Design Principles for Survivable System Architecture

1st IEEE Systems Conference
April 10, 2007

Matthew Richards
Research Assistant, MIT Engineering Systems Division

Adam Ross, Ph.D.
Postdoctoral Associate, MIT Engineering Systems Division

Daniel Hastings, Ph.D.
Professor, MIT Department of Aeronautics and Astronautics and Engineering Systems Division

Donna Rhodes, Ph.D.
Senior Lecturer, MIT Engineering Systems Division
Director, SEARI

Agenda

- Motivation
- Survivability Framework
- 12 Design Principles for Enhancing Survivability
- Passive vs. Active Survivability
- Conclusion

Motivation

- Despite increased geographic distribution, information technology has increased interdependence of engineering systems
- Interdependencies magnify risk from local disturbances that rapidly propagate within and among systems
- Risks exacerbated by emergence of new sources of disturbances
  - Physical: terrorism
  - Electronic: cyber-attacks
- Shortcomings associated with reductionist conventional approaches to survivability engineering
  - Limited to physical domain
  - Presuppose operating environments and hazards
  - Ineffective for managing emergent, context-dependent system properties

Research needed on how survivability should inform design decisions of system architectures

Practical Architectures for Survivable Systems and Networks by Peter G. Neumann (2000)

- U.S. Army Research Laboratory report assesses state of architecting for survivability
  - Scope: distributed systems, systems of systems
  - Identifies several inadequacies with current paradigm

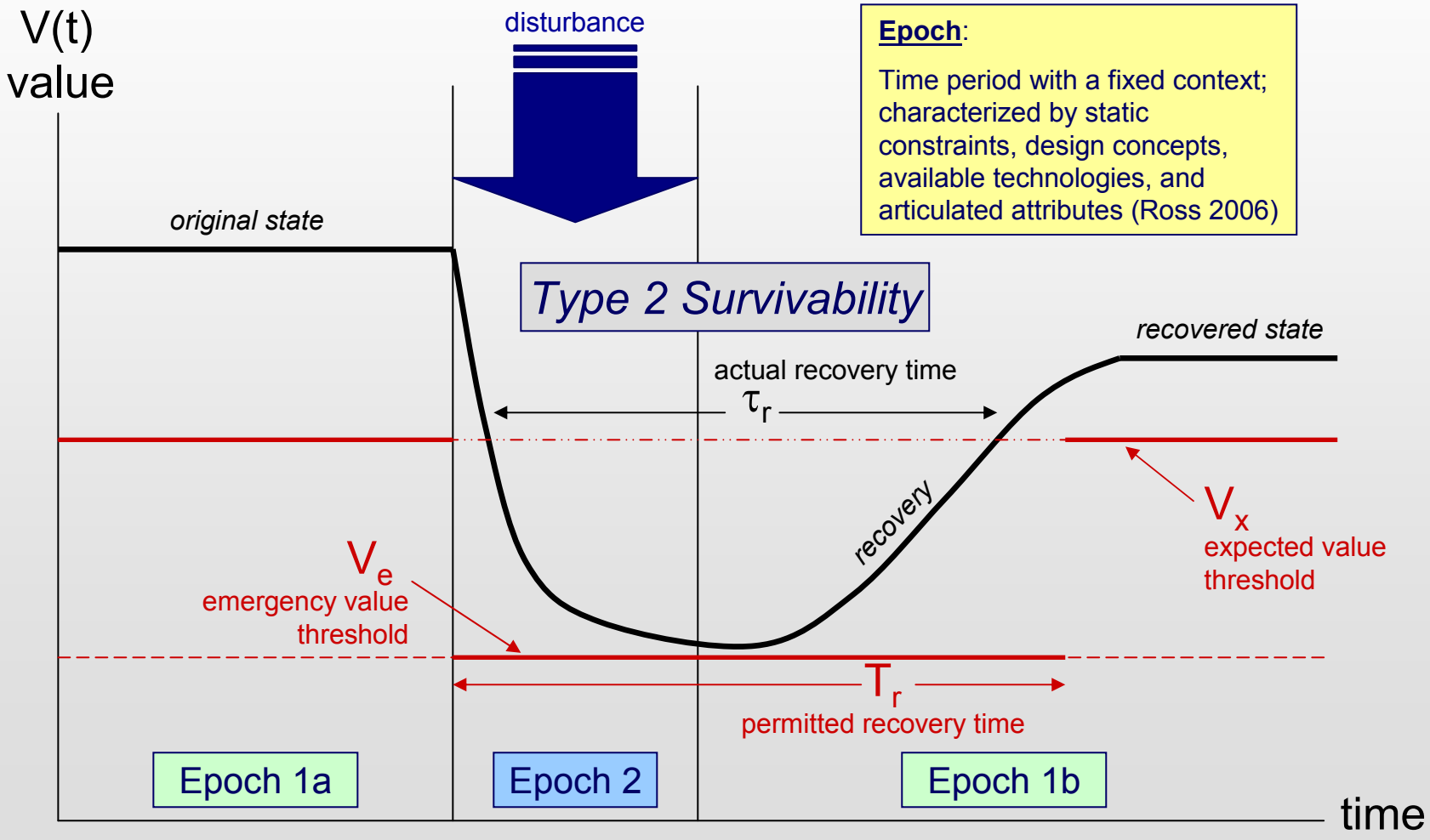
> "Systems and networks with critical survivability requirements are extremely difficult to specify, develop, procure, operate, and maintain."
>
> "The currently existing evaluation criteria frameworks are not yet comprehensively suitable for evaluating highly survivable systems."
>
> "…there is almost no experience in evaluating systems having a collection of independent criteria that might contribute to survivability, and the interactions among different criteria subsets are almost unexplored outside of the context of this report."

- Identifies several challenges requiring future work, including…
  - Generic mission models that can be readily tailored to specific systems to evaluate the adequacy of survivability requirements
  - Families of systems and network topologies that are inherently robust to catastrophic failures

Enumeration of design principles for survivability would be a first step towards development of a generic survivability framework

Definition of Survivability

Ability of a system to minimize the impact of a finite disturbance on value delivery, achieved through either (1) the reduction of the likelihood or magnitude of a disturbance or (2) the satisfaction of a minimally acceptable level of value delivery during and after a finite disturbance

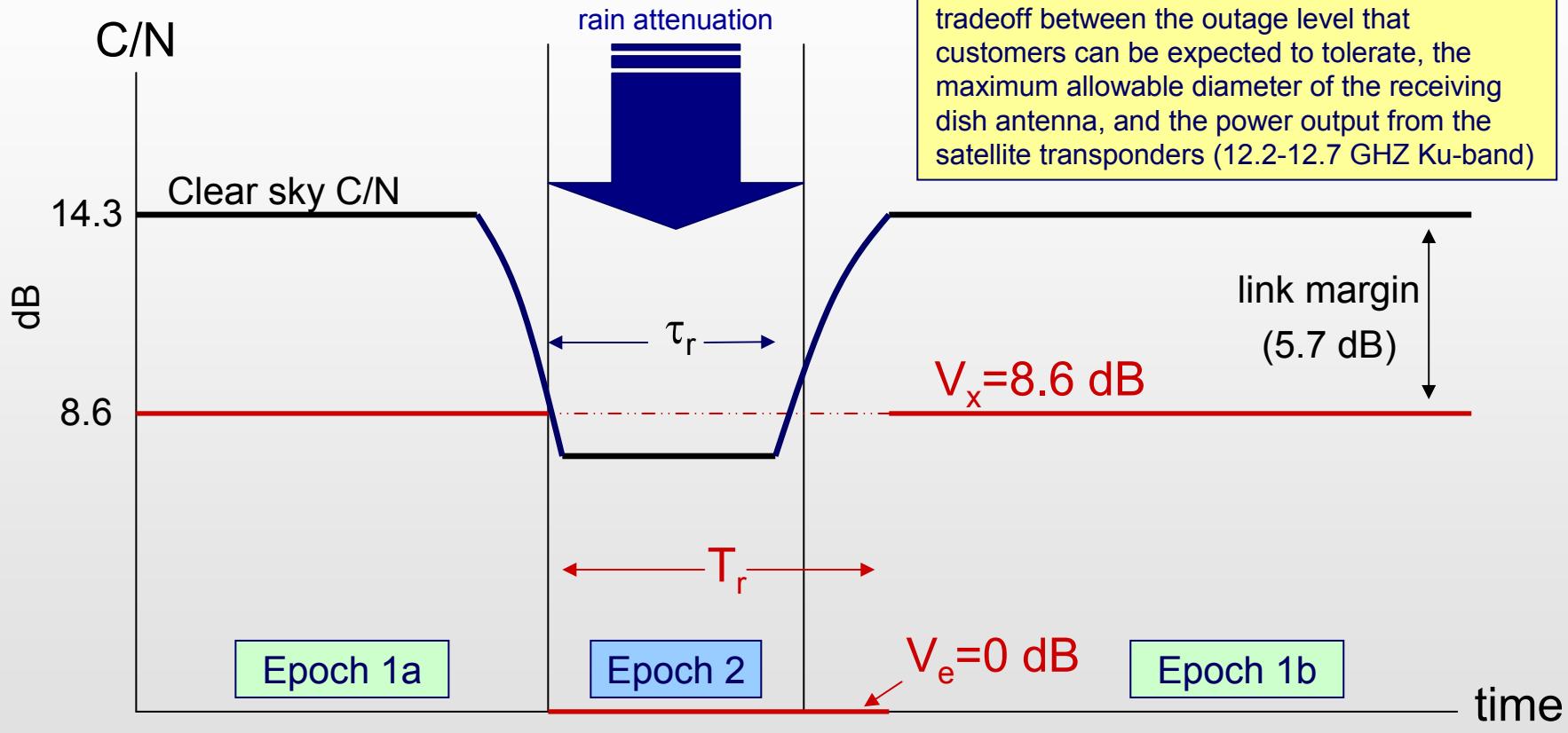


Epoch:

