Cyber Resiliency and Survivability in Aerospace & Defense Domains

2023 IFIP WG10.4 Workshop Panel
“Dependability and Security Challenges in the face of 21st Century Threats and Trends: Industry and Academic Perspectives”

25 June 2023

Dr. Jay Lala
Sr. Principal Technical Fellow
Raytheon
San Diego, CA 92123

Fault Classification*

Fault Classes addressed in 20th Century

NATURE		ORIGIN						PERSISTENCE		Usual Labelling
		Phenomenological Cause		System Boundaries		Phase of Creation				
Accidental Faults	Intentional Faults	Physical Faults	Human-made Faults	Internal Faults	External Faults	Design Faults	Operational Faults	Permanent Faults	Temporary Faults	
X		X		X			X	X		*Physical Faults*
X		X			X		X	X		
X		X			X		X		X	*Transient Faults*
X		X		X			X		X	*Intermittent Faults*
X			X	X		X			X	
X			X	X		X		X		*Design Faults*
X			X		X		X		X	*Interaction Faults*
	X		X	X		X		X		*Malicious Logic*
	X		X	X		X			X	
	X		X		X		X	X		*Intrusions*
	X		X		X		X		X	

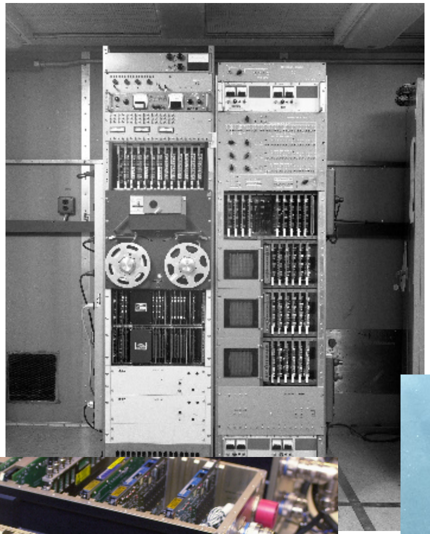
* J. C. Laprie (ed), "Dependability: Concepts & Terminology," Dependable Computing and Fault-Tolerant Systems, Vol. 5, Figure 3, Springer-Verlag, Wien-New York, 1992.

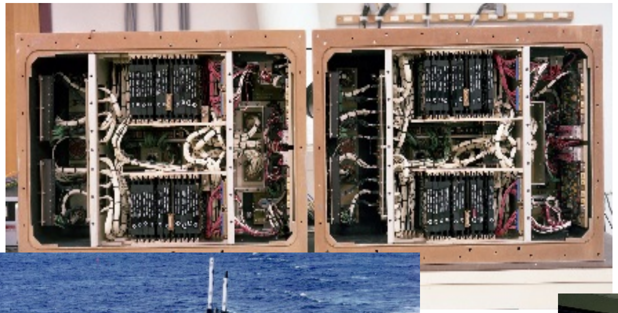
20th Century Progress in Dependable Systems

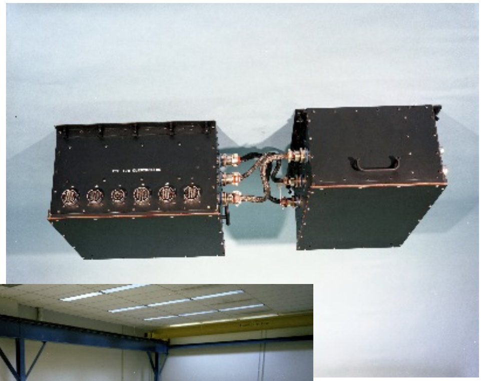
- As the use of digital systems (hardware, software, and networks) proliferated, their many shortcomings created impediments in applications demanding high dependability.
- Long-term efforts by the community (academia, industry, and governing bodies), resulted in remarkable progress in tackling 3 pillars of dependability (specifications, designs, and V&V).
- Systems that can tolerate accidental faults have been successfully deployed in all walks of life and at huge scales and at extremely high levels of dependability:
  - Air and space travel
  - Communications
  - Defense
  - e-commerce
  - Finance
  - Ground transportation
  - Industrial production

