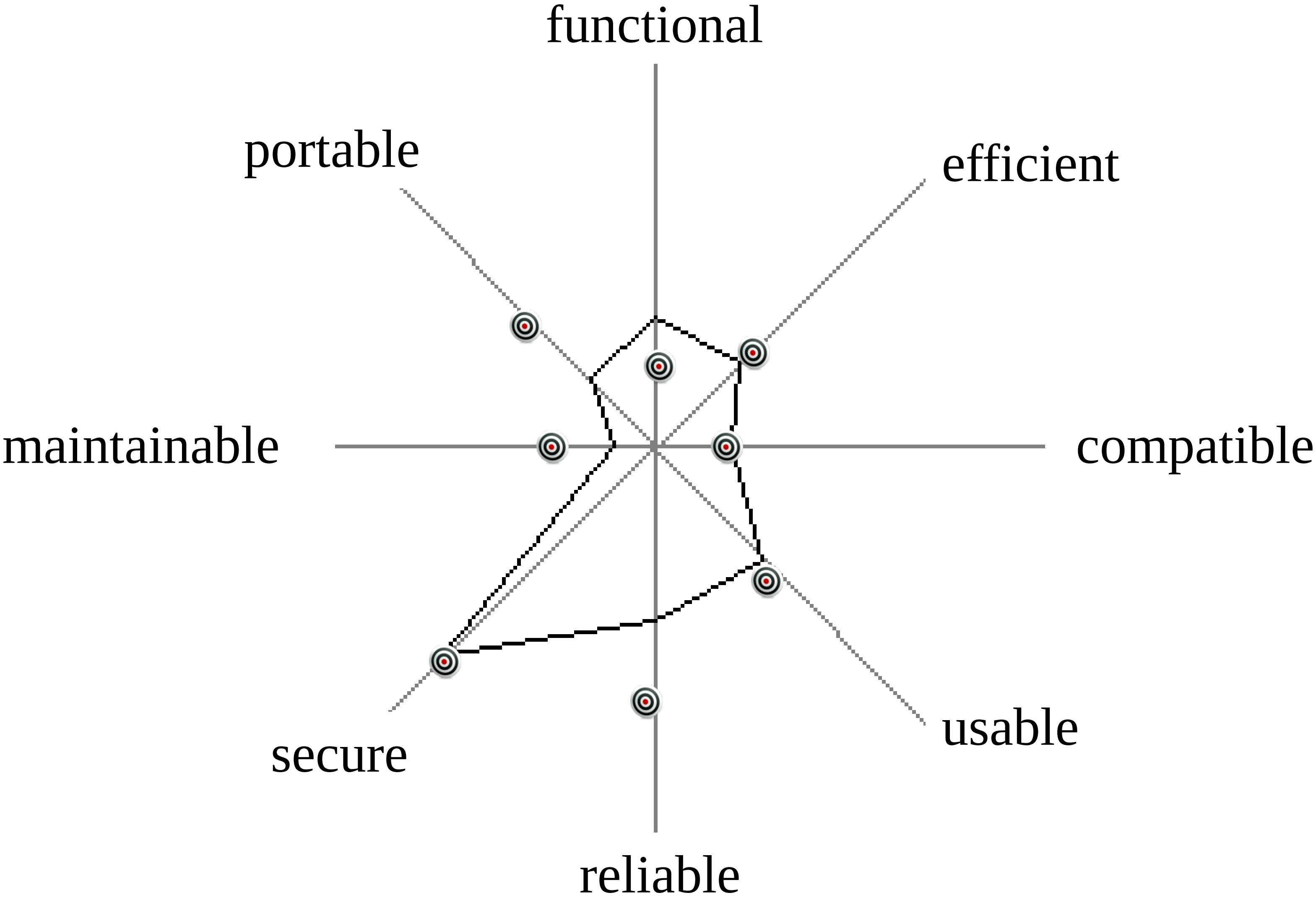
maintainable

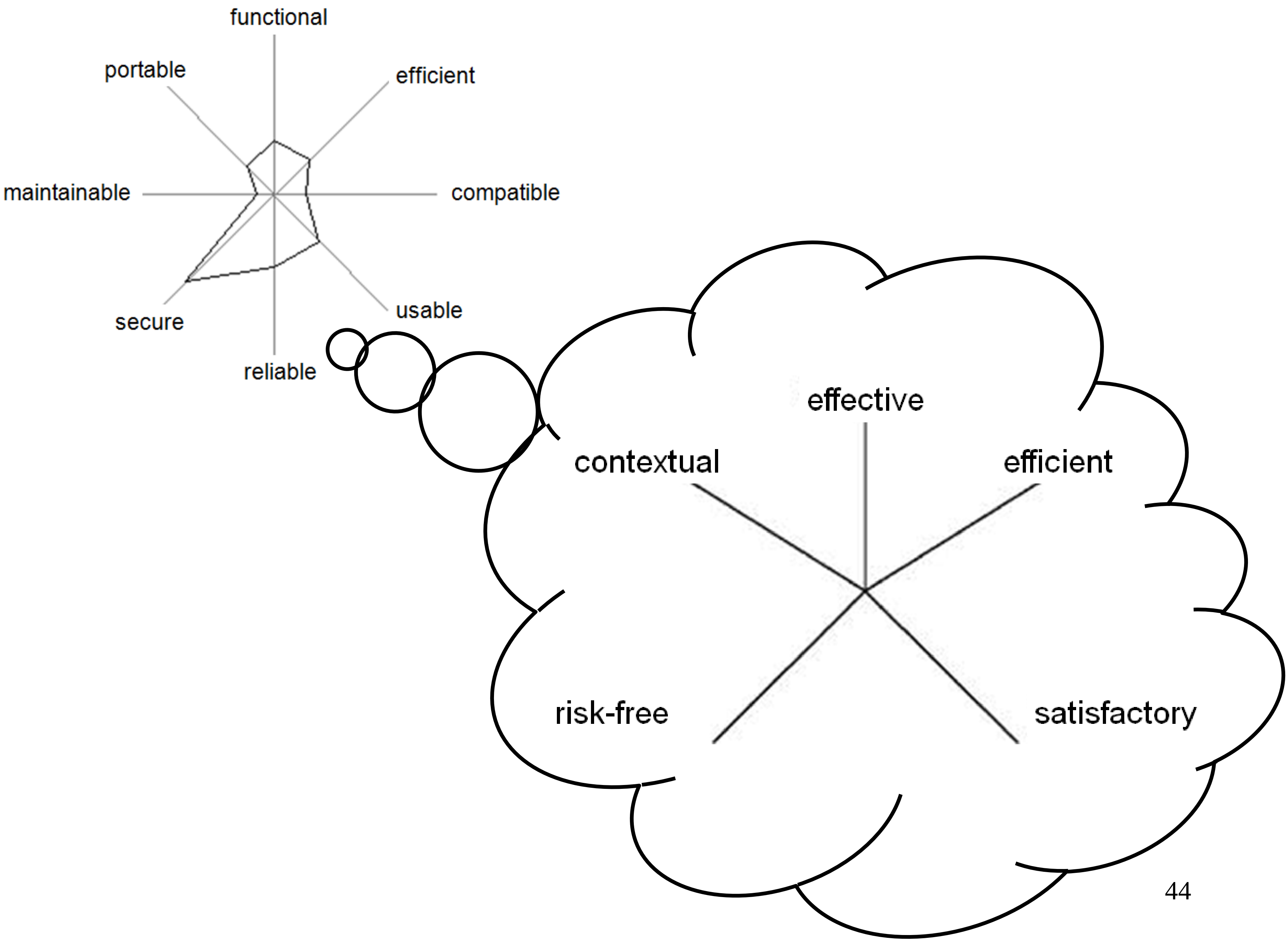
compatible

secure

usable

reliable


functional