Time period with a fixed context; characterized by static constraints, design concepts, available technologies, and articulated attributes (Ross 2006)

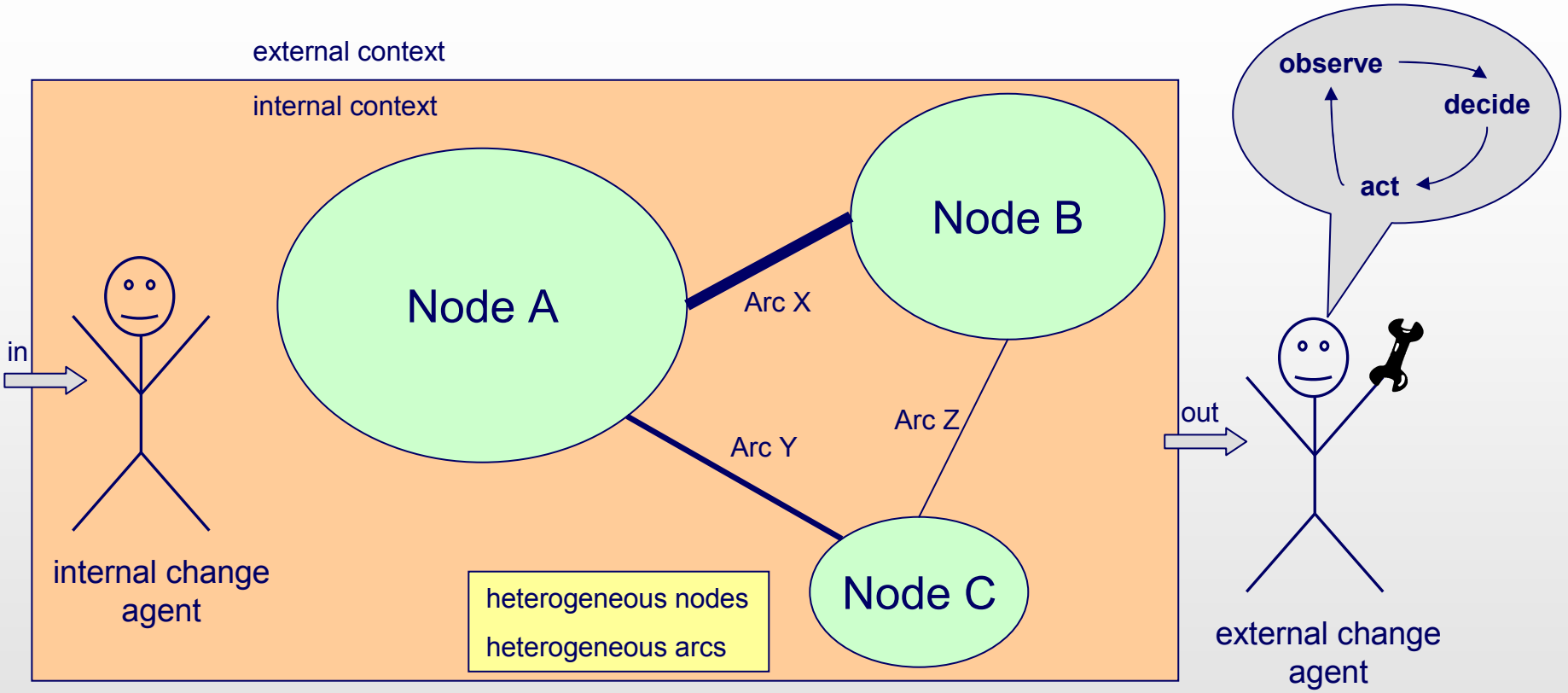
Type II : Direct Broadcast Satellite TV

Carrier-to-noise ratio (C/N) margin is a design tradeoff between the outage level that customers can be expected to tolerate, the maximum allowable diameter of the receiving dish antenna, and the power output from the satellite transponders (12.2-12.7 GHZ Ku-band)



Type II survivability is achieved here because $\tau_r < T_r$
In the case of DIRECTV, τ_r must be <0.3% of the time (about 25 hours each year)

Survivability Framework



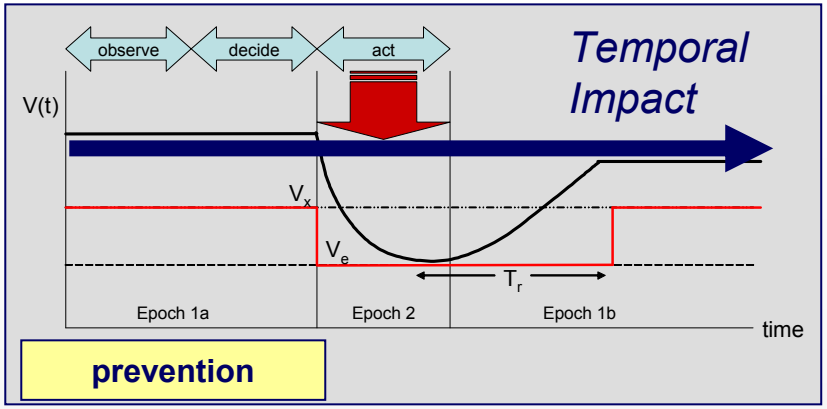
Framework consists of the minimum set of elements to describe system

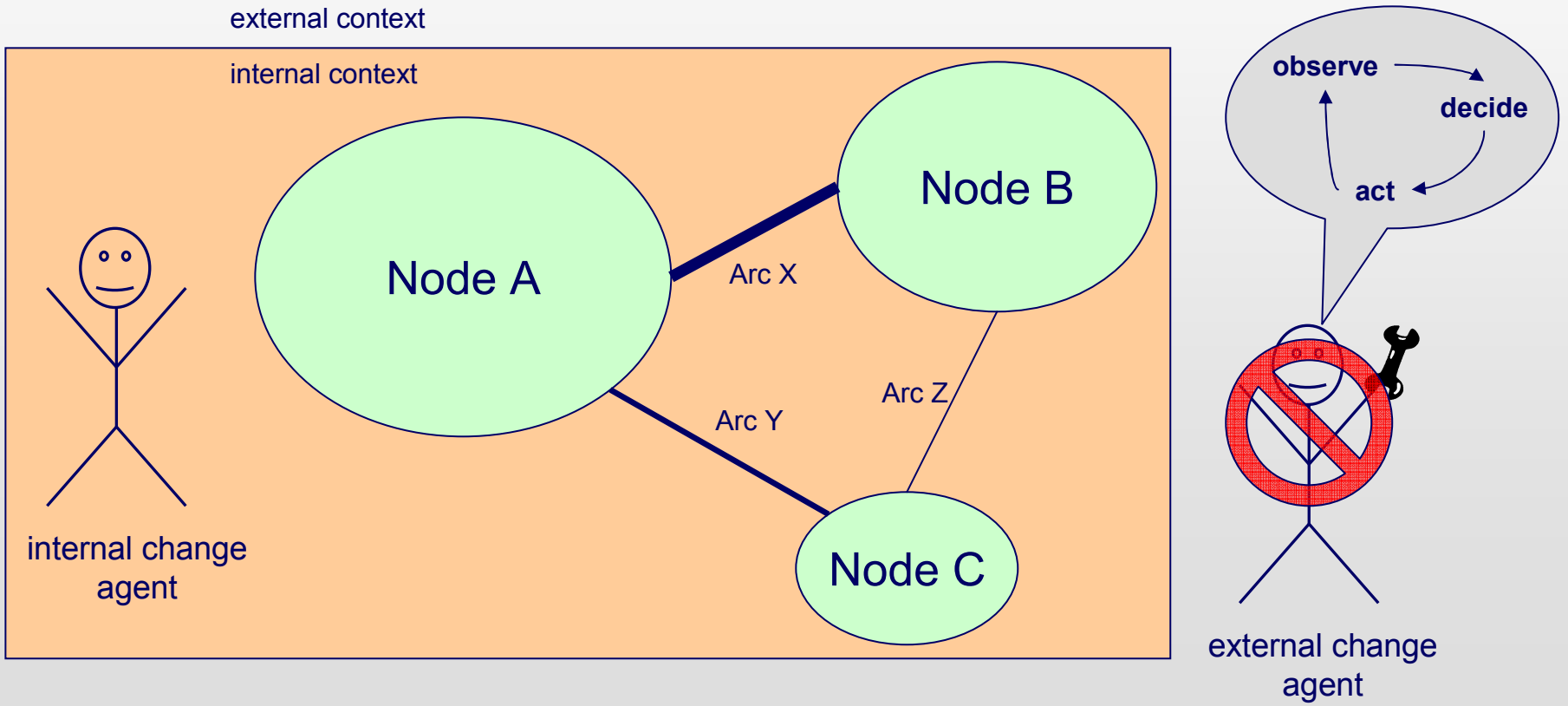
- Changes in elements will provide insights into survivability
- Used to enumerate 12 design principles for survivability
  - 6 identified for Type 1 survivability *(reduction in susceptibility)*
  - 6 identified for Type 2 survivability *(reduction in vulnerability)*