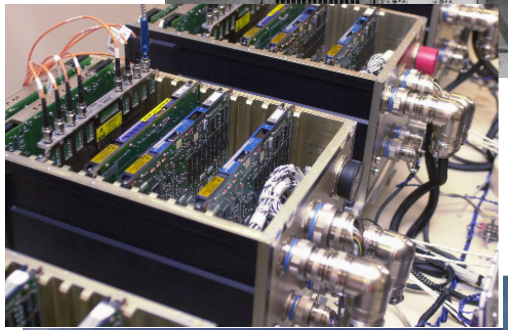
Digital fabric of society is highly reliable, available, and safe.

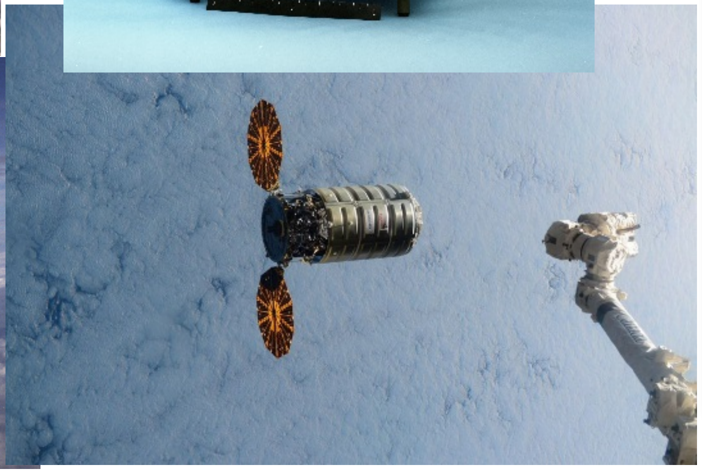
Example Safety-Critical Computers (Draper Lab)











- Numerous mission and safety-critical fault tolerant computers
- Space, Air, Ground, and Sea Platforms
- Triple, Quad or Higher Redundancy
- Theoretically Correct FT Architectures
- Fault-Tolerant Software
- Extensive Analytical & Empirical Validation

Turn of the Century: Change in Threat Landscape

- At the end of 20th century, having done enough damage for a quarter century at Draper, I was ready to retire from the dependable field.

- Then something happened that gave me job security ☺

Hackers Testifying at the United States Senate, May 19, 1998 (L0pht Heavy Industries)

