

STOCHASTIC CONSIDERATIONS IN SYSTEMS RESILIENCE ENGINEERING

JOSE EMMANUEL RAMIREZ-MARQUEZ
ASSOCIATE PROFESSOR
STEVENS INSTITUTE OF TECHNOLOGY

OCTOBER 12, 2011
RUTGERS - THE STATE UNIVERSITY OF
NEW JERSEY

DHS RESEARCH NEEDS

INFRASTRUCTURE PROTECTION:

**ANALYTICALLY QUANTIFY DISRUPTIONS ACROSS CRITICAL
INFRASTRUCTURE SECTORS**

**UNDERSTANDING OF FAILURE MECHANISMS AND PROTECTION
MEASURES FOR THE MOST VITAL COMPONENTS**

CYBER SECURITY:

**IMPROVED CAPABILITY TO MODEL THE EFFECTS OF CYBER
ATTACKS AND UNDERSTANDING OF INTERNET TOPOLOGY
INFORMATION SYSTEM THREAT DETECTION MODELS AND
MITIGATION TECHNOLOGIES**

CENTER FOR SECURE AND RESILIENT MARITIME COMMERCE:

**MARITIME INFRASTRUCTURE RECOVERY - RECOMMENDS
PROCEDURES AND STANDARDS FOR THE RECOVERY OF THE
MARITIME INFRASTRUCTURE FOLLOWING ATTACK OR SIMILAR
DISRUPTION.**

KEY RESEARCH QUESTIONS

WHAT IS NETWORK RESILIENCE? (MANY DEFINITIONS)

-THE WORD RESILIENCE HAS ITS ORIGINS IN THE LATIN WORD “RESILIERE”, WHICH CAN BE UNDERSTOOD AS TO “BOUNCE BACK”.

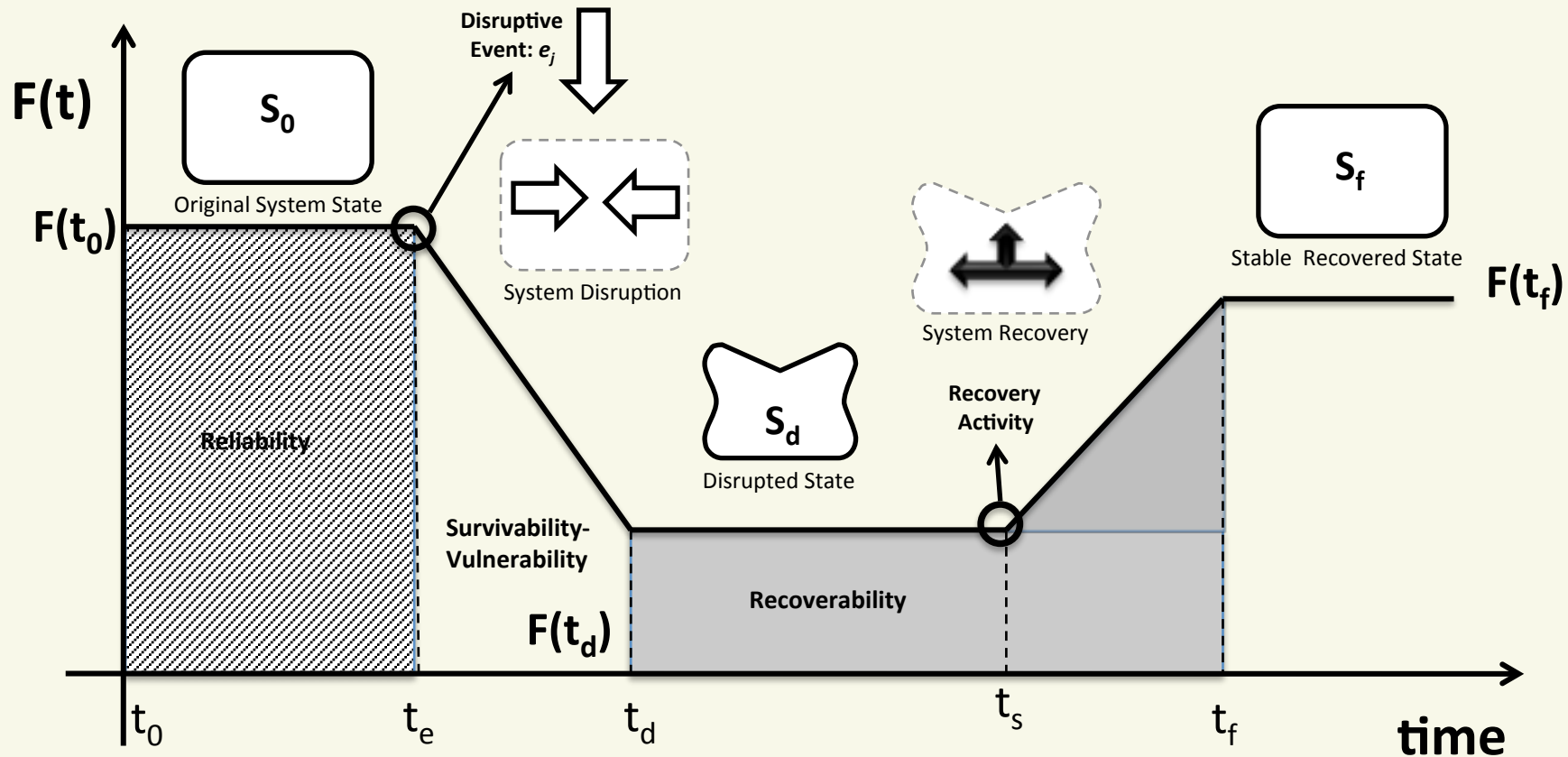
WHAT DOES NETWORK VULNERABILITY DESCRIBE?

-FROM THE LATIN VULNERARE, WHICH CAN BE DEFINED AS OPEN TO ATTACK OR DAMAGE

WHAT IS THE RELATIONSHIP AMONG NETWORK RESILIENCE, VULNERABILITY AND “PROTECTION/ RESTORATION” APPROACHES?

HOW ARE THESE CONCEPTS “QUANTIFIED” IN A NETWORK CONTEXT

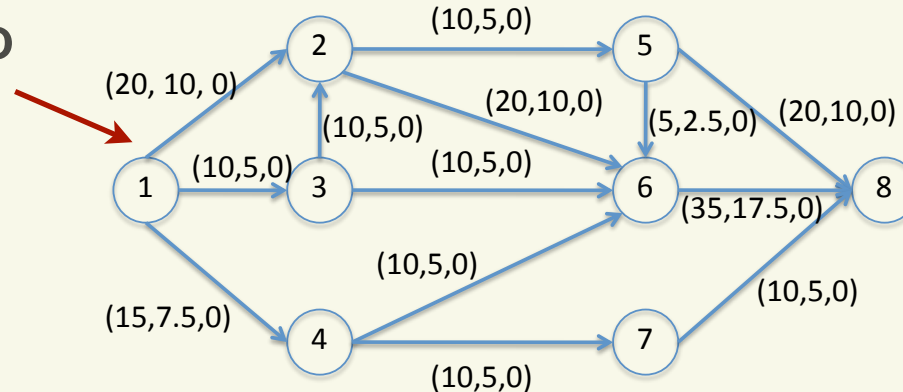
NETWORK RESILIENCE REPRESENTATION



CLEAR DISTINCTION AMONG CONCEPTS OF:
RELIABILITY, SURVIVABILITY, VULNERABILITY AND
RESTORATION/SUPPORTABILITY

MULTI-STATE RELIABILITY ANALYSIS

CAPACITATED NETWORK ELEMENTS



NETWORK IS USED TO DESCRIBE SOME DELIVERY FUNCTION

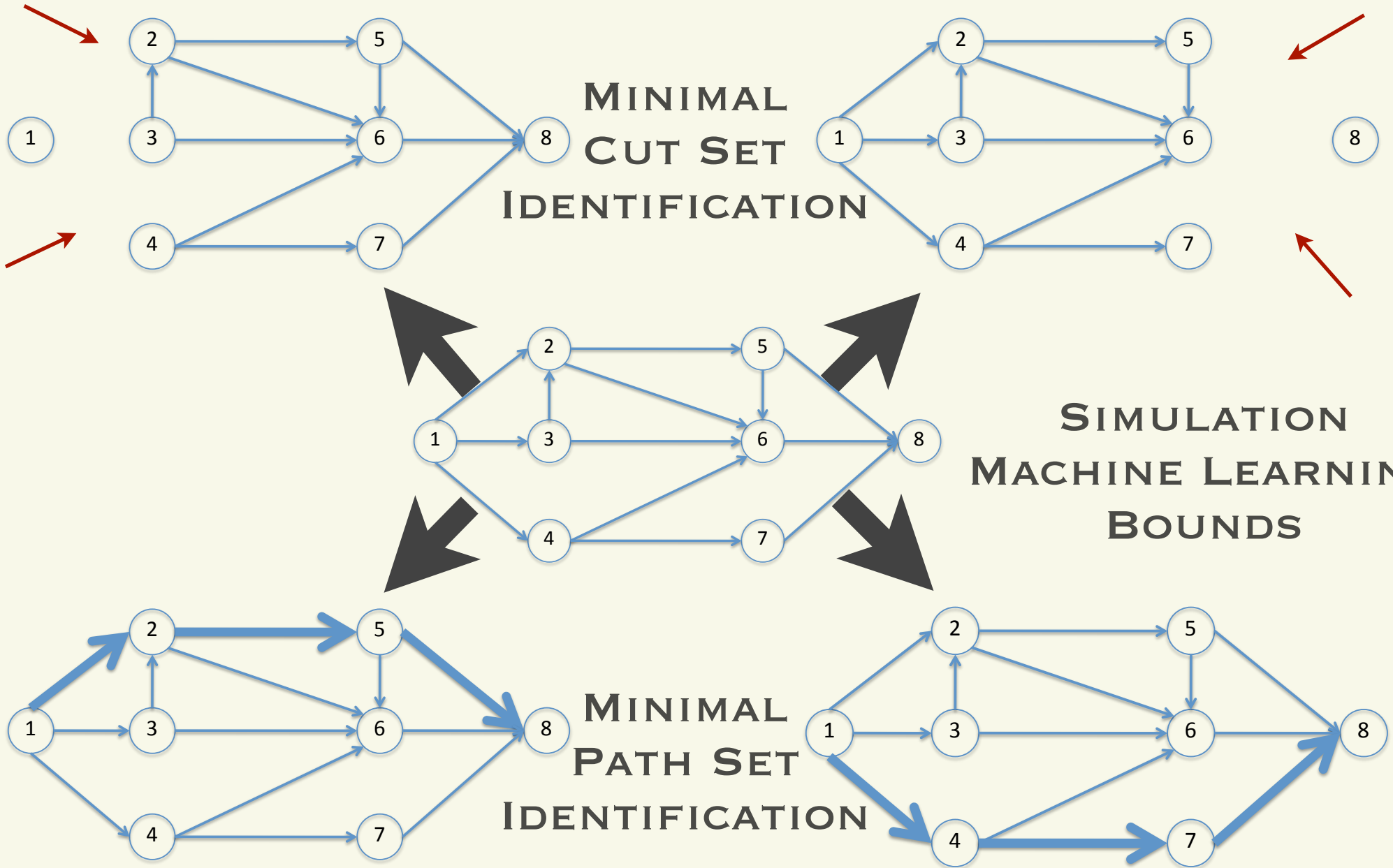
FLOW RELIABILITY - PROBABILITY A REQUIRED FLOW CAN BE “TRANSPORTED” BETWEEN TWO NETWORK NODES:

$$P(\varphi(x) \geq d)$$

DELAY RELIABILITY - PROBABILITY TWO NODES CAN BE TRANSVERSED IN A GIVEN TIME:

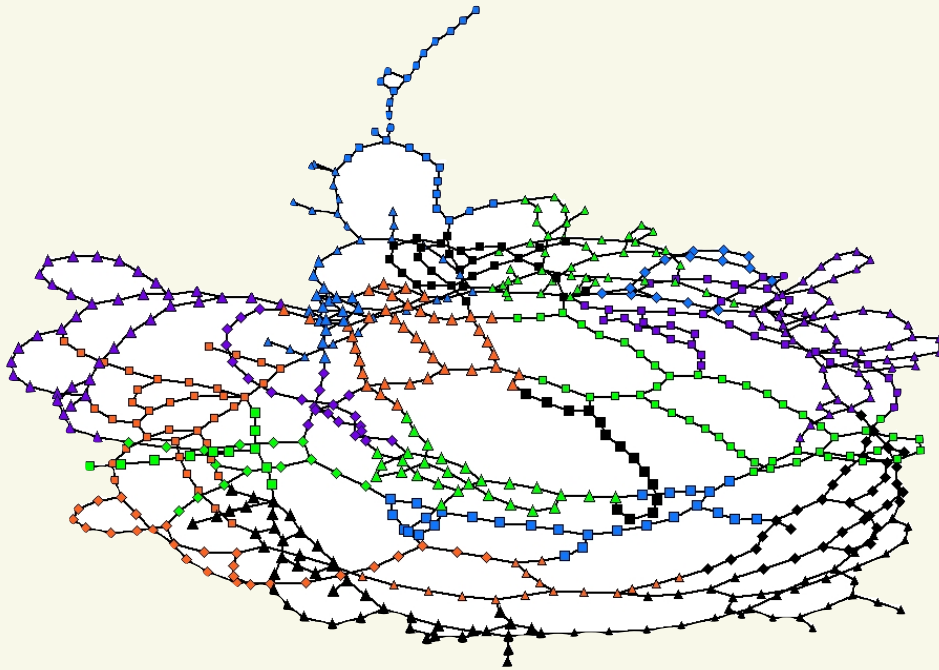
$$P(\varphi(x) \leq t)$$

RELIABILITY ANALYSIS



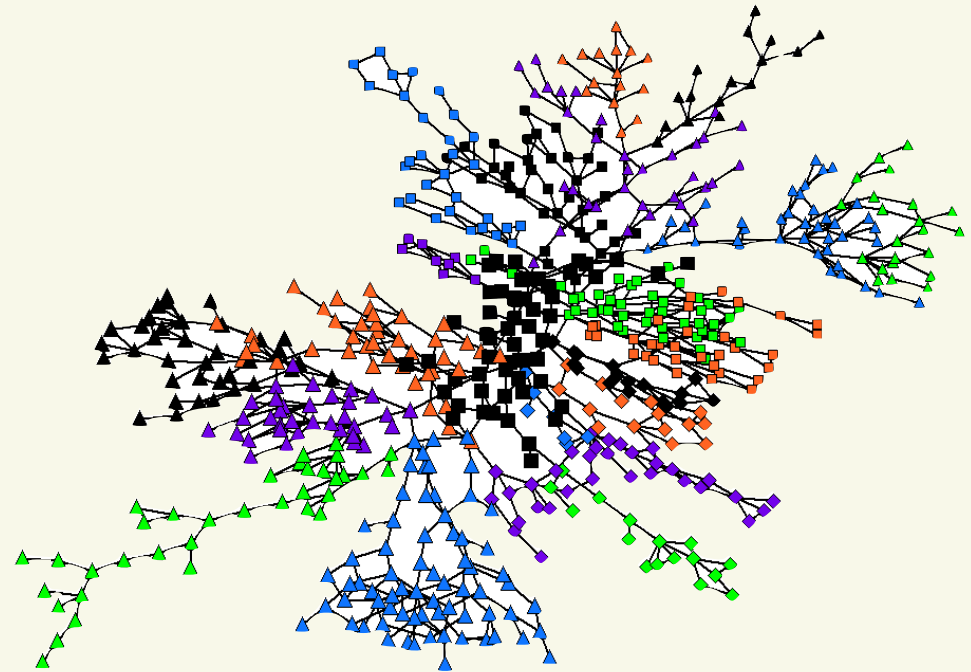
CURRENT NETWORK ANALYSIS?

TRANSIT NETWORK CITY OF
PIACENZA



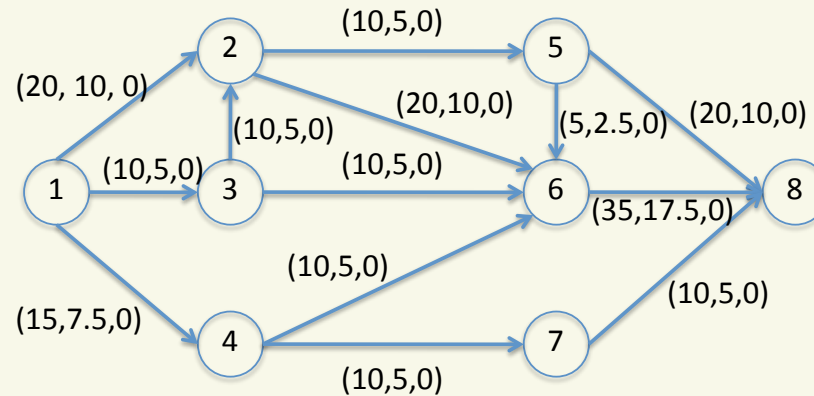
RELIABILITY: PROBABILITY
MAXIMUM DELAY TIME
BETWEEN EVERY NODE PAIR
IS LESS THAN t

POWER NETWORK FOR
VENEZUELA (SIMPLIFIED)



RELIABILITY: PROBABILITY
POWER SUPPLY SATISFIES
END NODES REQUIREMENTS

LIMITATIONS OF RELIABILITY ANALYSIS

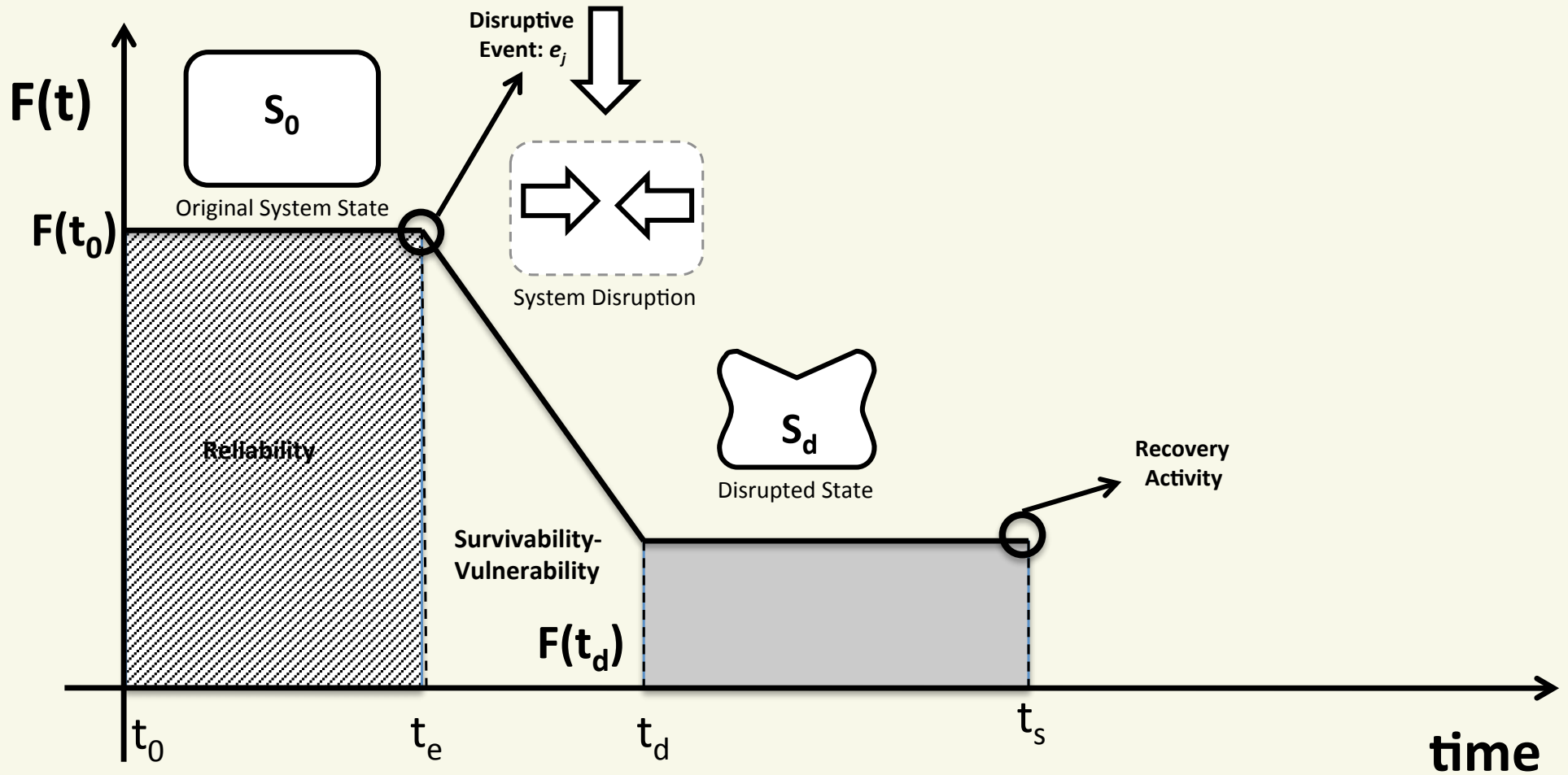


ONLY DESCRIBES COMPLETE FAILURE EVENTS (CUT SETS HARD TO OBTAIN FOR LARGE NETWORKS)

REDUNDANCY TECHNIQUES ARE USED TO MAKE THE NETWORK “SURVIVABLE”

COMPONENT FAILURES ARE INTRINSIC TO THE NETWORK AND NOT DUE TO HARMFUL EVENTS (GENERALLY)

NETWORK VULNERABILITY



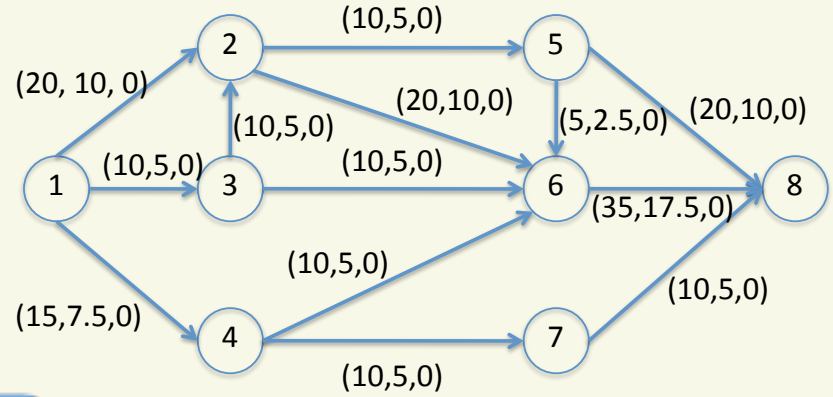
NETWORK TOPOLOGY

SERVICE/DELIVERY FUNCTION (COHERENT)

DISRUPTIVE EVENT ($F(t_0) > F(t_d)$)