Prevention (1.1)

Definition: *suppression of a future or potential future disturbance*

examples: aircraft suppression of enemy air defense (SEAD), 2nd Persian Gulf War

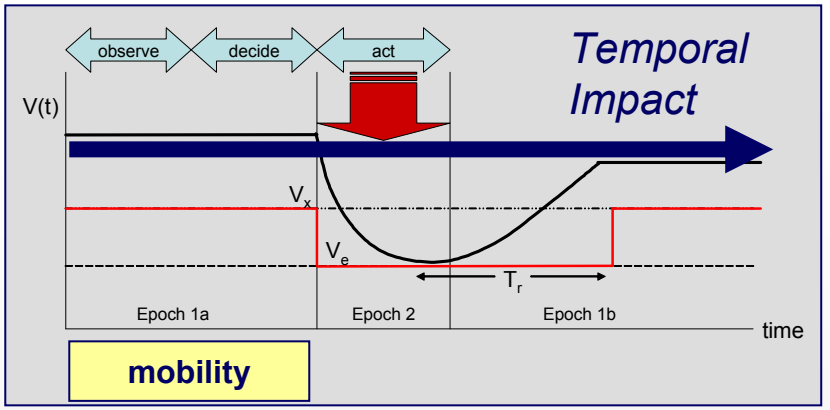


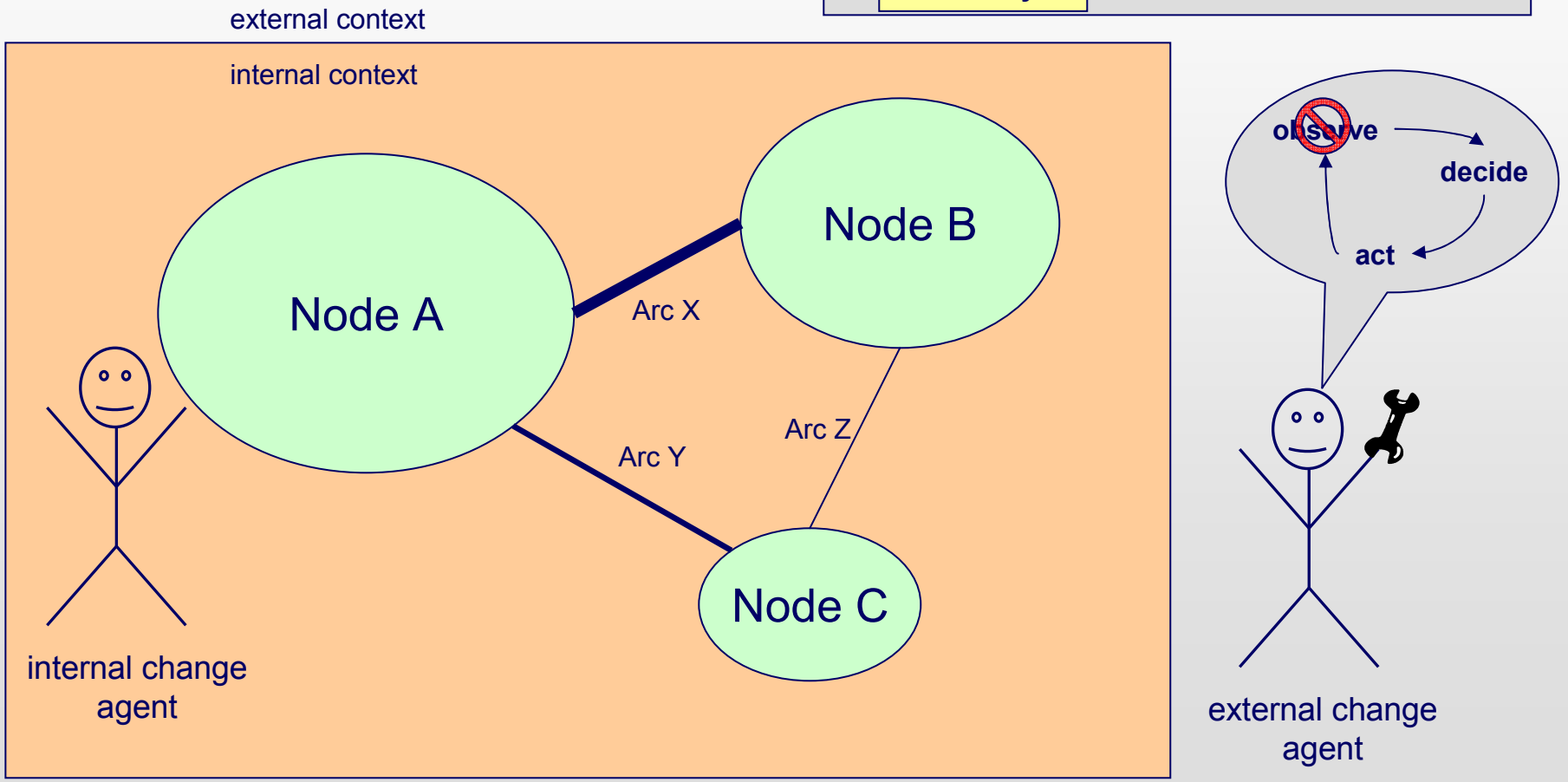


Mobility (1.2)

Definition: *ability to relocate to avoid detection*

examples: Navy TACAMO E-6 strategic communications aircraft, Scud launcher vehicles

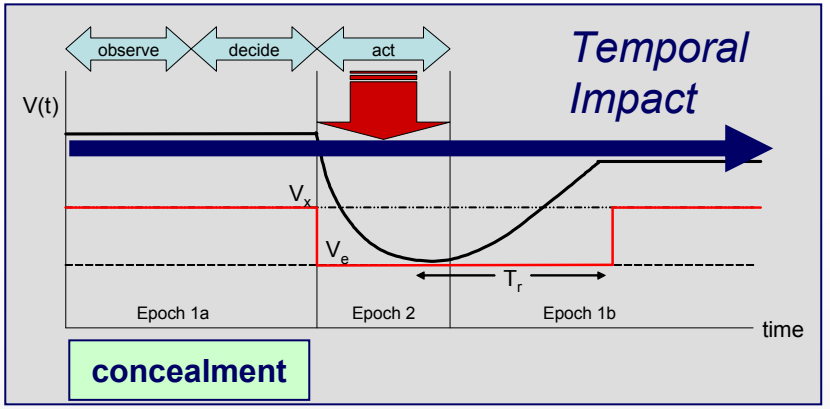




Concealment (1.3)

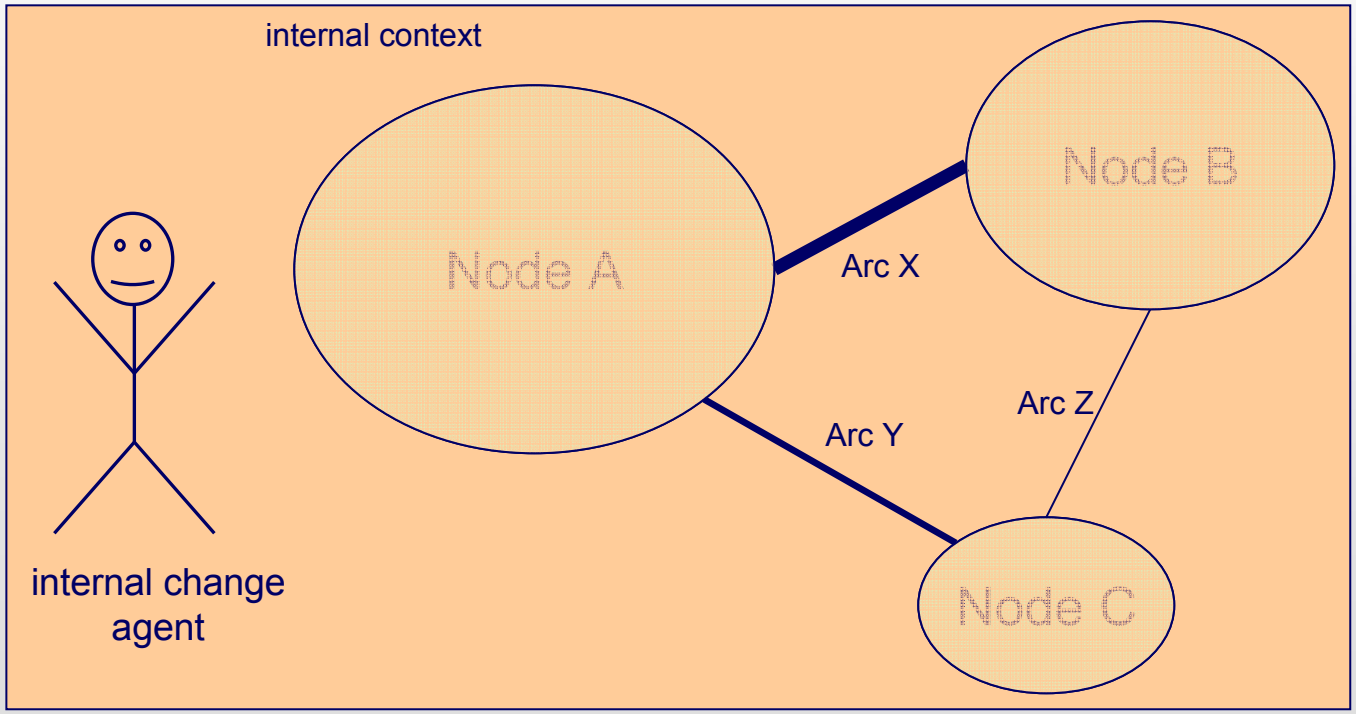
Definition: *act of reducing the visibility of a system from an external change agent*