portable
efficient
maintainable
compatible
secure
usable
reliable



functional

efficient

compatible

usable

reliable

secure

maintainable

portable

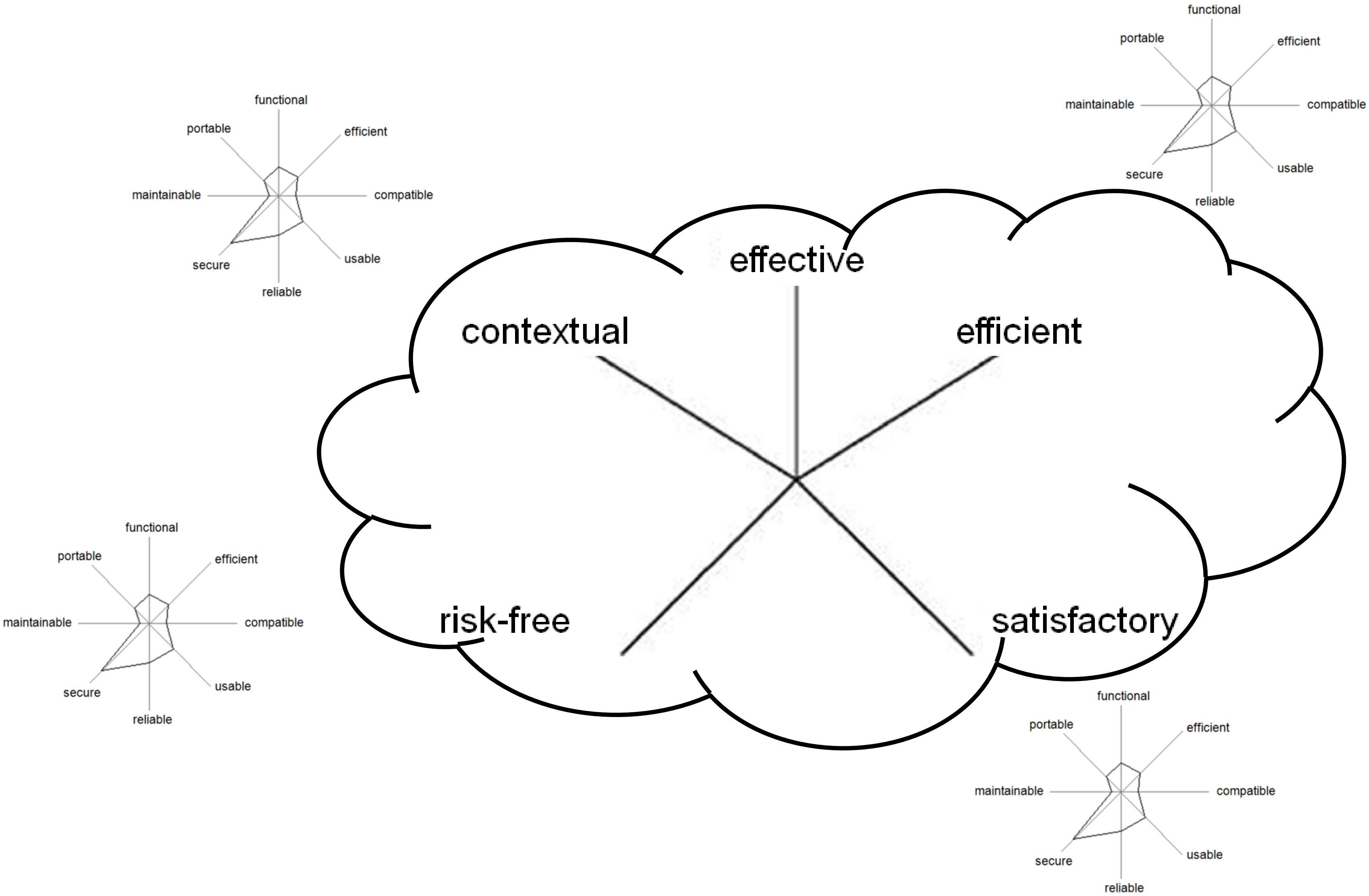
effective

efficient

satisfactory

risk-free

contextual



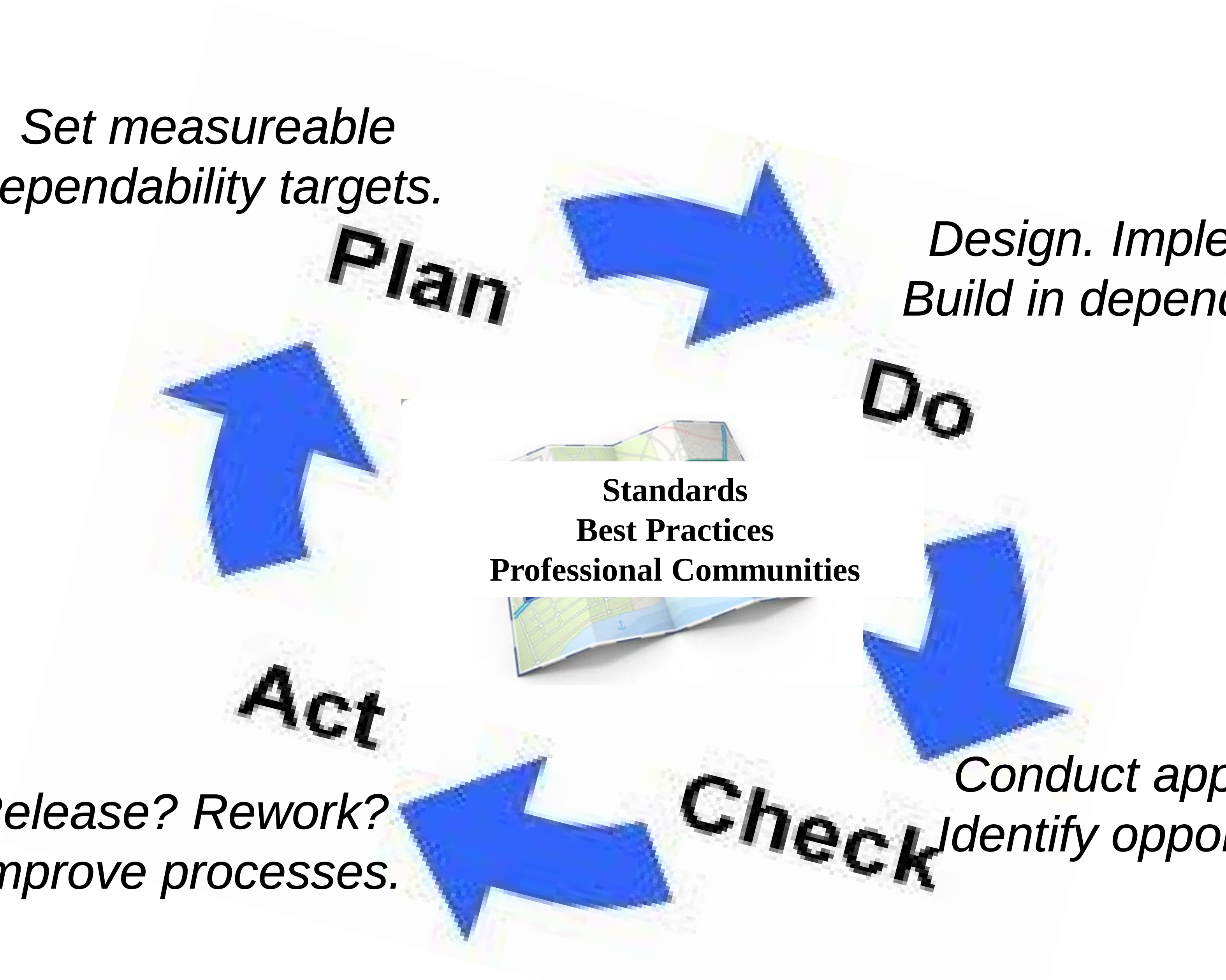
effective