VULNERABILITY & RESILIENCE

$F(T)$



$F(T_0)$

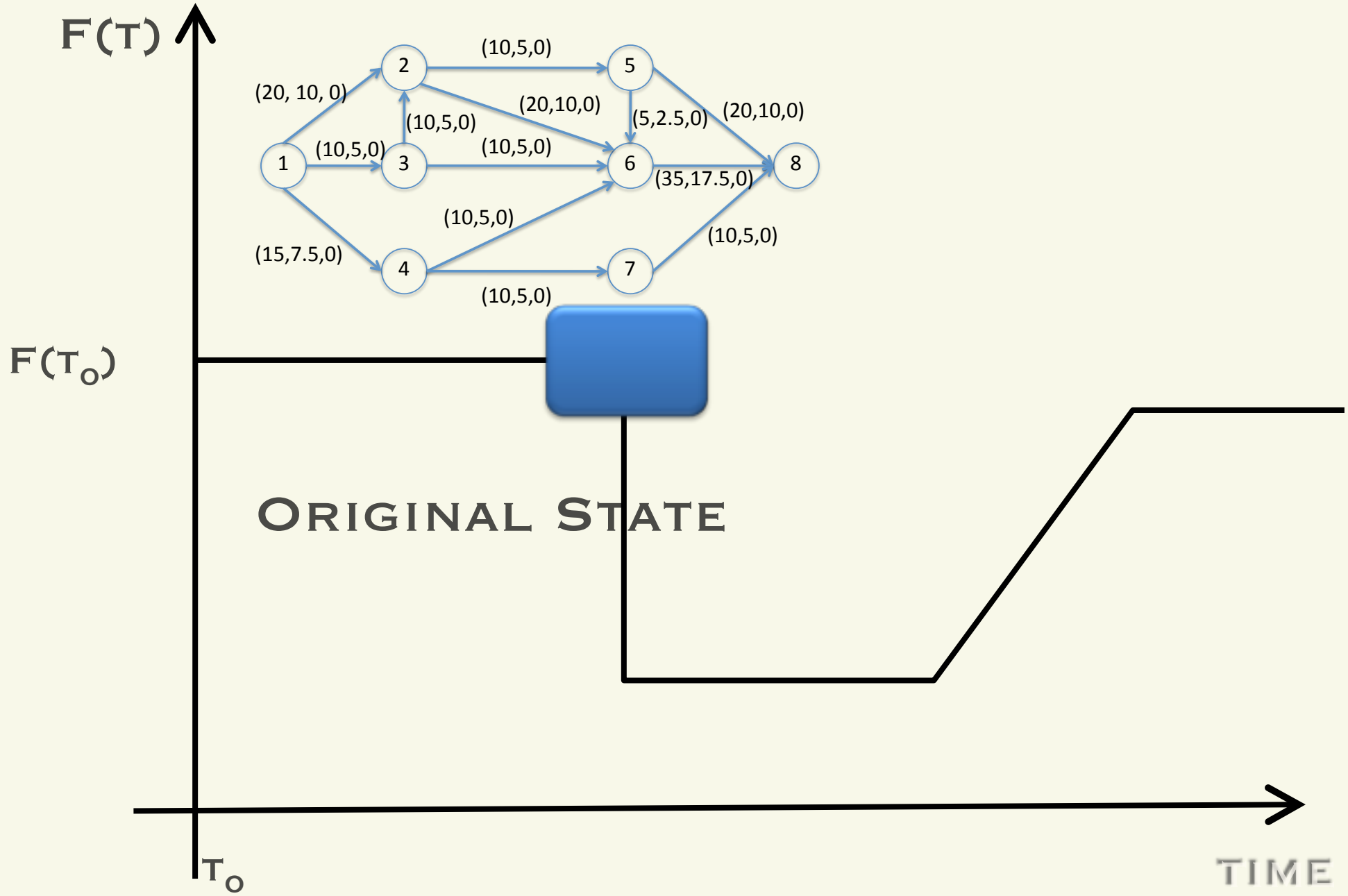


ORIGINAL STATE

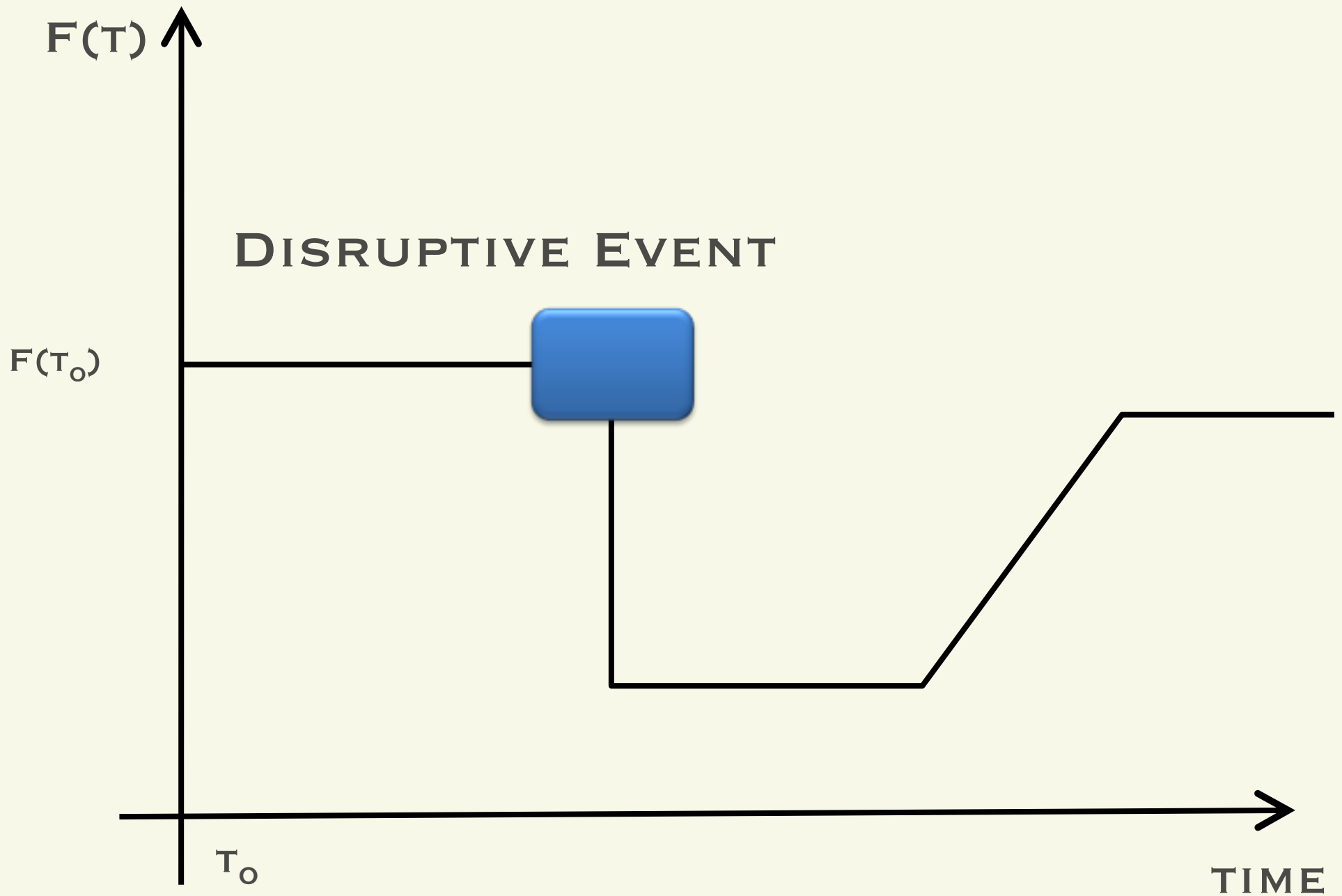
T_0

TIME

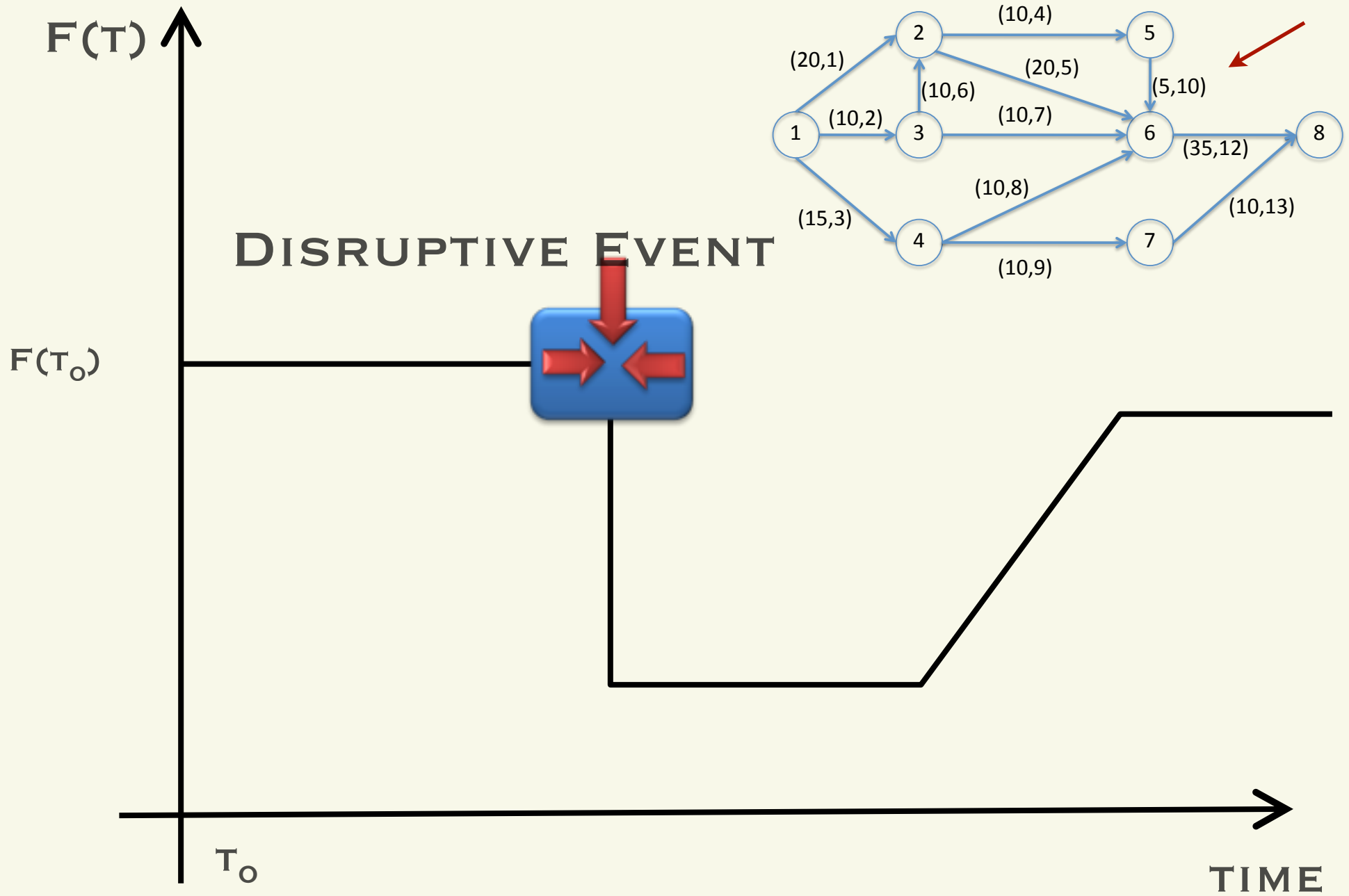
VULNERABILITY & RESILIENCE



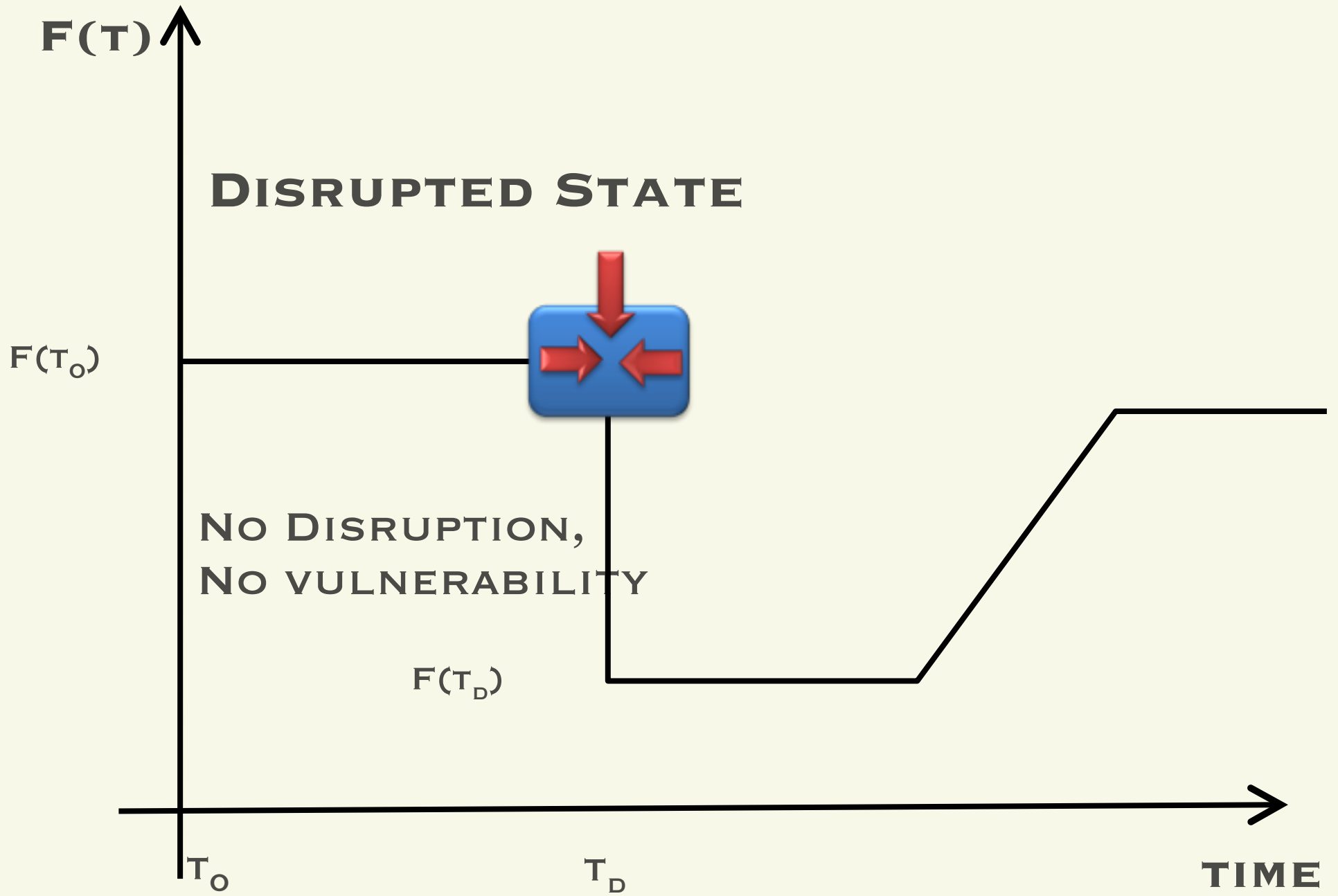
VULNERABILITY ANALYSIS



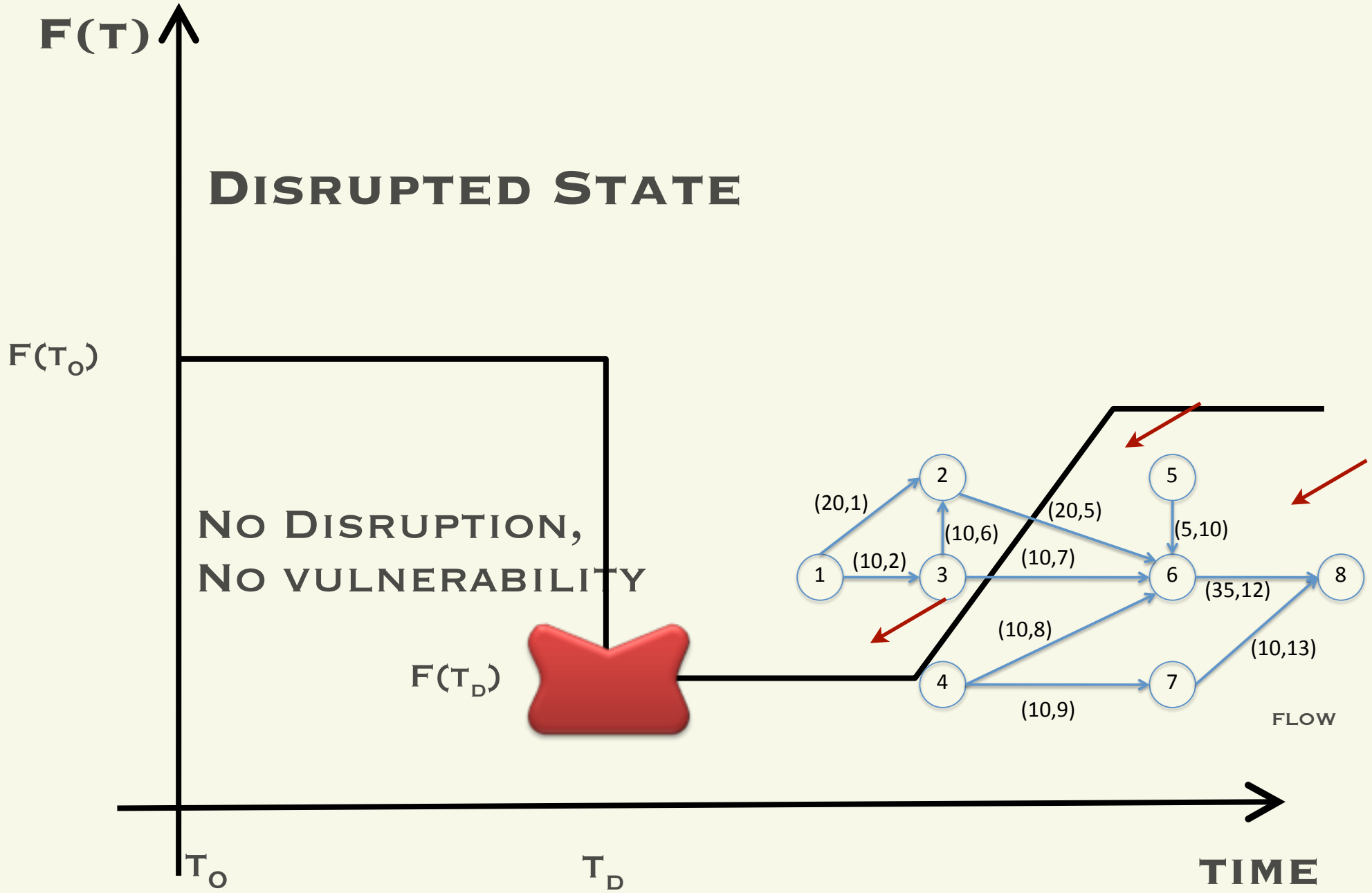
VULNERABILITY ANALYSIS



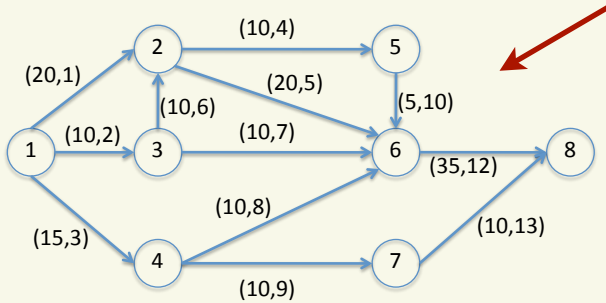
VULNERABILITY ANALYSIS



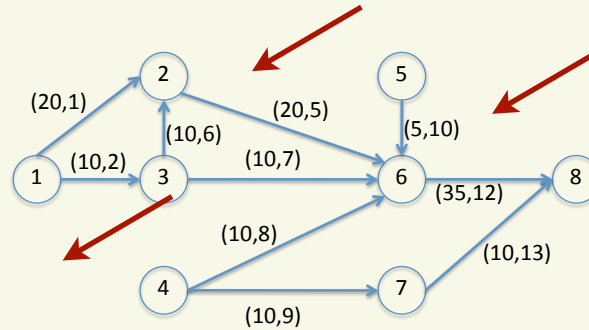
VULNERABILITY ANALYSIS



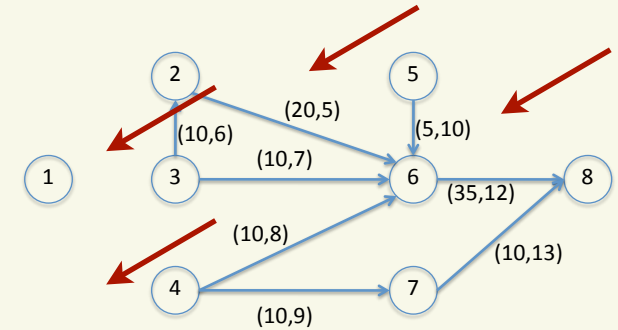
COMPUTATIONAL ISSUES IN ANALYZING VULNERABILITY



1 FAILURE EVENT



3 FAILURES EVENT



4 FAILURES EVENT

COMPUTATIONALLY EXPENSIVE TO ENUMERATE ALL FAILURE EVENTS FOR LARGE NETWORKS

APPROXIMATE:

$$FR(w_1, w_2, \dots, w_j, \dots, w_\alpha) = F(\mathbf{x}) - F(\mathbf{x} \mid x_{w_1} = x_{w_2} = \dots = x_{w_j} = \dots = x_{w_\alpha})$$