examples: radar signature reduction on B-2 Spirit and F-117 Nighthawk

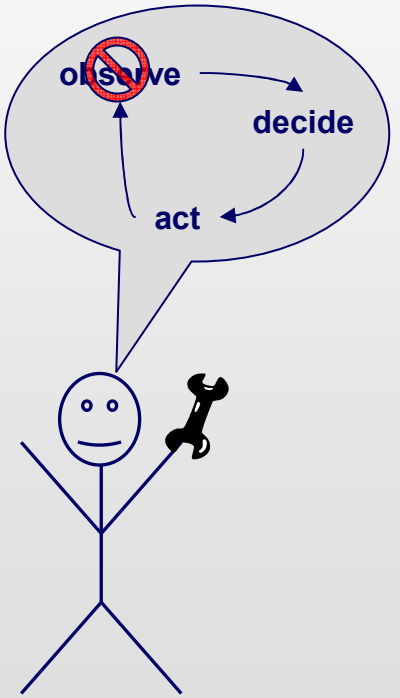


external context

internal context



internal change agent

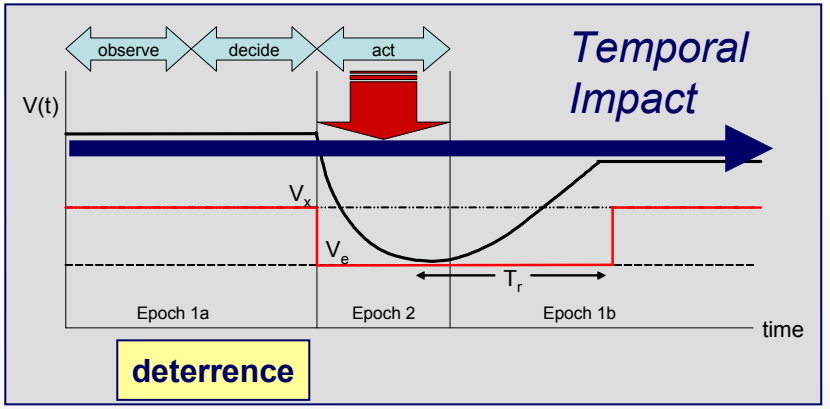


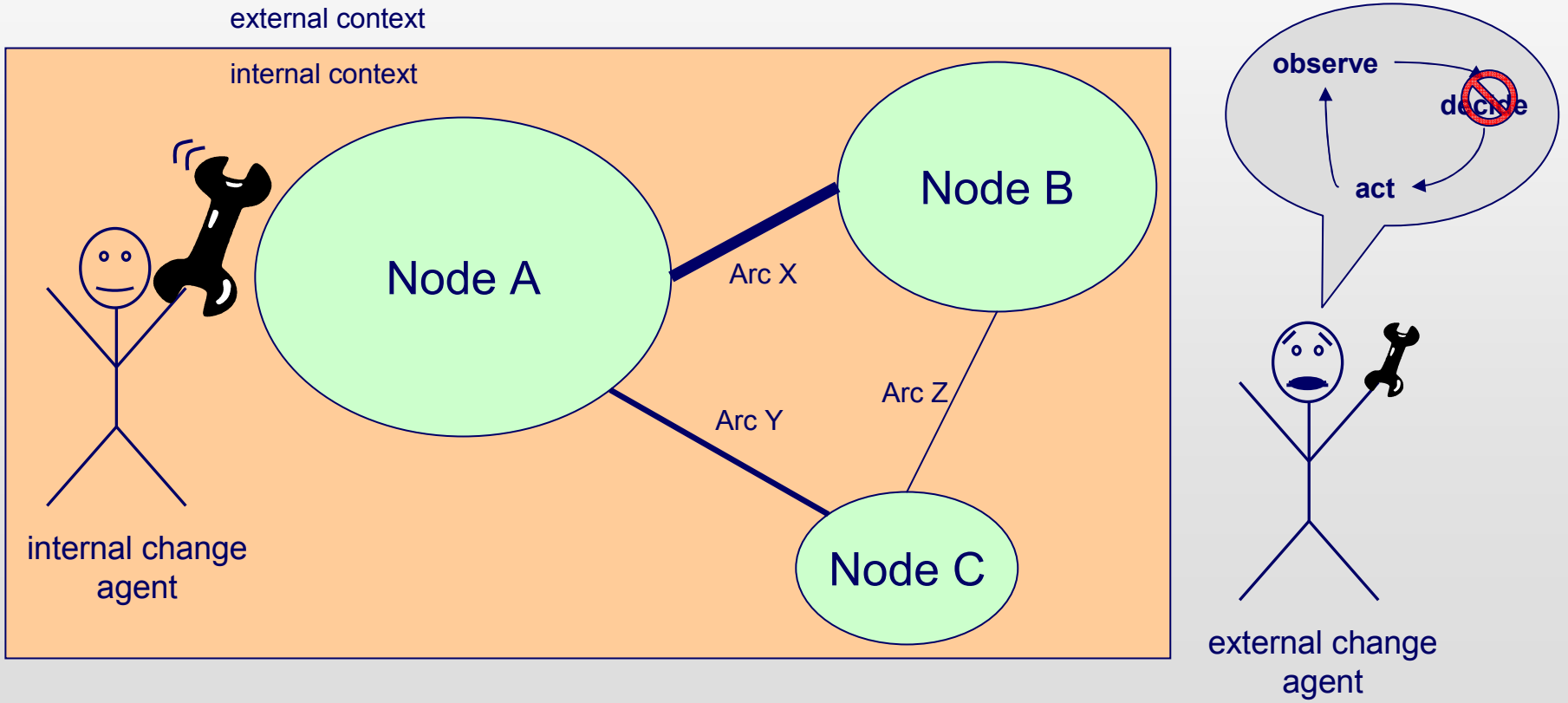
external change agent

Deterrence (1.4)

Definition: *dissuasion of a rational external change agent from committing a disturbance; increases perceived costs above perceived benefits of attack*