contextual

efficient

risk-free

satisfactory



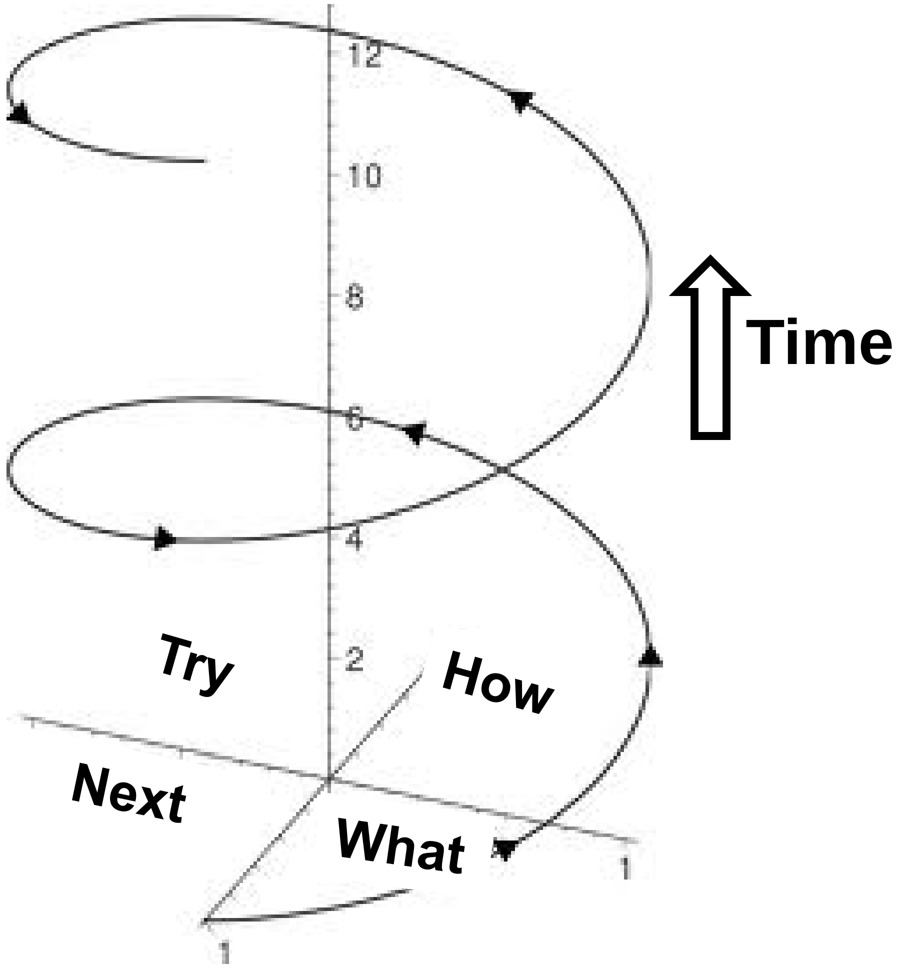
Set measureable dependability targets.