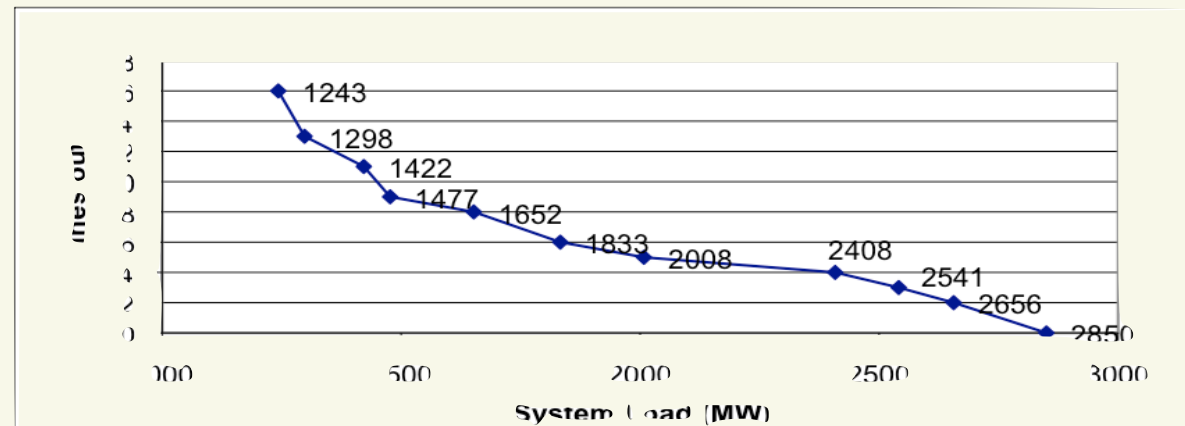
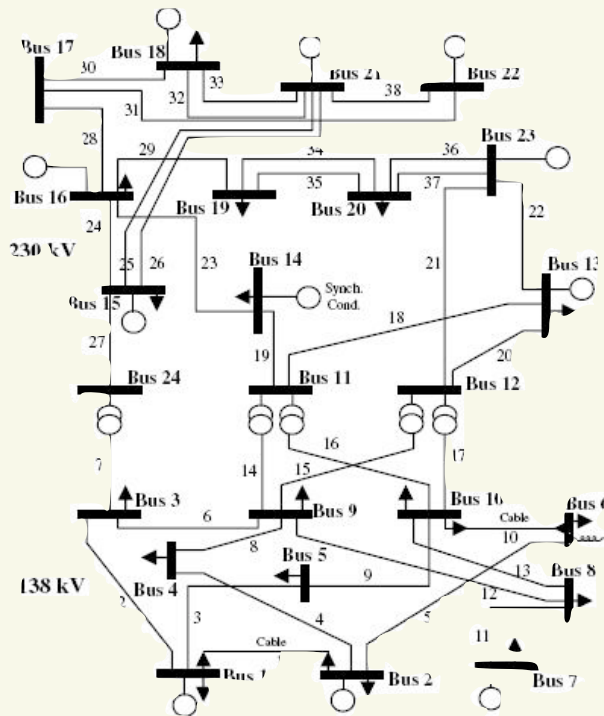
$$V(\alpha) = \left\{ FR(w_1, w_2, \dots, w_j, \dots, w_\alpha) \mid \forall w_1 \neq w_2 \neq \dots \neq w_j \neq \dots \neq w_\alpha \right\}$$

$$D(\alpha) = \underset{w_1 \neq w_2 \neq \dots \neq w_j \neq \dots \neq w_\alpha}{\operatorname{argmax}} \{V(\alpha)\}$$

CURRENT RESEARCH IN VULNERABILITY

-IDENTIFICATION OF $D(\alpha) = \underset{w_1 \neq w_2 \neq \dots \neq w_j \neq \dots \neq w_\alpha}{\operatorname{argmax}} \{V(\alpha)\}$

VIA MULTI-OBJECTIVE OPTIMIZATION
PARETO FRONT CONSTRUCTION

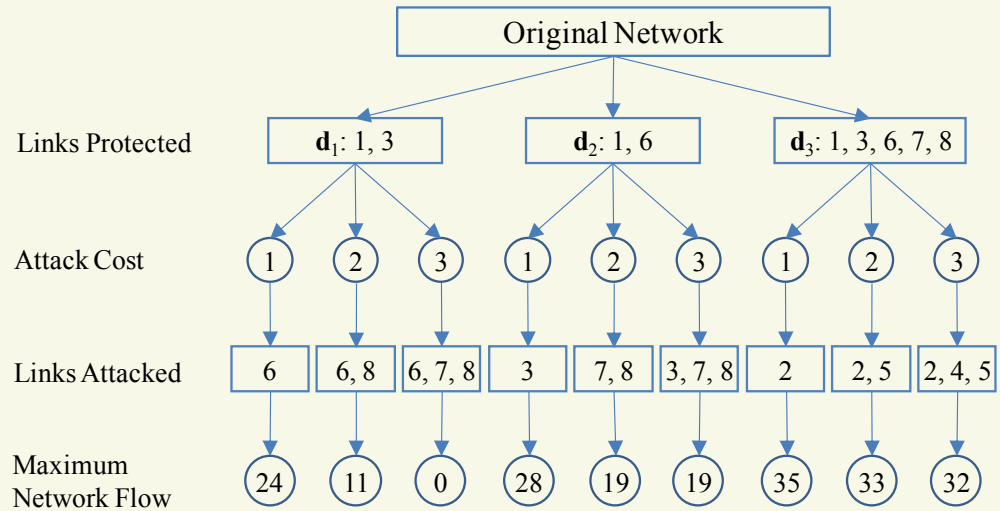
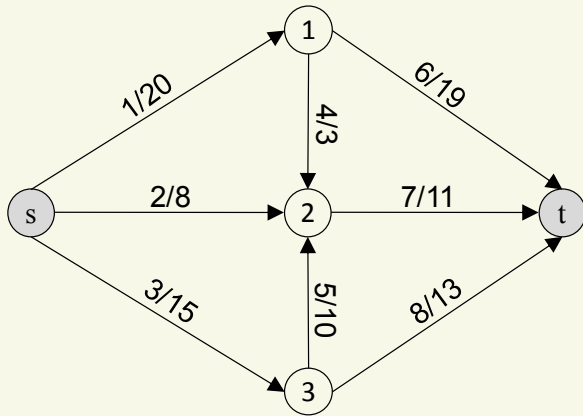


OPEN RESEARCH QUESTION:

OBTAIN ALL EVENTS THAT REDUCE FLOW BY SOME GIVEN %

CURRENT RESEARCH IN VULNERABILITY

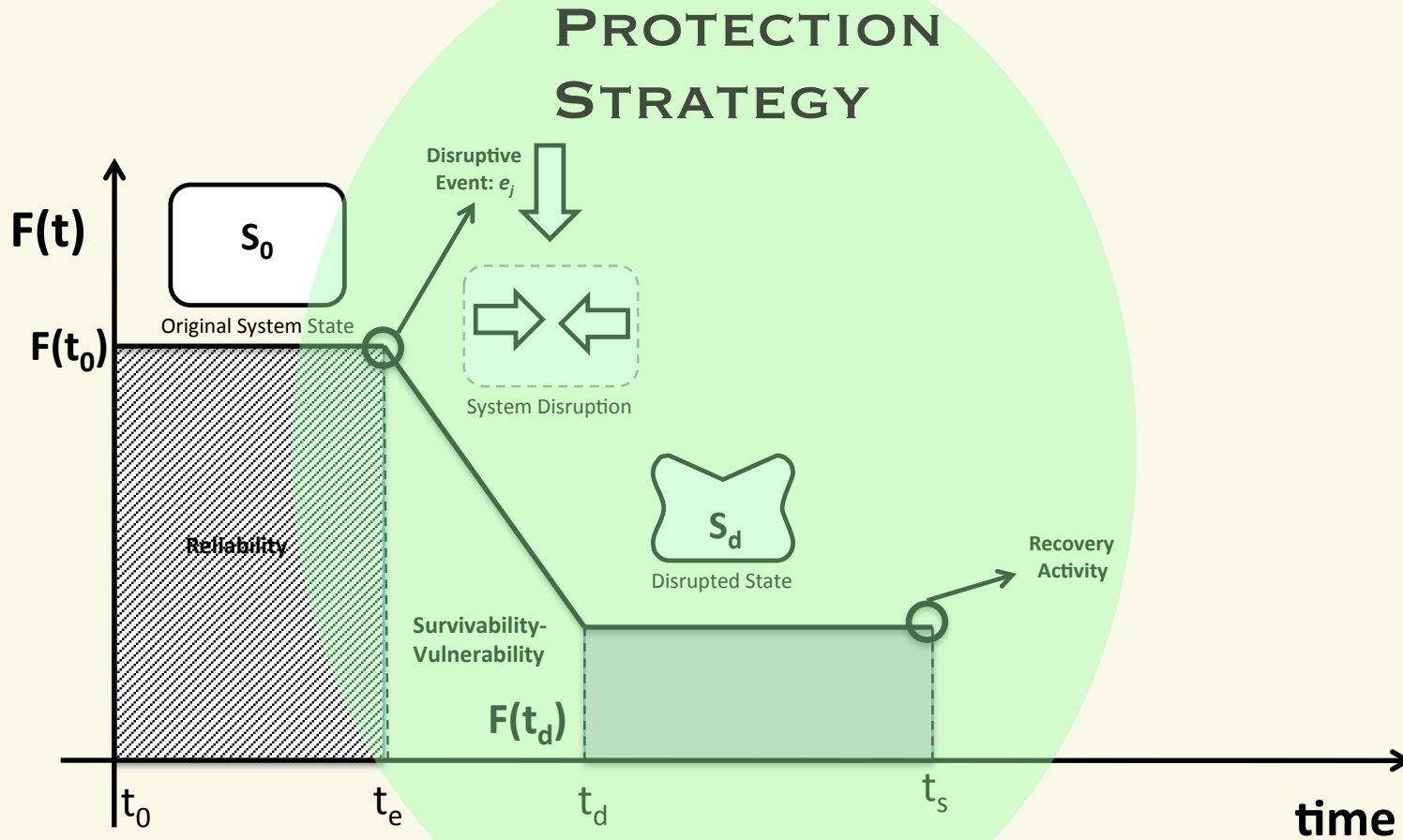
CONTEST BETWEEN ATTACKER & DEFENDER:
 -RATIONAL PLAYERS MAXIMIZE “GAINS”:



Protection Strategy			Maximum Network Flow Under Attack Cost k		
Index	Link Protected	Cost	1	2	3
1	1	1	24	11	0
2	1, 6	2	28	19	19
3	1, 3, 6	3	30	19	19
4	1, 6, 7	3	28	20	19
5	1, 3, 6, 8	4	32	32	32
6	1, 3, 6, 7, 8	5	35	33	32
7	1, 3, 6, 8, 2, 7	6	41	40	40

OPEN RESEARCH:
 DEFENSE/ATTACK INTENSITY FUNCTION

NETWORK VULNERABILITY



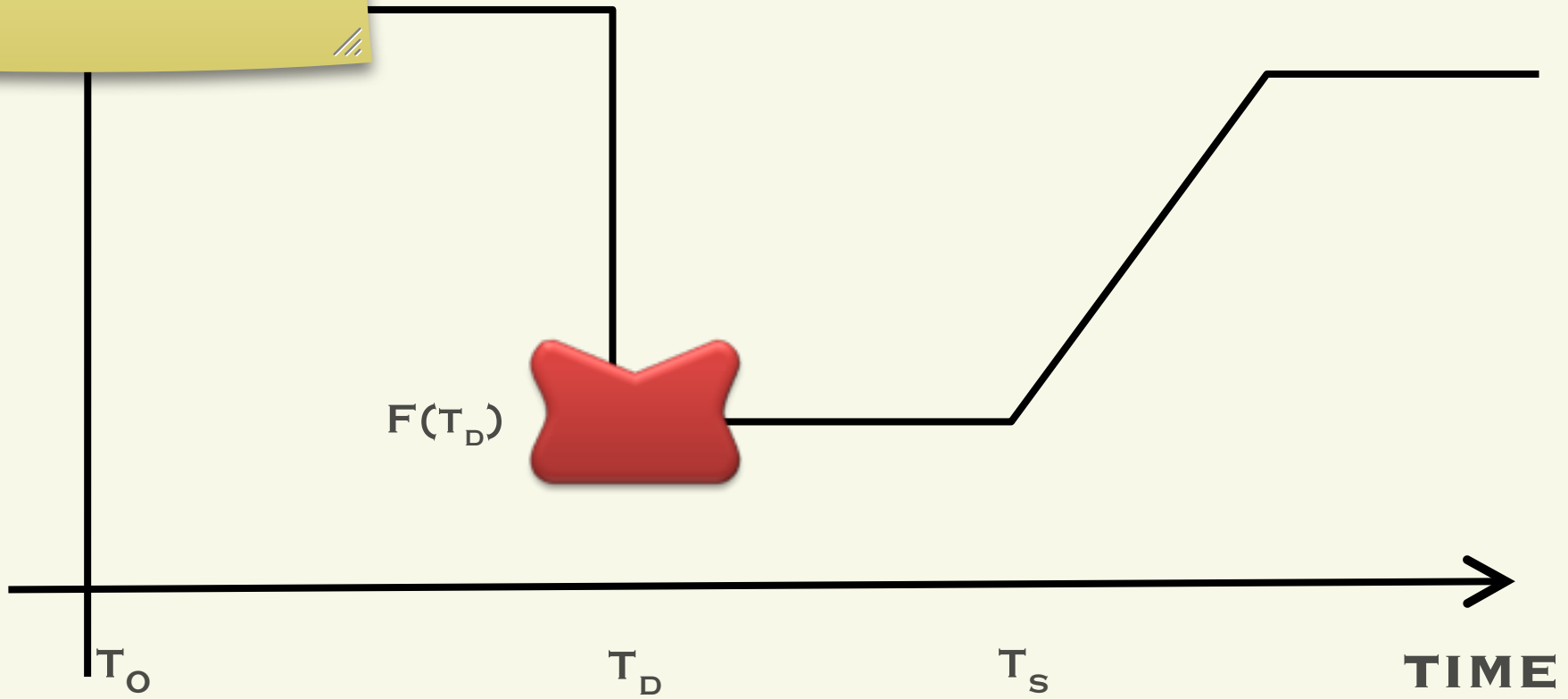
NETWORK VULNERABILITY: DESCRIBES HOW THE DELIVERY FUNCTION OF A NETWORK IS AFFECTED BY EXTERNAL FAILURE EVENTS

RESILIENCE ANALYSIS

$F(t)$ ↑

Talk about time dependency

RESILIENCE RESPONSE

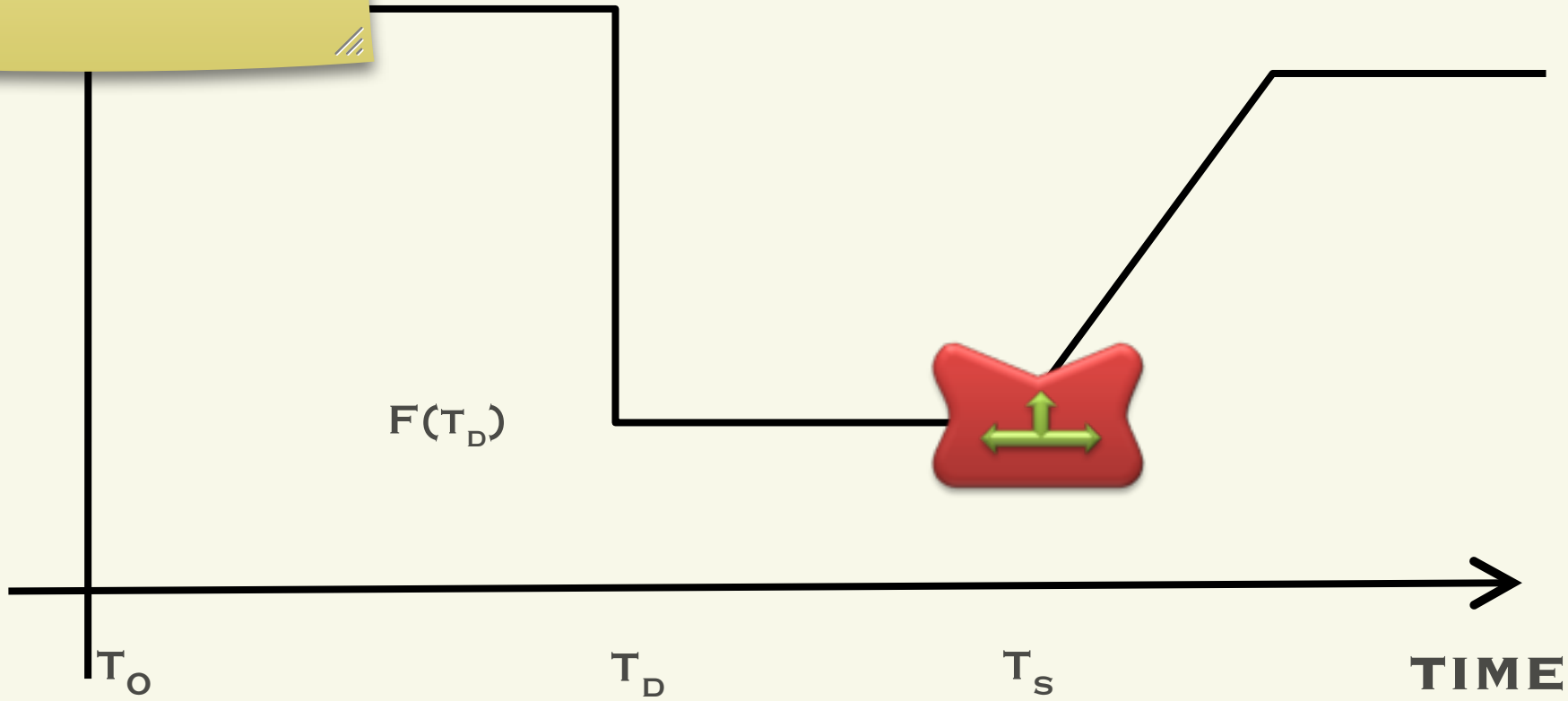
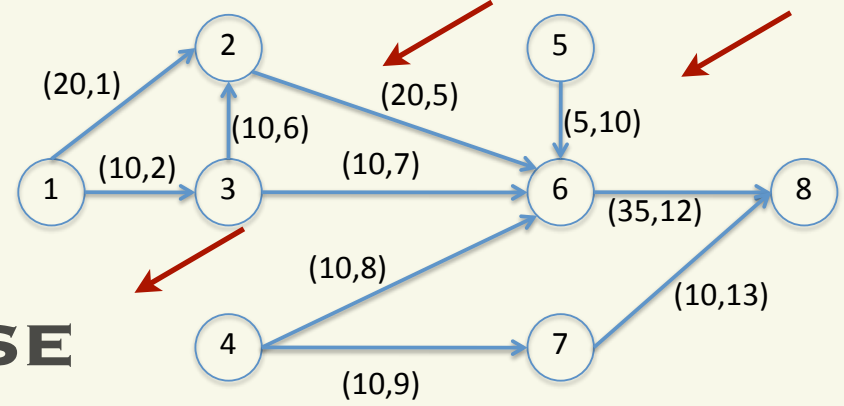