example: Mutually Assured Destruction

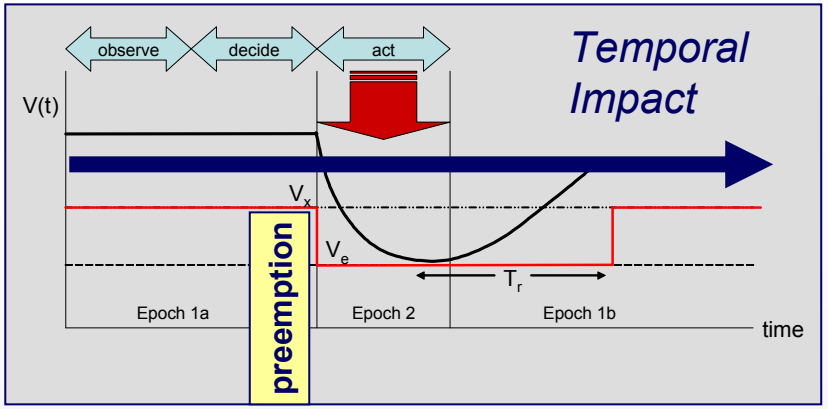


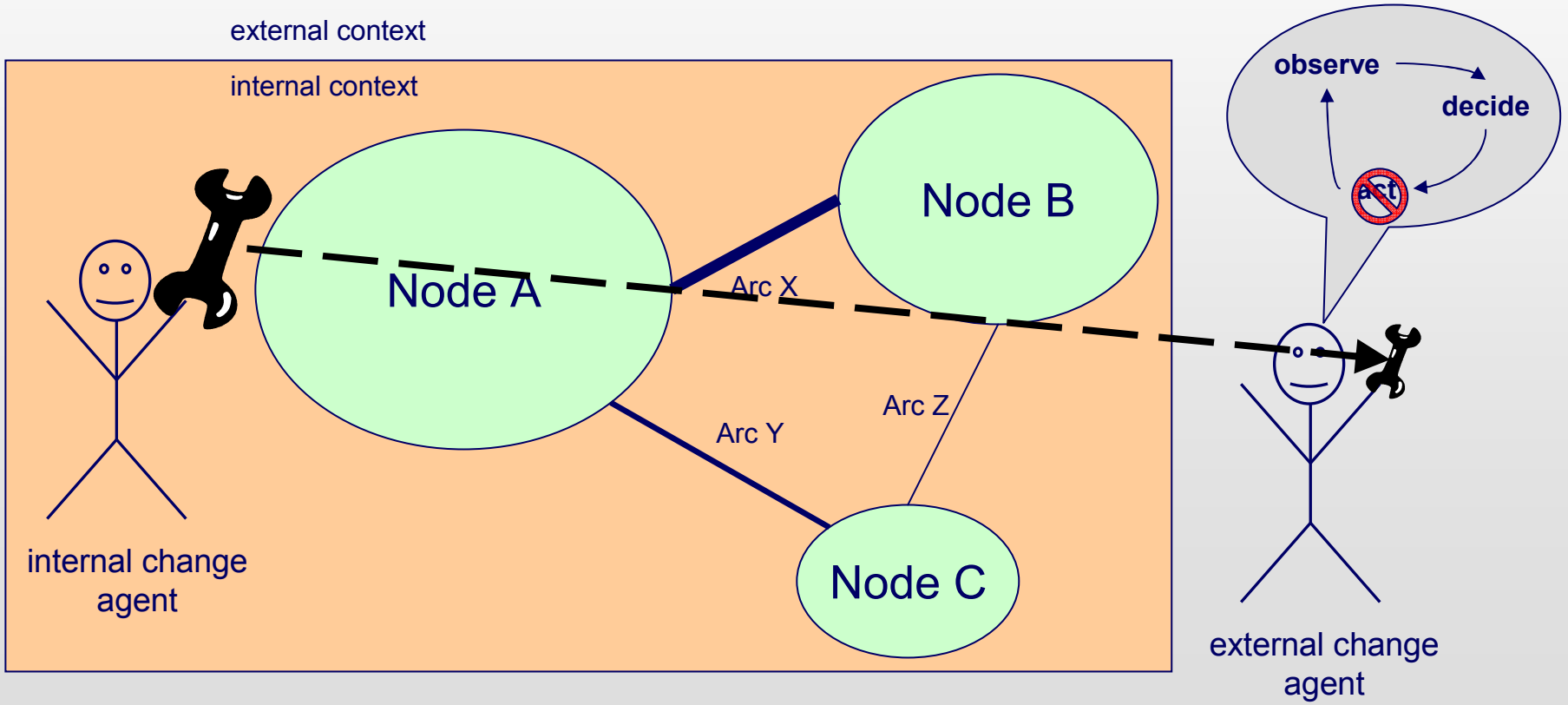


Preemption (1.5)

Definition: *suppression of an imminent disturbance*

example: missile defense, Israeli attack on Egyptian forces in 1967 Six Day War

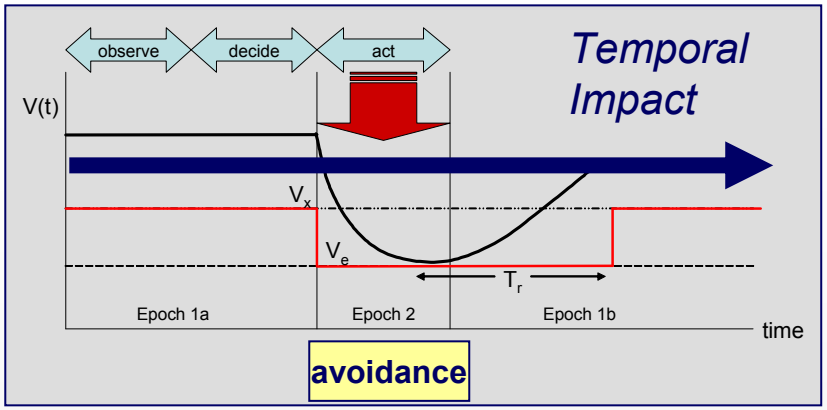




Avoidance (1.6)

Definition: *ability to maneuver away from a disturbance*

examples: aircraft missile evasion, precision landing on Mars Science Laboratory (MSL)