https://www.youtube.com/watch?v=VVJldn_MmMY

Intrusion Tolerant Systems
Fault Classification & ITS Scope

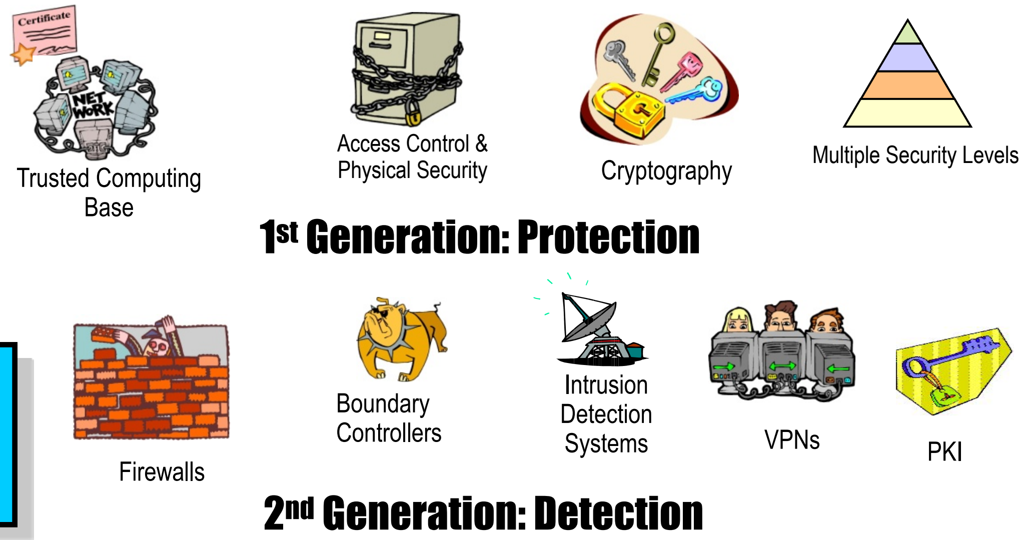
	NATURE		ORIGIN						PERSISTENCE		Usual Labelling
			Phenomenological Cause		System Boundaries		Phase of Creation				
	Accidental Faults	Intentional Faults	Physical Faults	Human-made Faults	Internal Faults	External Faults	Design Faults	Operational Faults	Permanent Faults	Temporary Faults	
Fault Tolerance	X		X		X			X	X		Physical Faults
	X		X			X		X	X		
	X		X			X		X		X	Transient Faults
	X		X		X			X		X	Intermittent Faults
	X			X	X		X			X	
	X			X	X		X		X		Design Faults
	X			X		X		X		X	Interaction Faults
ITS		X		X	X		X		X		Malicious Logic
		X		X	X		X			X	
		X		X		X		X	X		Intrusions
		X		X		X		X		X	

Cyber Resilient Architectures

Prevent Intrusions
(Access Controls, Cryptography, Trusted Computing Base)

But intrusions will occur

Detect Intrusions, Limit Damage
(Firewalls, Intrusion Detection Systems, Virtual Private Networks, PKI)



Cyber Resilient Architectures

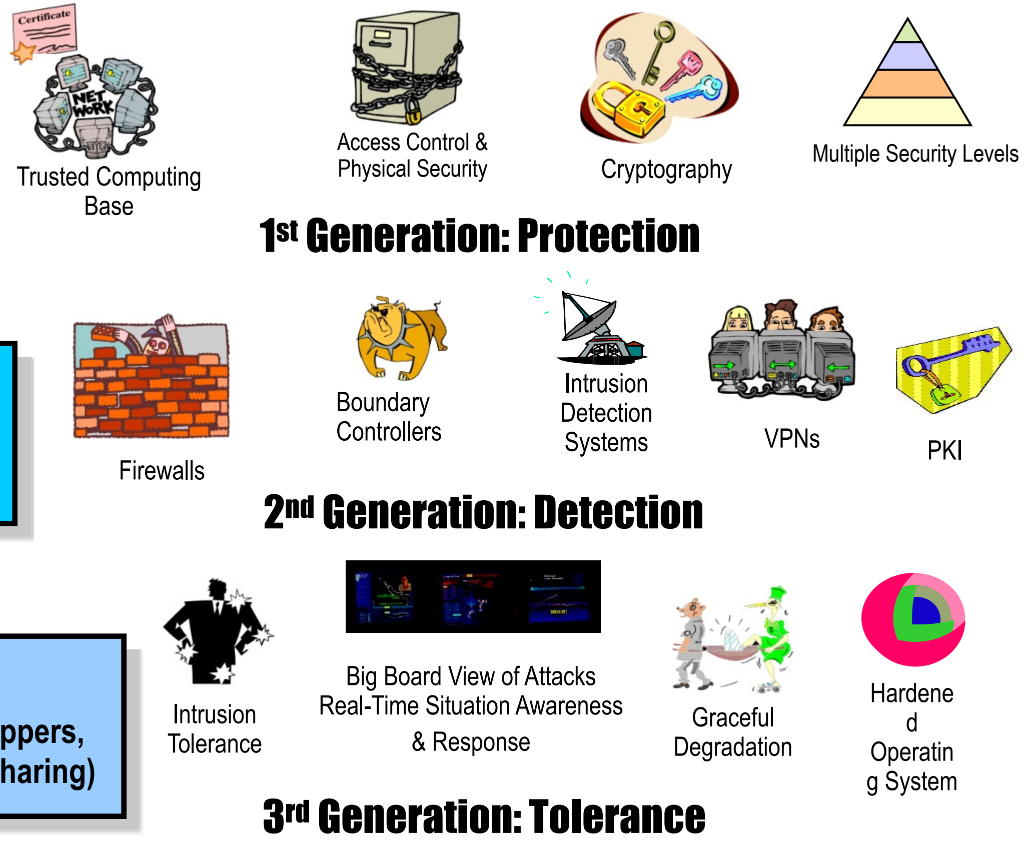
Prevent Intrusions
(Access Controls, Cryptography, Trusted Computing Base)