RESILIENCE ANALYSIS

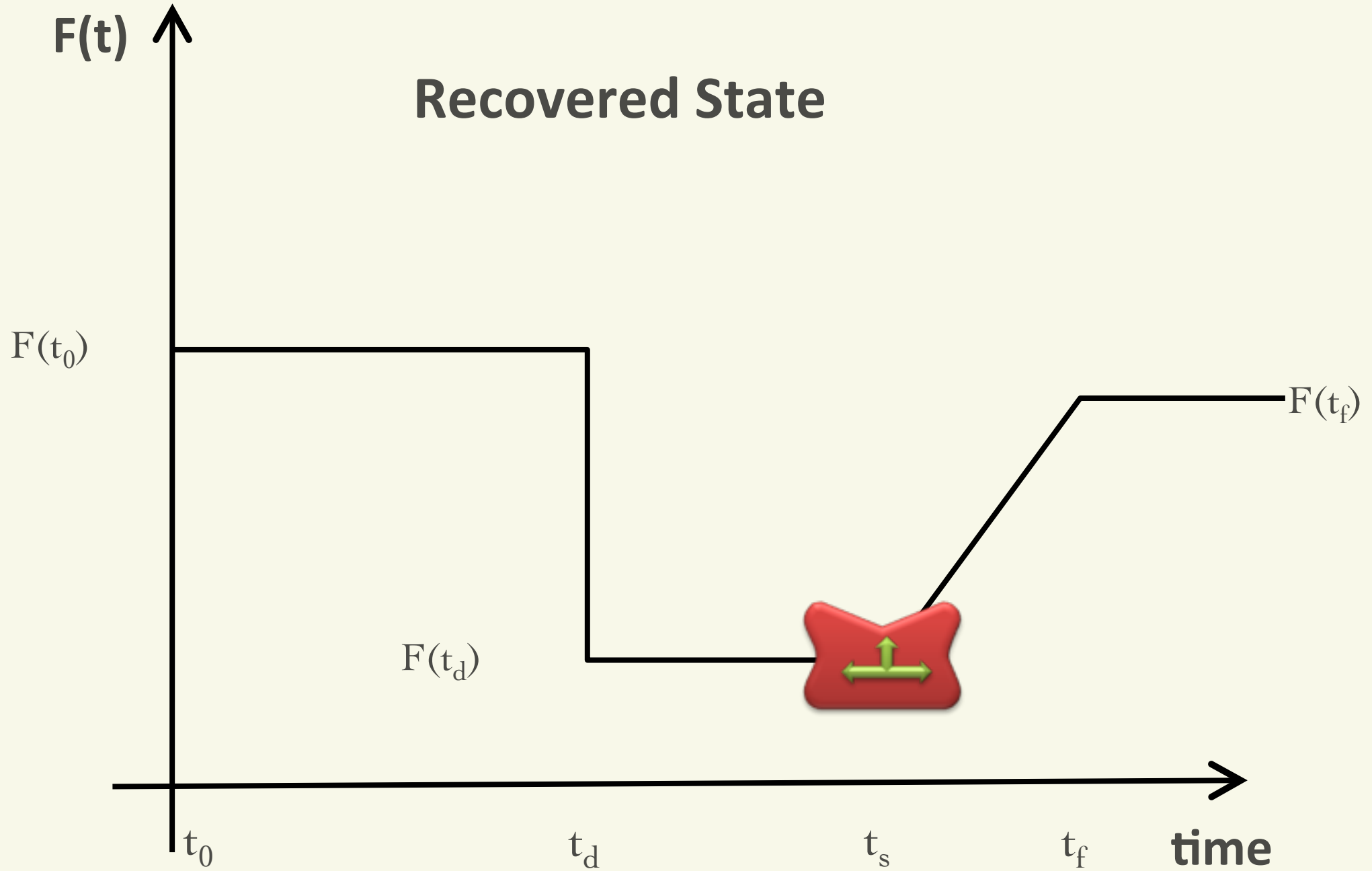
$F(T)$ ↑

Talk about time dependency

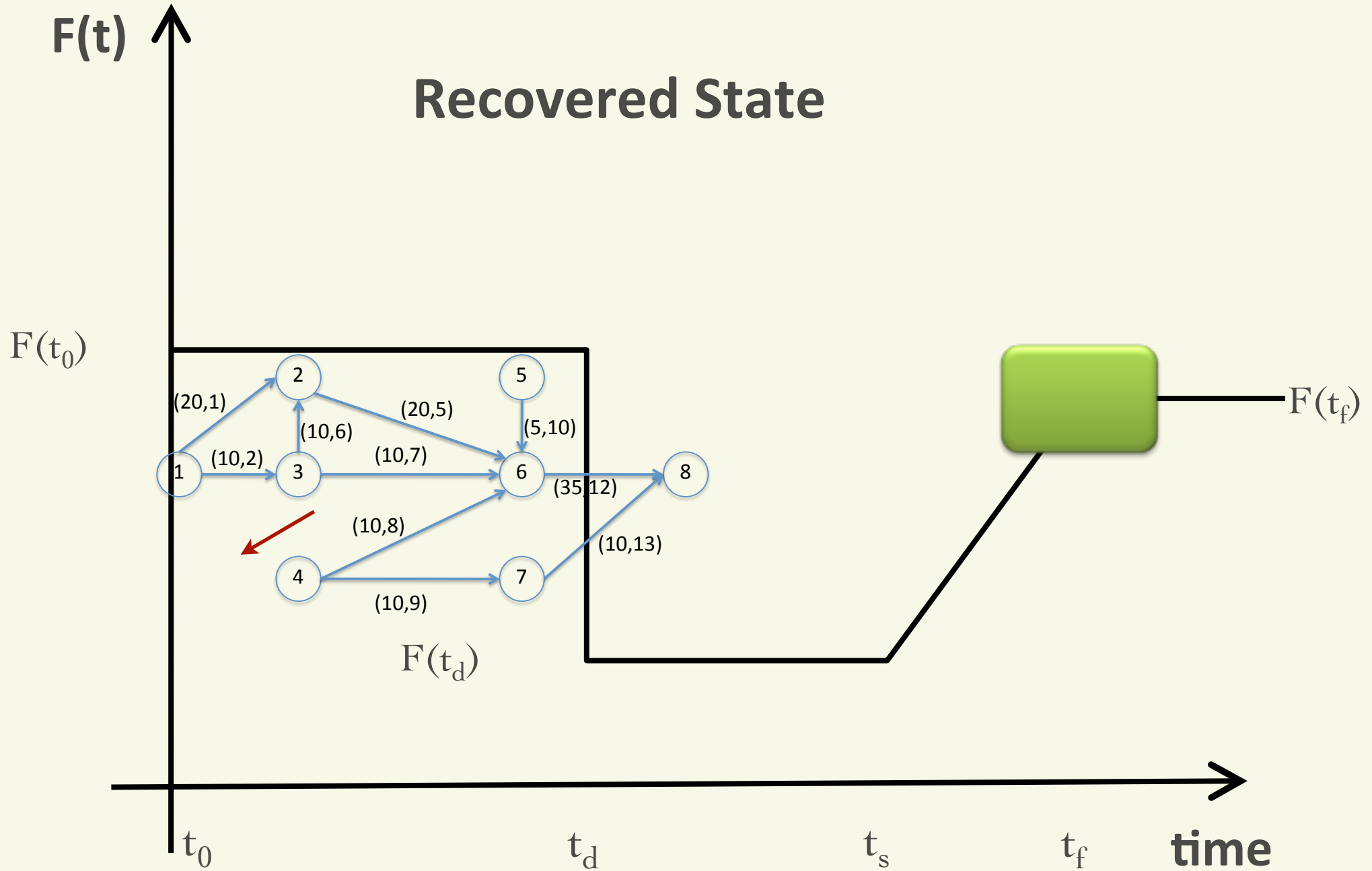
RESILIENCE RESPONSE



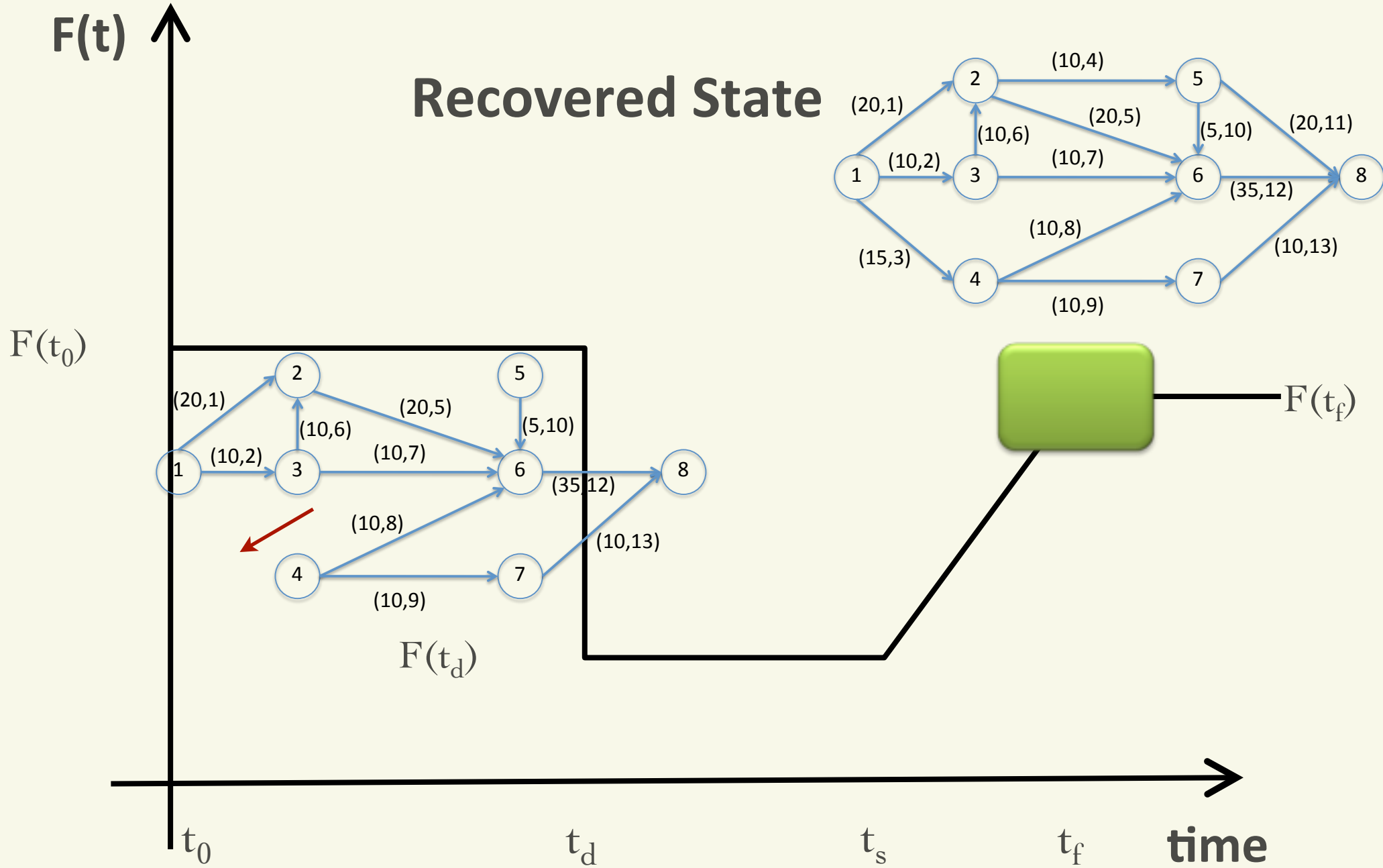
RESILIENCE ANALYSIS



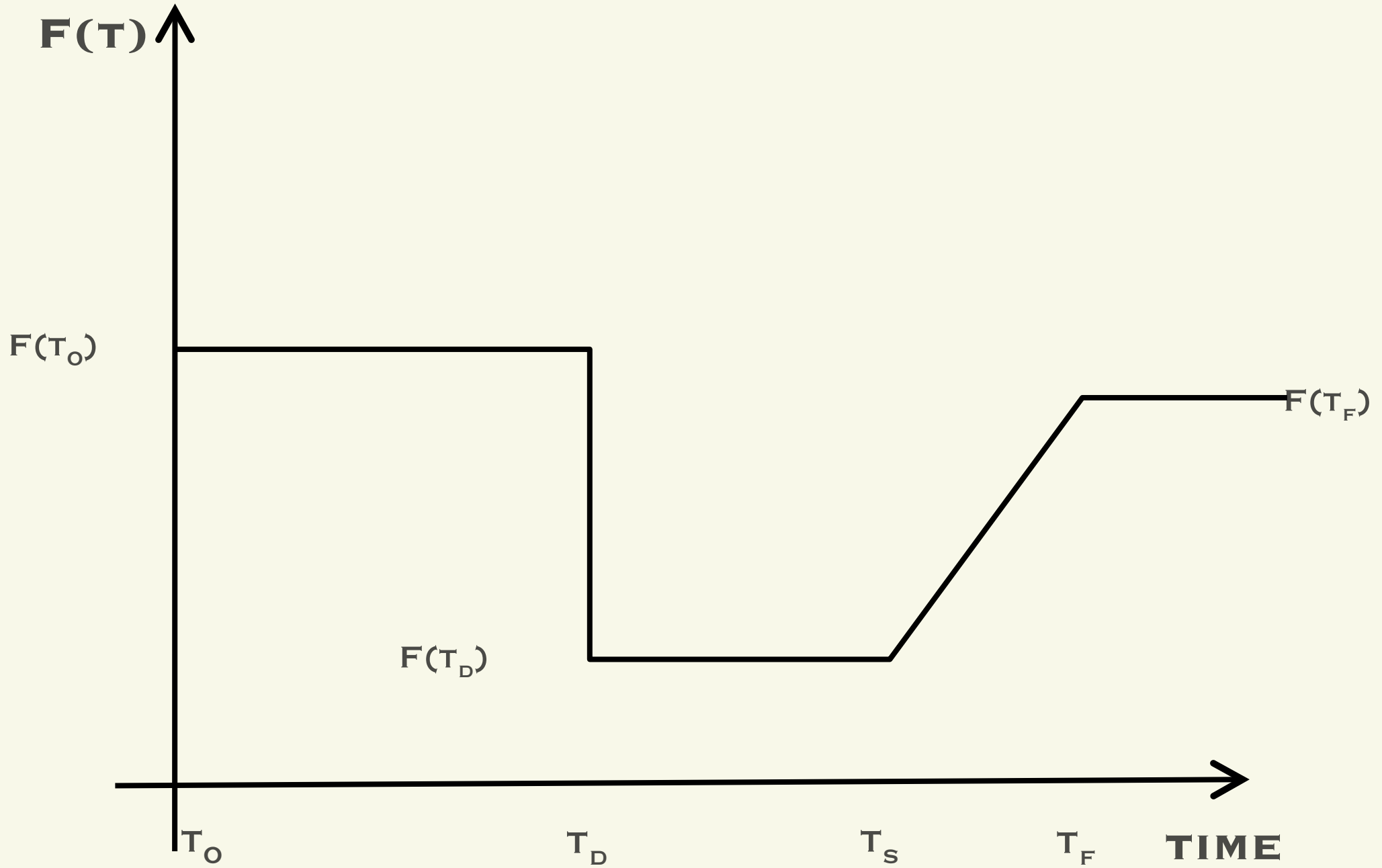
RESILIENCE ANALYSIS



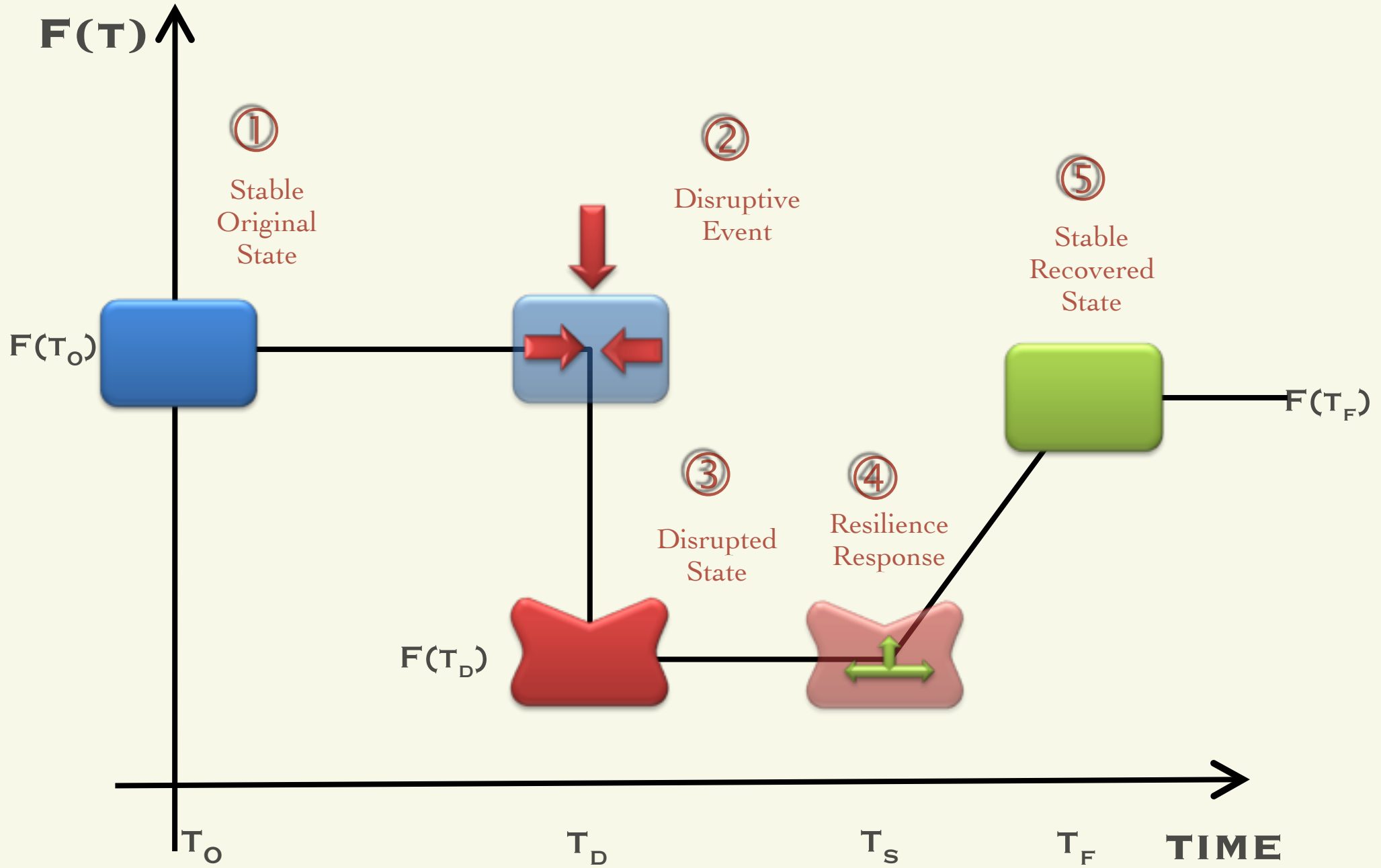
RESILIENCE ANALYSIS



RESILIENCE ANALYSIS



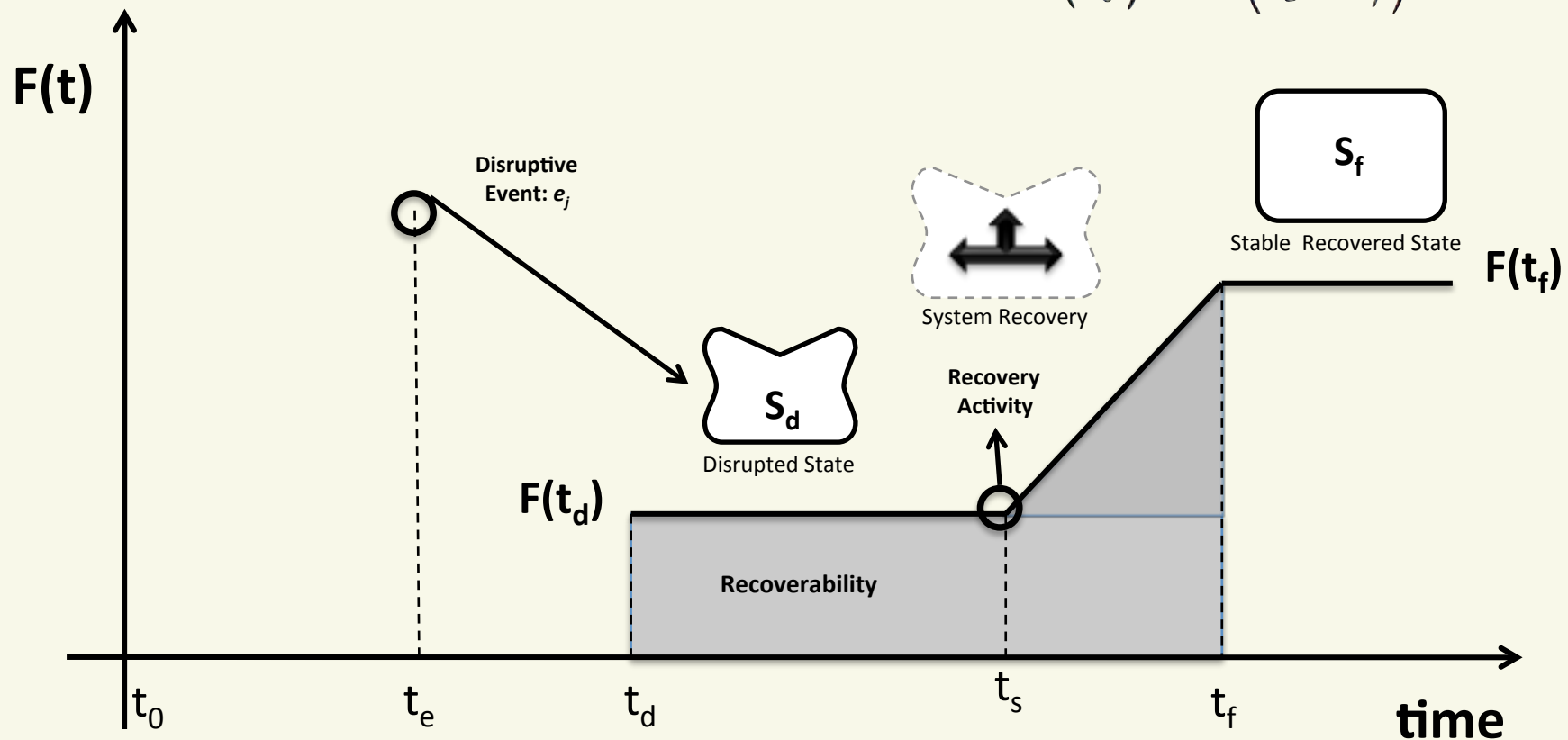
RESILIENCE ANALYSIS



RESILIENCE ANALYSIS

RESILIENCE: DESCRIBES HOW THE DELIVERY FUNCTION OF A NETWORK RETURNS TO “NORMALCY” AFTER A VULNERABLE EVENT

$$\mathcal{R}_F(t_r | e_j) = \frac{F(t_r | e_j) - F(t_d | e_j)}{F(t_0) - F(t_d | e_j)}$$



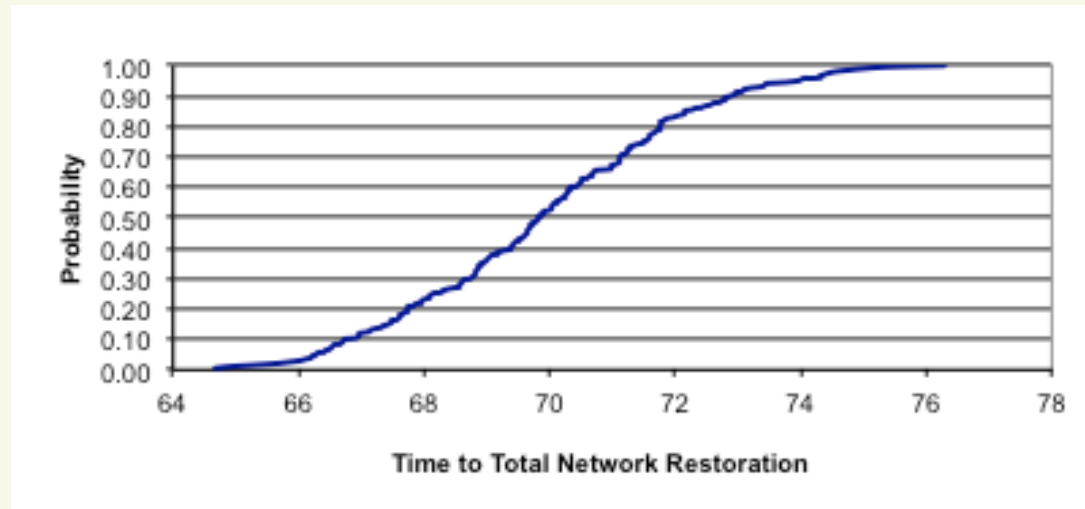
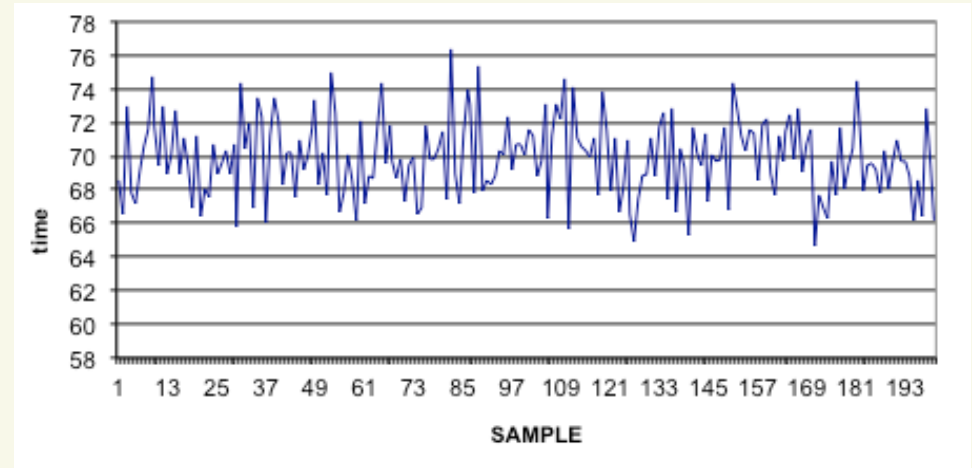