external context

internal context

Node A

Node B

Node C

Arc X

Arc Y

Arc Z

observe

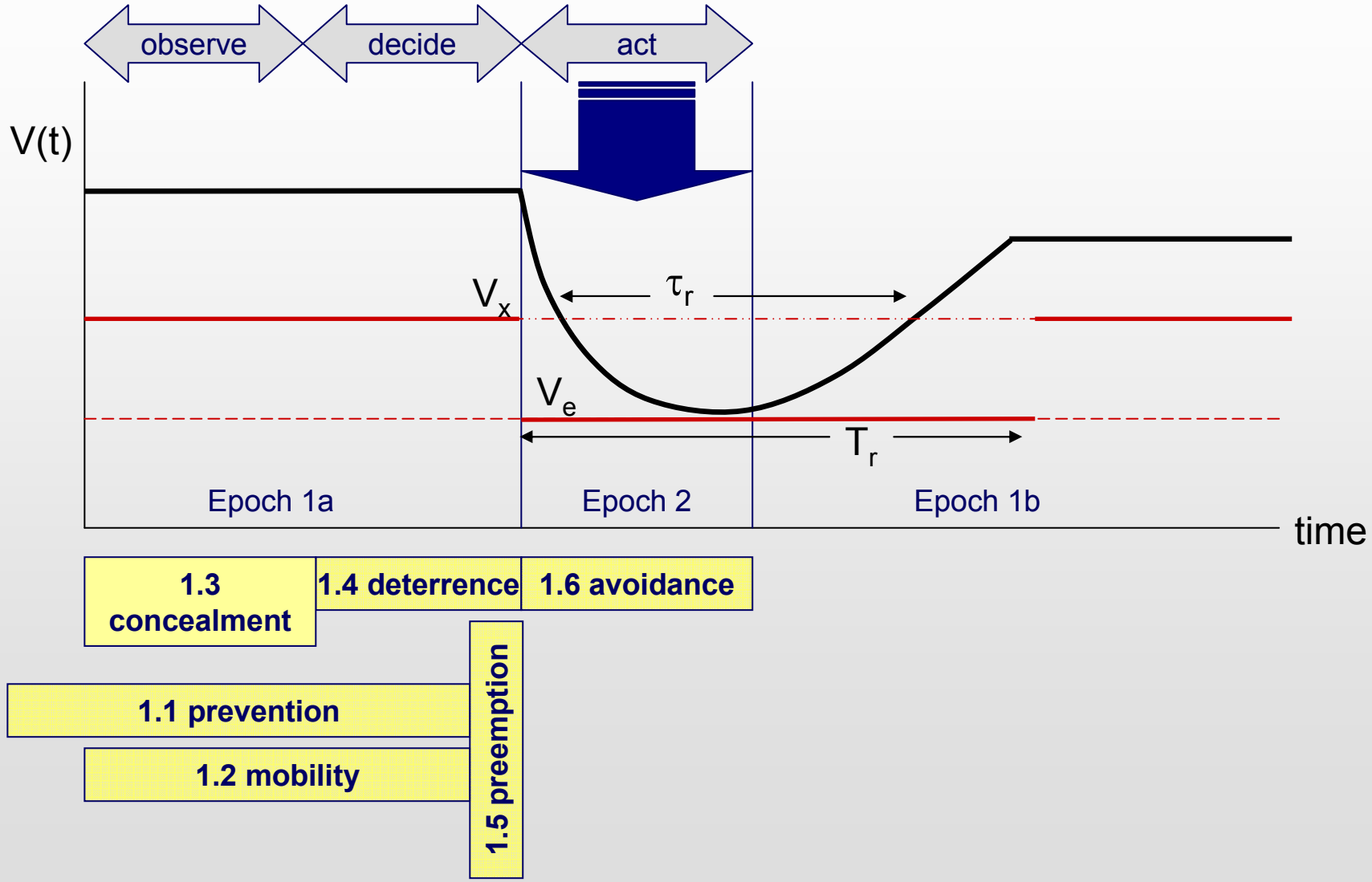
decide

act

internal change agent

external change agent

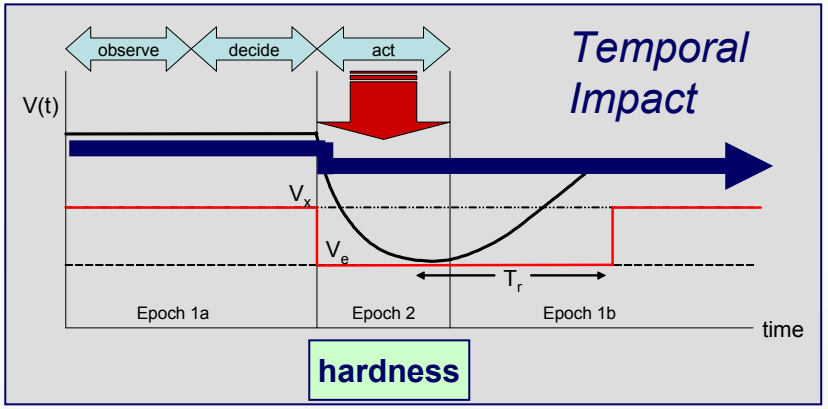
Type I Survivability Principles at Work

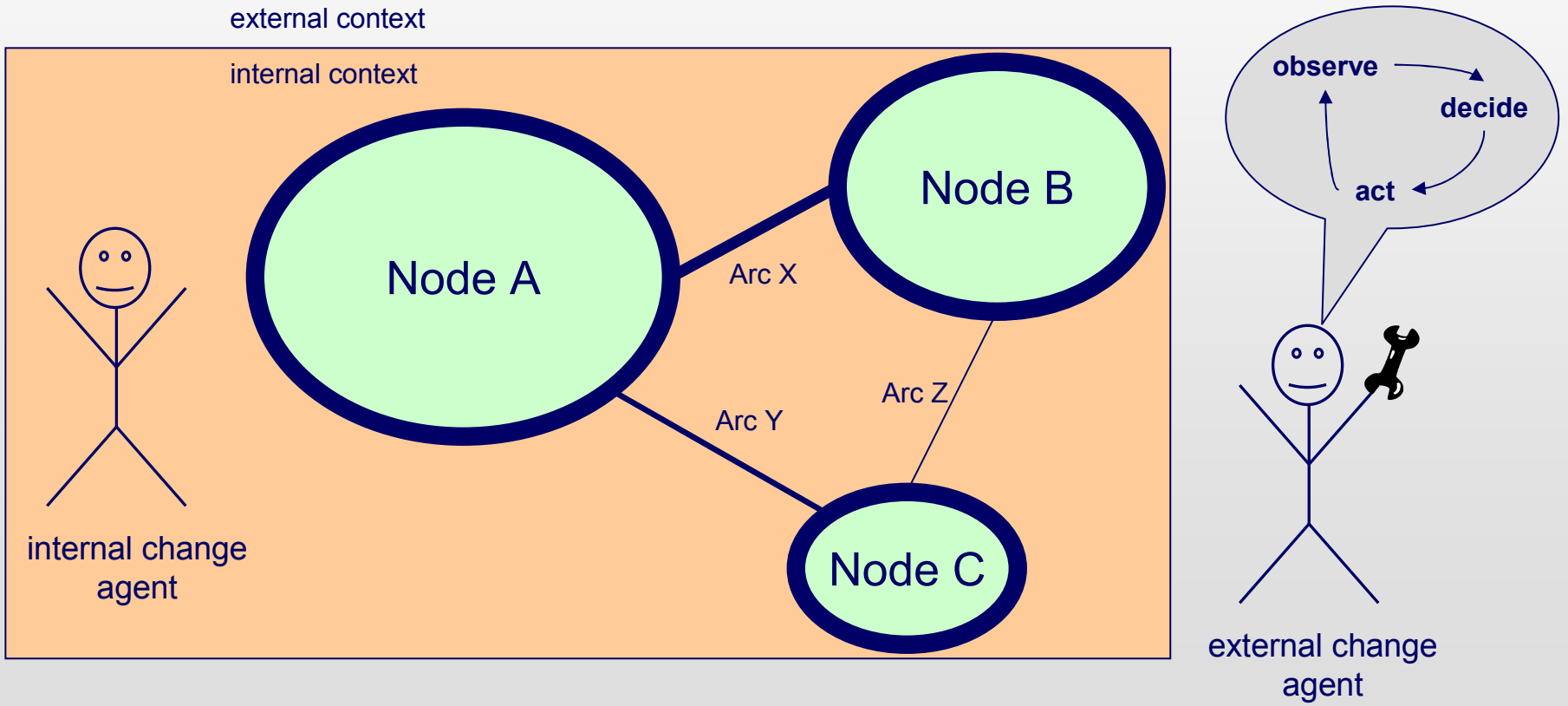


Hardness (2.1)

Definition: *resistance of a system to deformation*

examples: error correcting codes, Milstar satellite radiation hardening

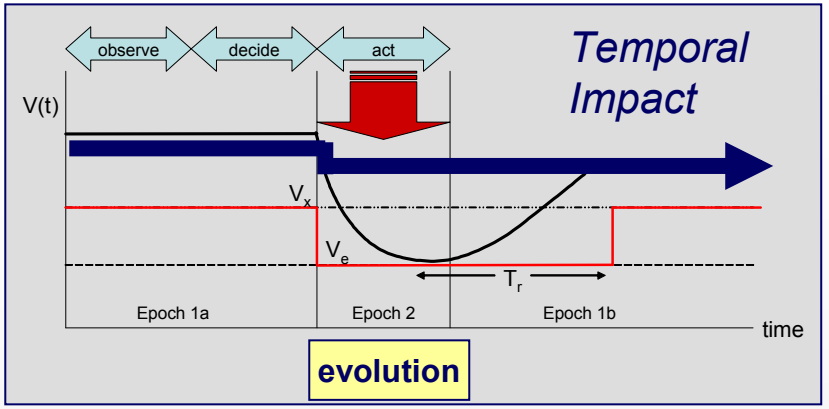


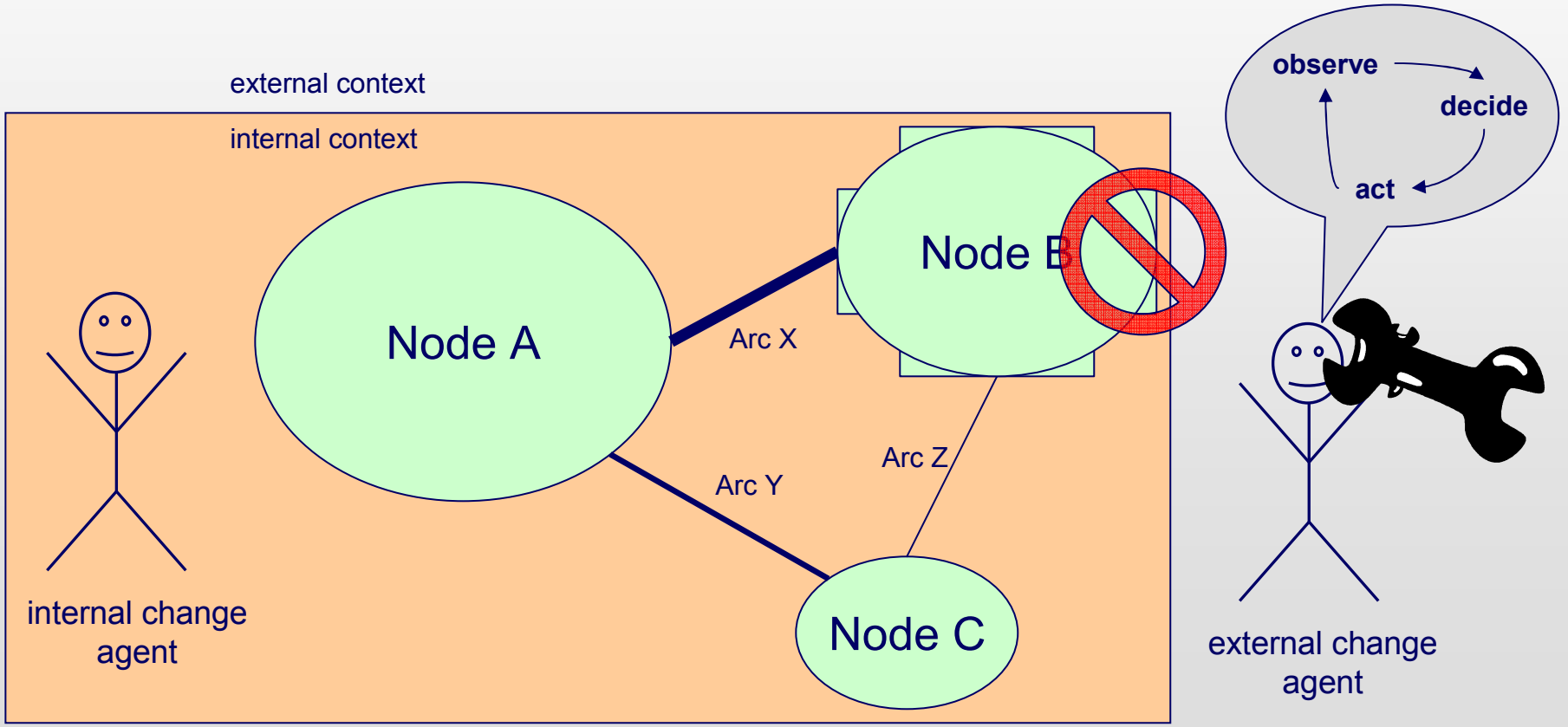


Evolution (2.2)

Definition: *alteration of system elements to reduce disturbance effectiveness (engineered mismatch)*