But intrusions will occur

Detect Intrusions, Limit Damage
(Firewalls, Intrusion Detection Systems, Virtual Private Networks, PKI)

But some attacks will succeed

Tolerate Attacks
(Redundancy, Diversity, Deception, Wrappers, Proof-Carrying Code, Proactive Secret Sharing)



Cyber Resilient Architectures

Prevent Intrusions
(Access Controls, Cryptography, Trusted Computing Base)

But intrusions will occur

Detect Intrusions, Limit Damage
(Firewalls, Intrusion Detection Systems, Virtual Private Networks, PKI)

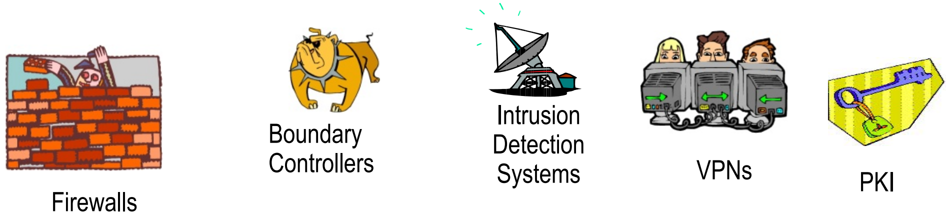
But some attacks will succeed

Tolerate Attacks
(Redundancy, Diversity, Deception, Wrappers, Proof-Carrying Code, Proactive Secret Sharing)

So the system must reconstitute

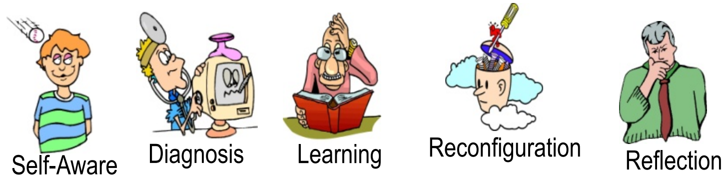
Restore System
(Diagnosis, Learning, Reconfiguration, S/W Rejuvenation, Natural Immunity, Reflection)