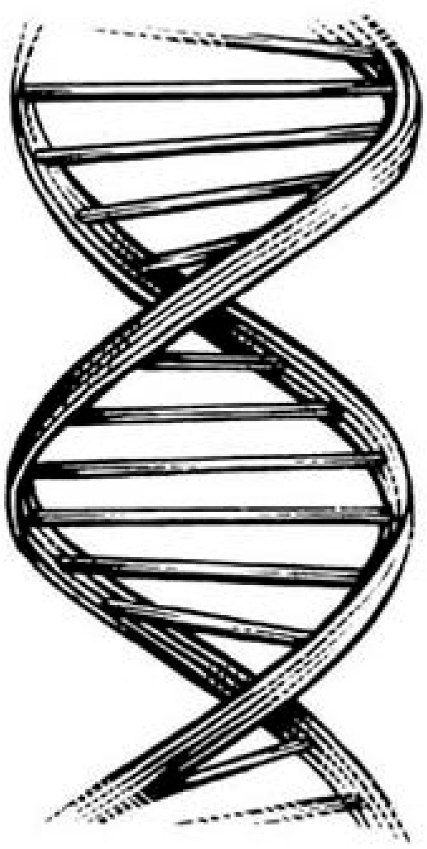
Design. Implement. Build in dependability.

Conduct appraisals. Identify opportunities.

Release? Rework? Improve processes.