example: post-deployment armor-plating of Humvees

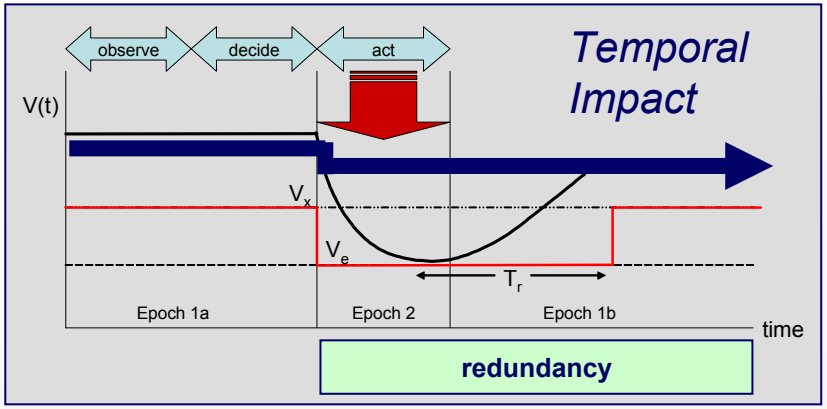


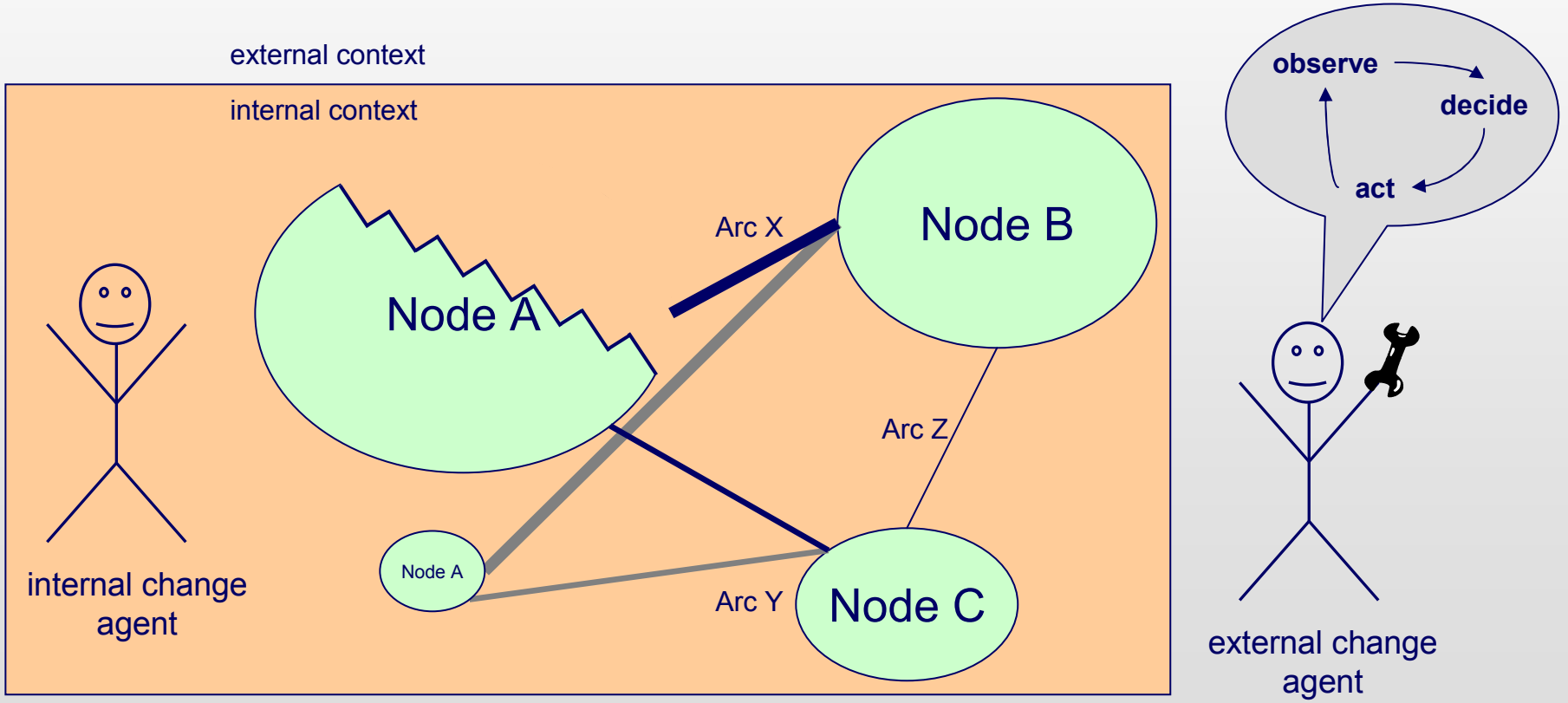


Redundancy (2.3)

Definition: *duplication of critical system components to increase reliability*

examples: back-up GEO communications satellites, Space Shuttle avionics system of 5 identical general-purpose computers

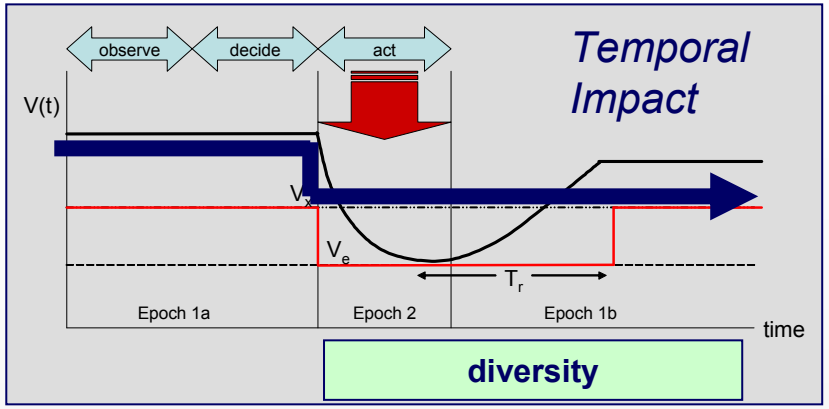


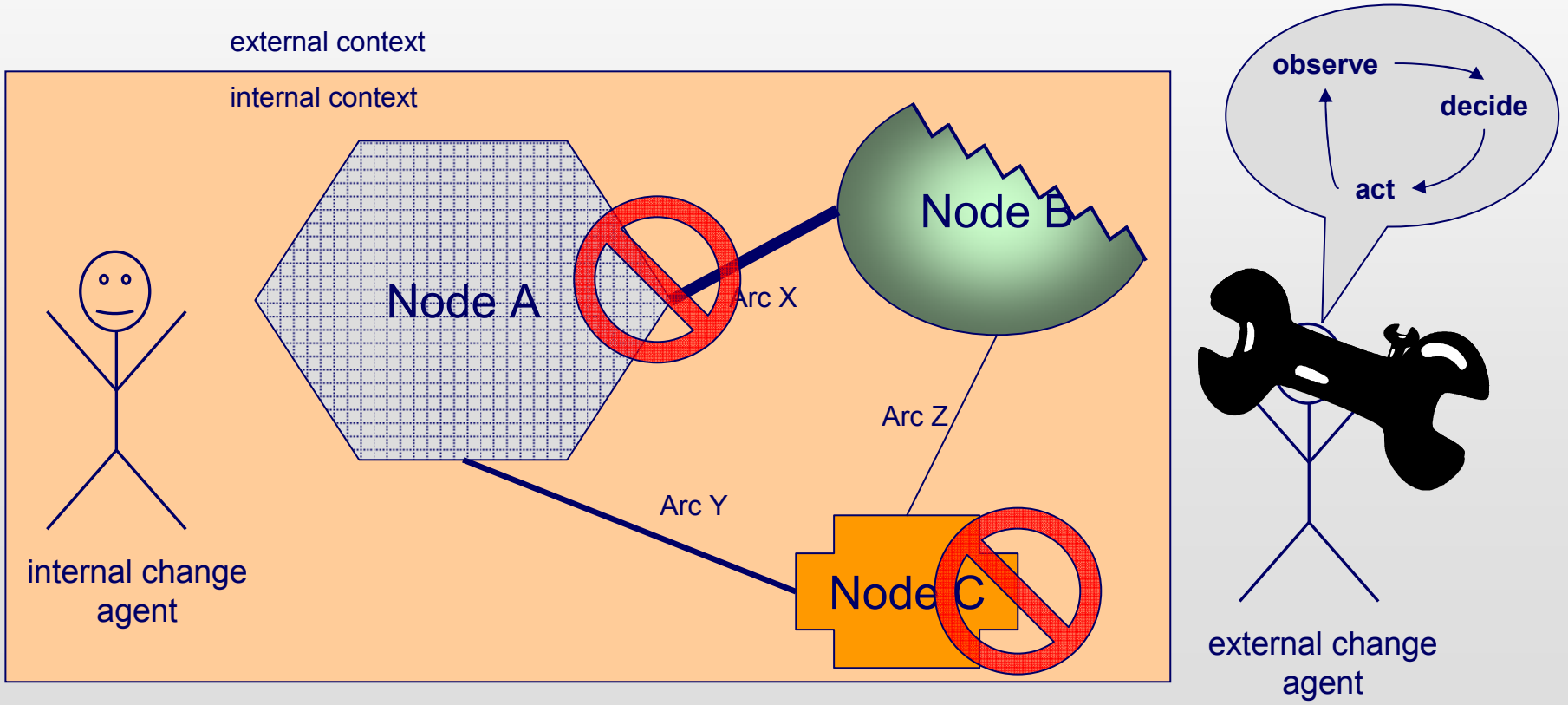


Diversity (2.4)

Definition: *variation in system elements (characteristic or spatial) to decrease effectiveness of homogeneous disturbances*

example: heterogeneous operating systems decreases effectiveness of malware, separation of computers on spacecraft