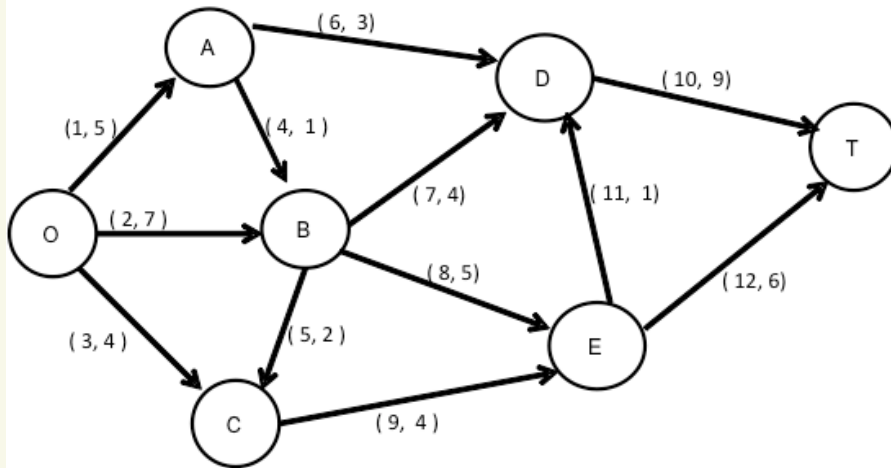
RESILIENCE METRICS

-TIME TO TOTAL NETWORK RESTORATION - THIS METRIC RECORDS THE TOTAL TIME SPENT FROM WHEN RECOVERY ACTIVITIES ARE STARTED, AT TIME T_S , UP TO THE TIME WHEN ALL RECOVERY ACTIVITIES ARE FINALIZED

-TIME TO FULL NETWORK SERVICE RESILIENCE - THIS METRIC RECORDS THE TOTAL TIME SPENT FROM WHEN RECOVERY ACTIVITIES ARE STARTED, AT TIME T_S , UP TO THE EXACT TIME, T_F , WHEN THE NETWORK SERVICE IS COMPLETELY RESTORED.

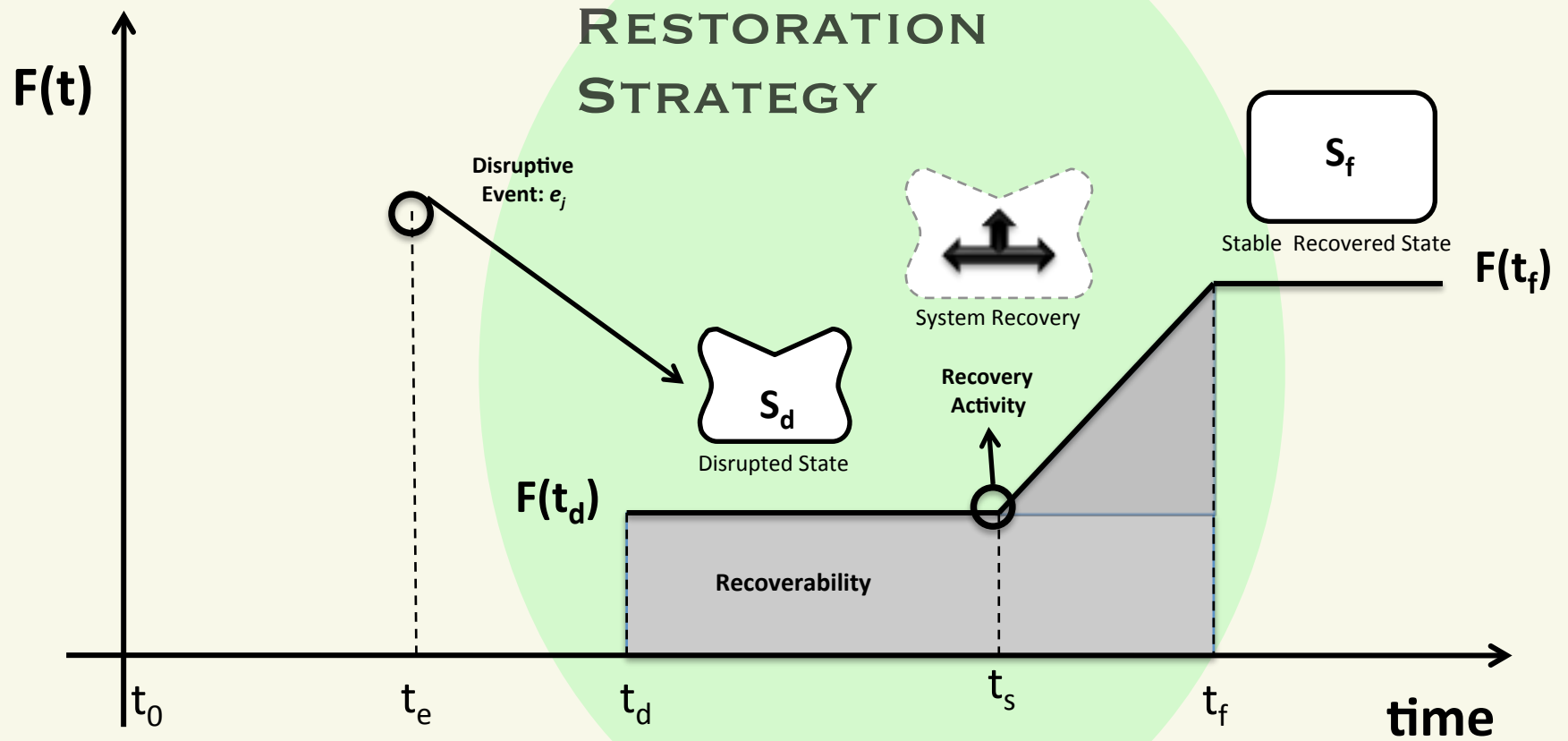
**TIME TO ALPHA%-RESILIENCE - THIS METRIC RECORDS THE TOTAL TIME SPENT FROM WHEN RECOVERY ACTIVITIES ARE STARTED, AT TIME T_S , UP TO THE EXACT TIME, T , WHEN THE NETWORK SERVICE IS RESTORED
ALPHA %**