1st Generation: Protection



2nd Generation: Detection

3rd Generation: Tolerance



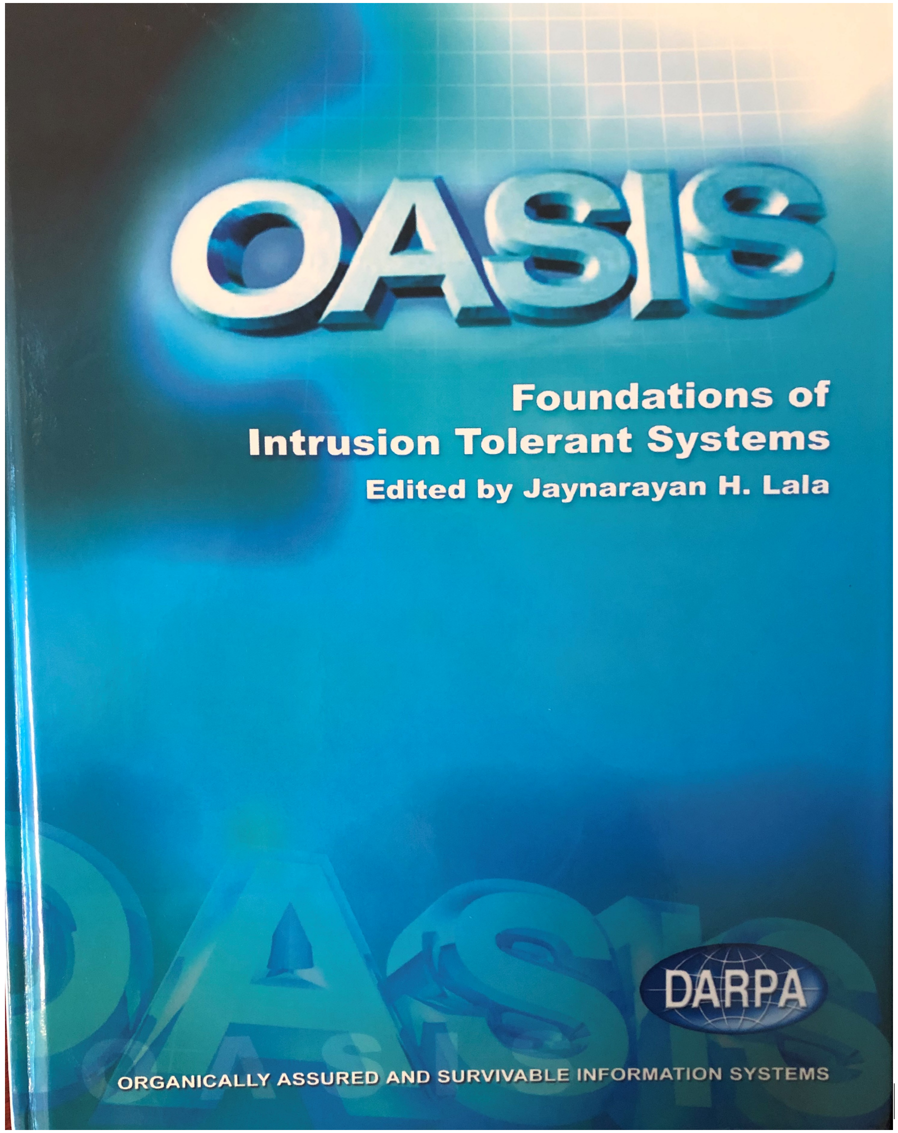
4th Generation: Regeneration

From Fault-Tolerance to Cyber Survivability

OASIS

Self- Regenerative Systems

Operate Through Attacks!!



US Dept of Defense Policy: Cyber Survivability

- Programs will employ system security engineering methods and practices, including cybersecurity, cyber resilience, and cyber survivability in design, test, manufacture, and sustainment.

- Such methods and practices will ensure that systems function as intended, mitigating risks associated with known and exploitable vulnerabilities to provide a level of assurance commensurate with technology, program, system, and mission objectives.

DoD Instruction 5000.83

Technology and Program Protection to Maintain Technological Advantage

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Effective:	July 20, 2020
Change 1 Effective:	May 21, 2021
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	See Paragraph 1.3.
Approved by:	Michael D. Griffin, Under Secretary of Defense for Research and Engineering
Change 1 Approved by:	Barbara K. McQuiston, Performing the Duties of the Under Secretary of Defense for Research and Engineering

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, the policy in Section 133a of Title 10, United States Code, and Directive-type Memorandum S-DTM-19-005, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to:
  - DoD-sponsored research and technology that is in the interest of national security.
  - DoD warfighting capabilities.
- Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans (TAPPs), S&T protection, program protection plans (PPPs), and engineering cybersecurity activities.

Cyber Survivability is now a Key Performance Parameter (KPP): Must meet requirement