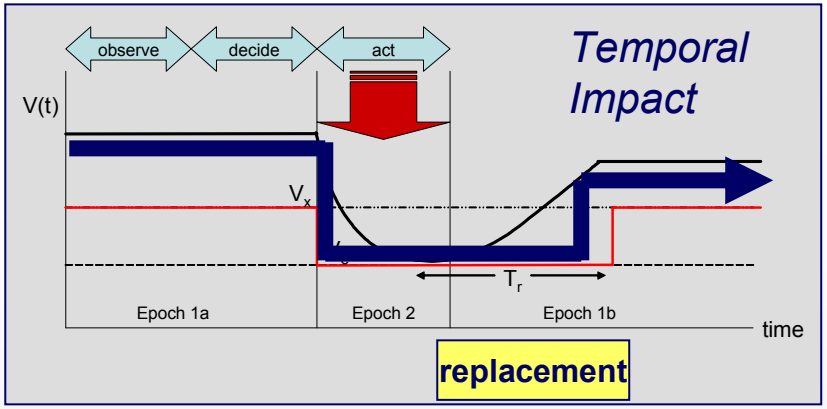


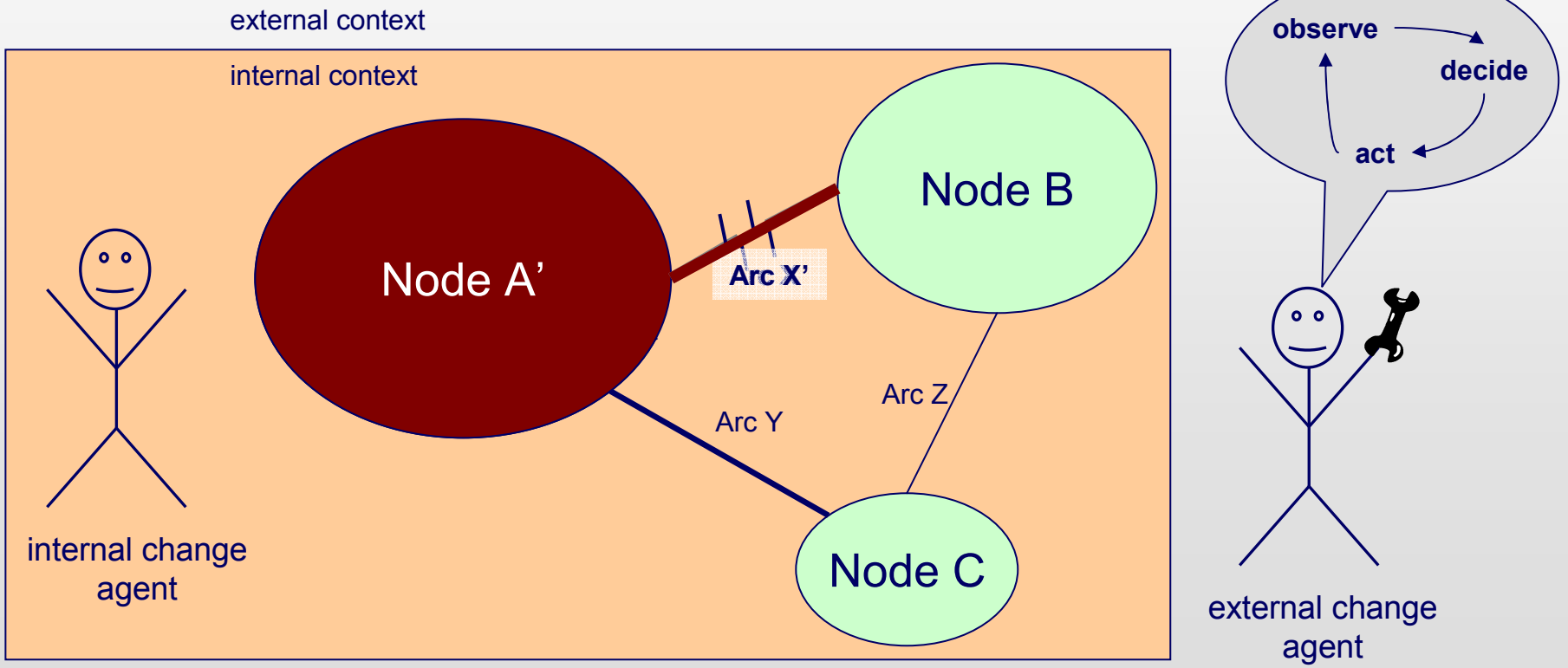


Replacement (2.5)

Definition: *substitution of system elements to improve value delivery*

example: launch of XM-3 and XM-4 to replace XM-1 and XM-2 due to solar panel fogging that reduced Boeing 702 lifetimes from 15 to 6 years

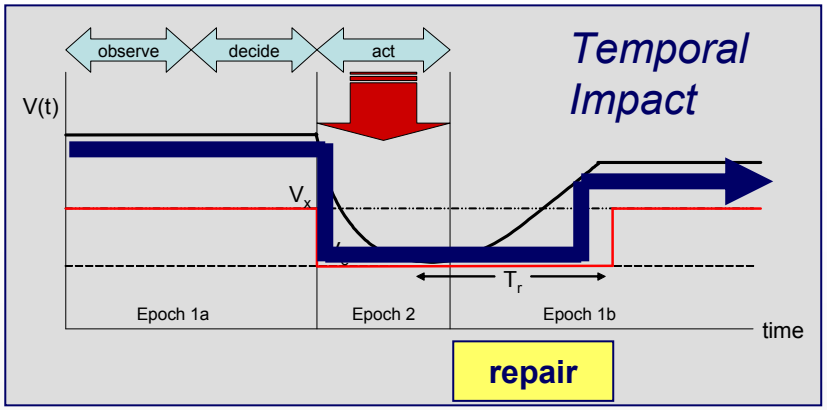




Repair (2.6)

Definition: *restoration of system to improved state of value delivery*

example: Hubble servicing missions



external context

internal context

Node A

Node B

Node C

Arc X

Arc Y

Arc Z

internal change agent

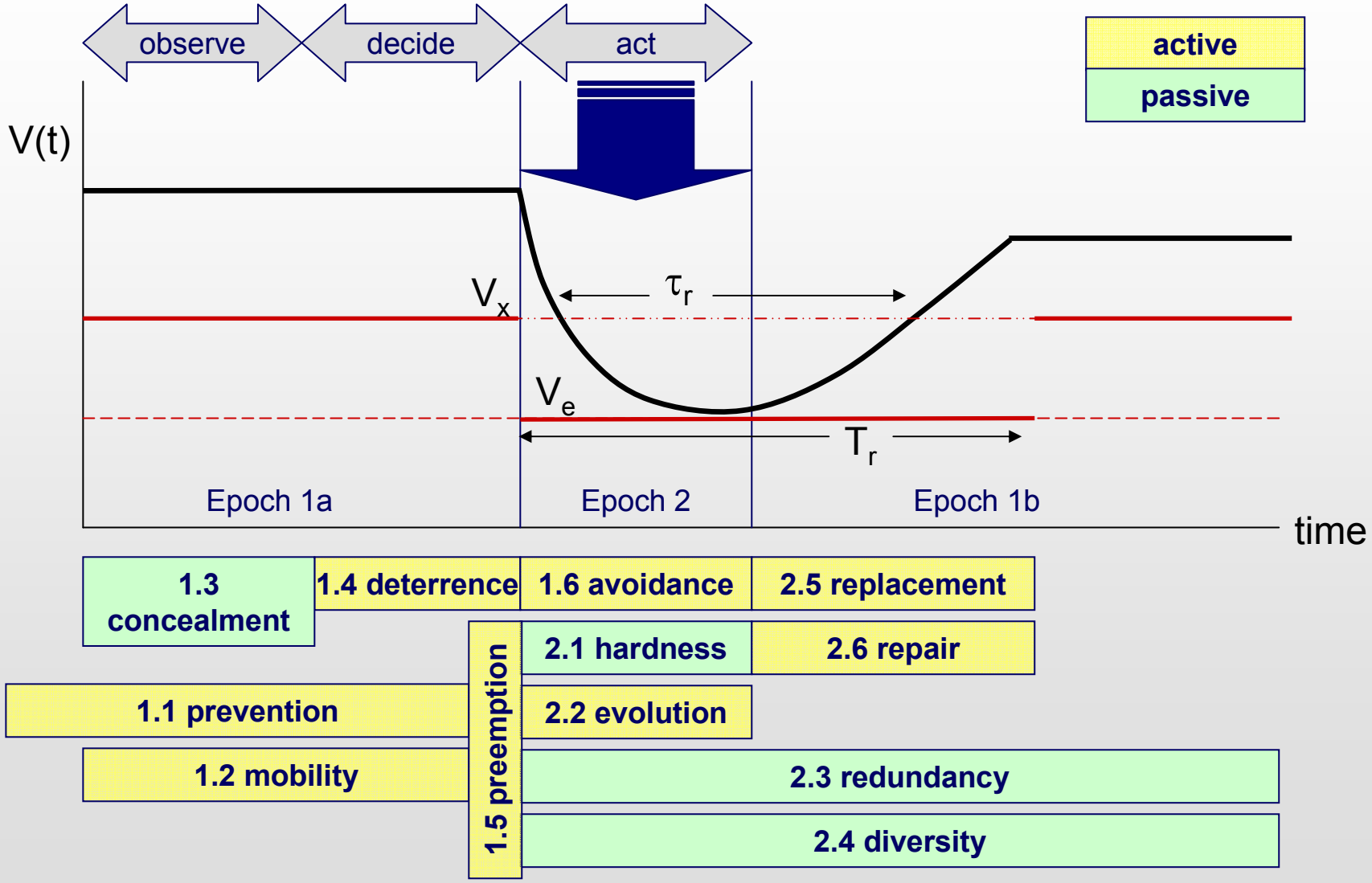
observe

decide

act

external change agent

Survivability Principles at Work



Passive vs. Active Survivability

	Passive Survivability	Active Survivability
Philosophy	Survivability is something that a system *has*	Survivability is something that a system *does*
Characteristics	proactive, resistant, robust	reactive, flexible, adaptive
Design Principles	concealment, hardness, redundancy, diversity	prevention, mobility, deterrence, preemption, avoidance, evolution, replacement, repair
Forecasting	Presupposes knowledge of disturbance environment	Acknowledges uncertainty in projection of future disturbances
Architecture	Closed (static)	Open (dynamic)
Design Focus	Defensive barriers at system-level to resist disturbances	Architectural agility to avoid, deter, and recover from disturbances
Failures	Causal chain (often linear)	Tight couplings, functional resonance (nonlinear)
Relevant Disciplines	Component reliability, safety engineering, risk analysis, domain-specific technologies	Real options, organizational theory, process design, domain-specific technologies

Conclusion

- Definition, framework, and enumeration of passive and active survivability design principles is ***only a first step***
  - Helpful for understanding a larger set of survivability techniques
- Enumeration is not intended as a systems engineering checklist
  - ***Intended to provide designers with a portfolio of options*** from which to consider a larger tradespace of survivable designs
- Successful ***designs must balance investments in survivability with performance and cost***
  - e.g., incorporate subset of the twelve principles with varying weights
- Future work
  - Development of ***quantitative metrics*** for each design principle
  - Incorporation of survivability as an attribute in an existing satellite ***tradespace***