Standards
Best Practices
Professional Communities


12
10
8
6
4
2
Time
Try
How
Next
What
1
1



Development Assurance

Costs of
meeting requirements

Costs of *not*
meeting requirements

- Prevention
- Appraisal

- Internal failures
- External failures

COST OF QUALITY

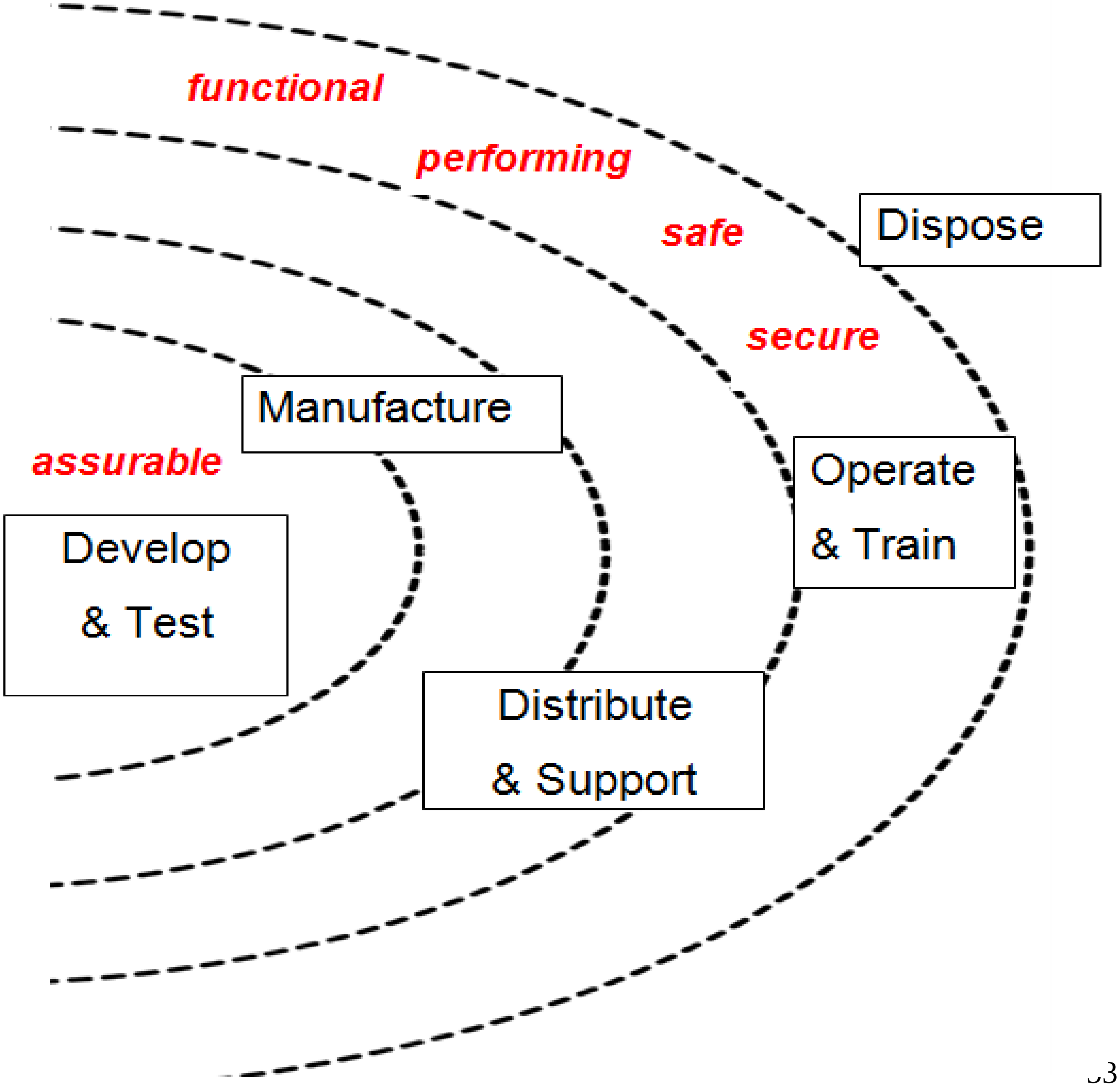
- **Prevention**
  - ✓ **Planning**
  - ✓ **Training**
  - ✓ **Tools**
- **Appraisal**
  - ✓ **Inspections**
  - ✓ **Audits**
  - ✓ **Tests**

COST OF QUALITY

- Internal failures
  - Scrap
  - Rework
- External failures
  - Warranty
  - Liability
  - Loss of reputation

COST OF QUALITY

Likelihood	negligible	consequence		catastrophic
reasonable	2	3	4	4
				4
	1		3	
infrequent	1	1		3



functional

performing

safe

Dispose

secure

Manufacture

assurable

Operate & Train

Develop & Test

Distribute & Support

Systems-of-Systems Assurance

Taz Daughtrey

hdaughtrey@csiac.org

434 841 5444

Cyber Security and Information Systems
Information Analysis Center

Cyber Security & Information Systems
Information Analysis Center

"Everybody has won
and all must have prizes."