NETWORK RESILIENCE



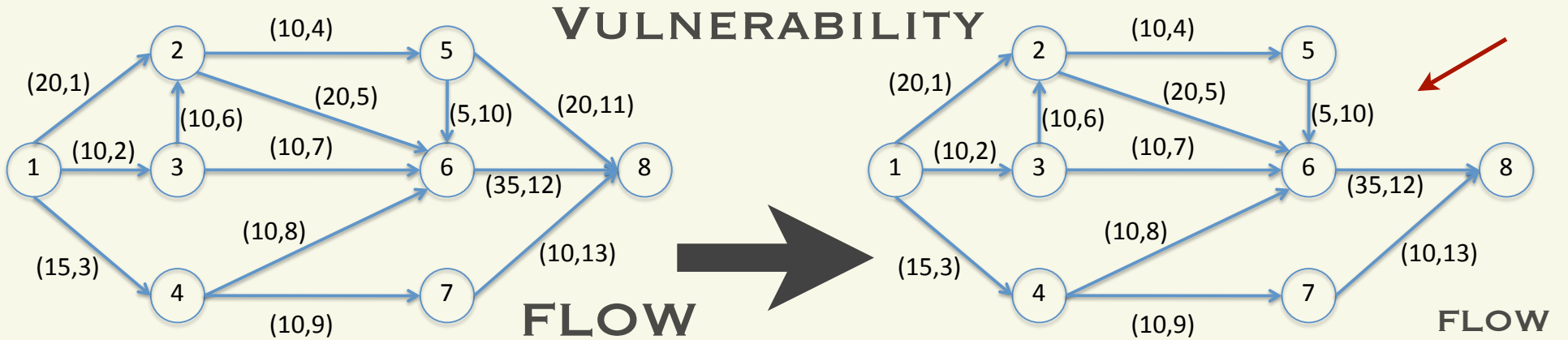
-TIME TO

NETWORK RESILIENCE



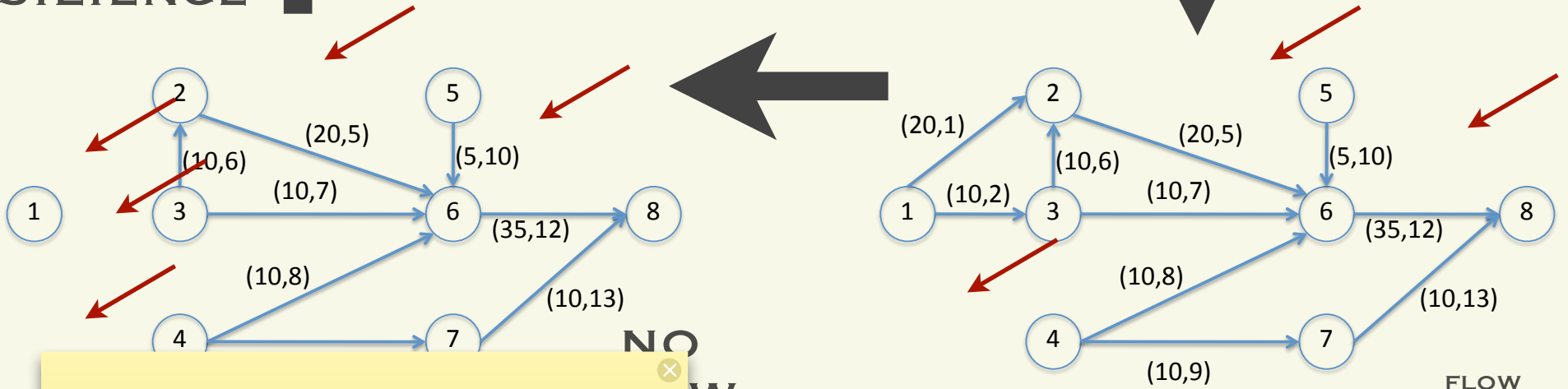
RESILIENCE: DESCRIBES HOW THE DELIVERY FUNCTION OF A NETWORK RETURNS TO “NORMALCY” AFTER A VULNERABLE EVENT

NEW RESEARCH AREAS



PROTECTION POLICIES

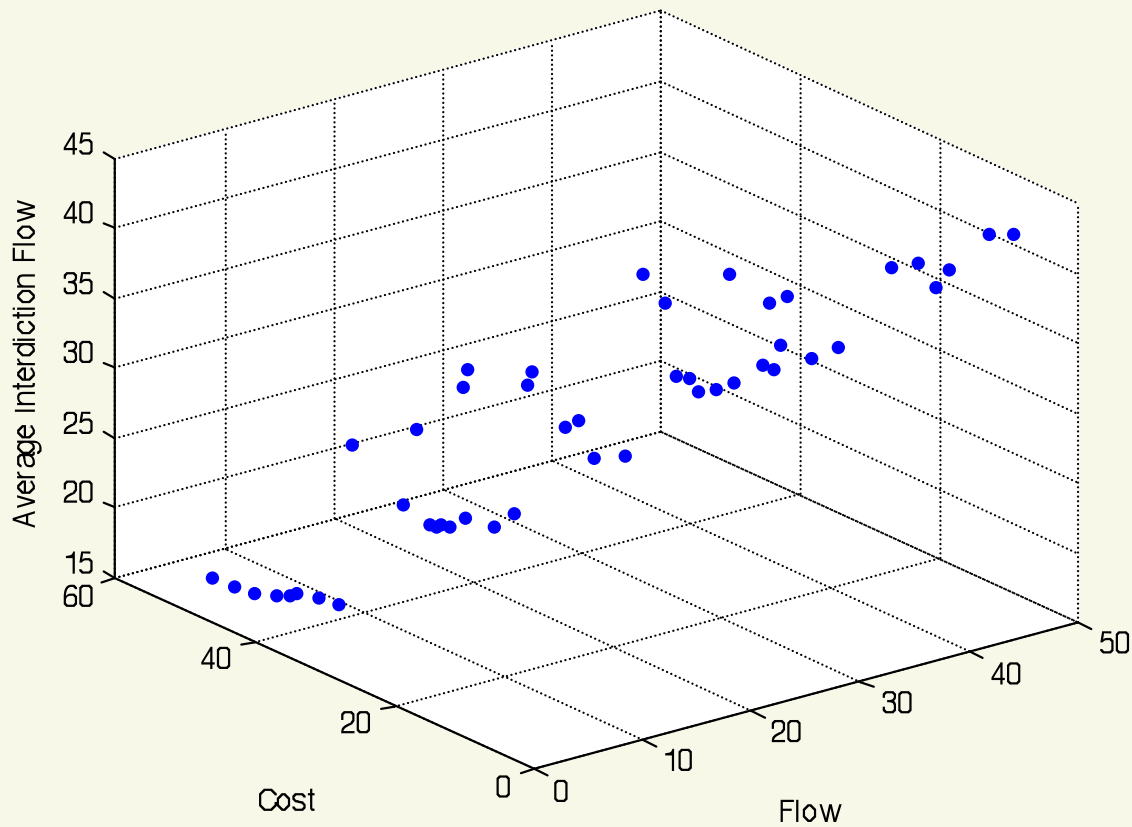
RESILIENCE



Vulnerare= open to attack or damage

Resilience= ability of a system to bounce back

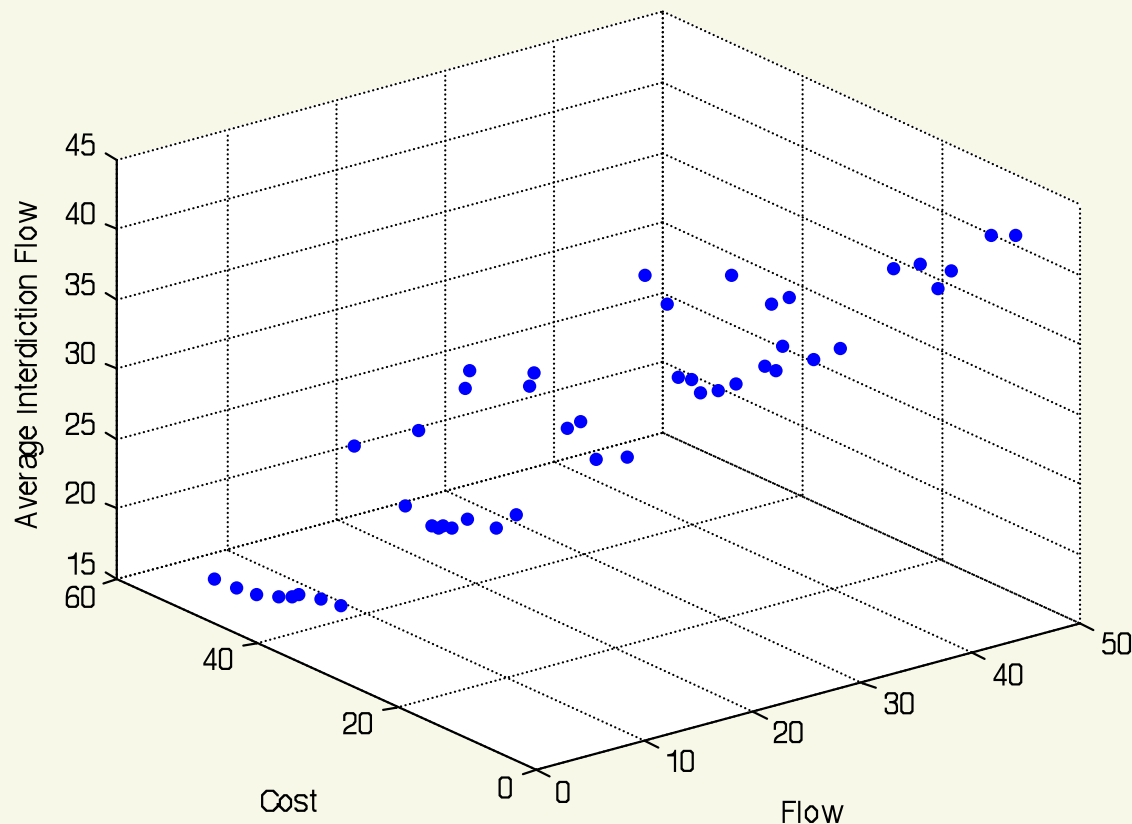
VULNERABILITY & RESILIENCE OPTIMIZATION



VULNERABILITY & RESILIENCE OPTIMIZATION

ANALYSIS OF WORST CASE FAILURE EVENTS
FAILURE EVENTS, NETWORK DESCRIPTION

RESPONSE OR NETWORK RECOVERY APPROACH
RECOVERY TIME FOR EACH COMPONENT
RECOVERY POLICY SYSTEM WIDE
RECOVERY RESOURCES



POLICIES FOR
PROTECTION SHOULD
BE BASED ON THE
OPTIMIZATION OF
RESOURCES

CONCLUSIONS

CONCLUSIONS

THEORETICALLY NETWORK VULNERABILITY CAN BE “QUANTIFIED” BUT THERE PERSIST COMPUTATIONAL ISSUES. GOOD AREA FOR RESEARCH

ALSO CAN BE THEORETICALLY ANALYZED BUT FROM A PRACTICAL PERSPECTIVE THERE ARE TOO MANY INPUTS VERY GOOD AREA FOR RESEARCH

PROTECTION POLICIES IN DEVELOPMENT. FERTILE GROUND FOR RESEARCH. REMEMBER THE IDEA IS TO INCREASE RELIABILITY, REDUCE VULNERABILITY AND INCREASE RESILIENCE

WHO AND WHERE



**JOSE EMMANUEL
RAMIREZ-MARQUEZ
ASSOCIATE PROFESSOR
[HTTP://
PERSONAL.STEVENS.EDU/
~,ARQUEZ](http://personal.stevens.edu/~,arquez)**

**PH.D OPPORTUNITIES
AVAILABLE**

