Systemic Vulnerabilities

Allen D. Householder

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 OCT 2014	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Systemic Vulnerabilities	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Householder /Allen D.	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**66**	

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0001744

Systemic Vulnerabilities

Allen D. Householder

Systemic Vulnerabilities

An Allegorical Tale of Steampunk Vulnerability to Aero-Physical Threats

Allen D. Householder

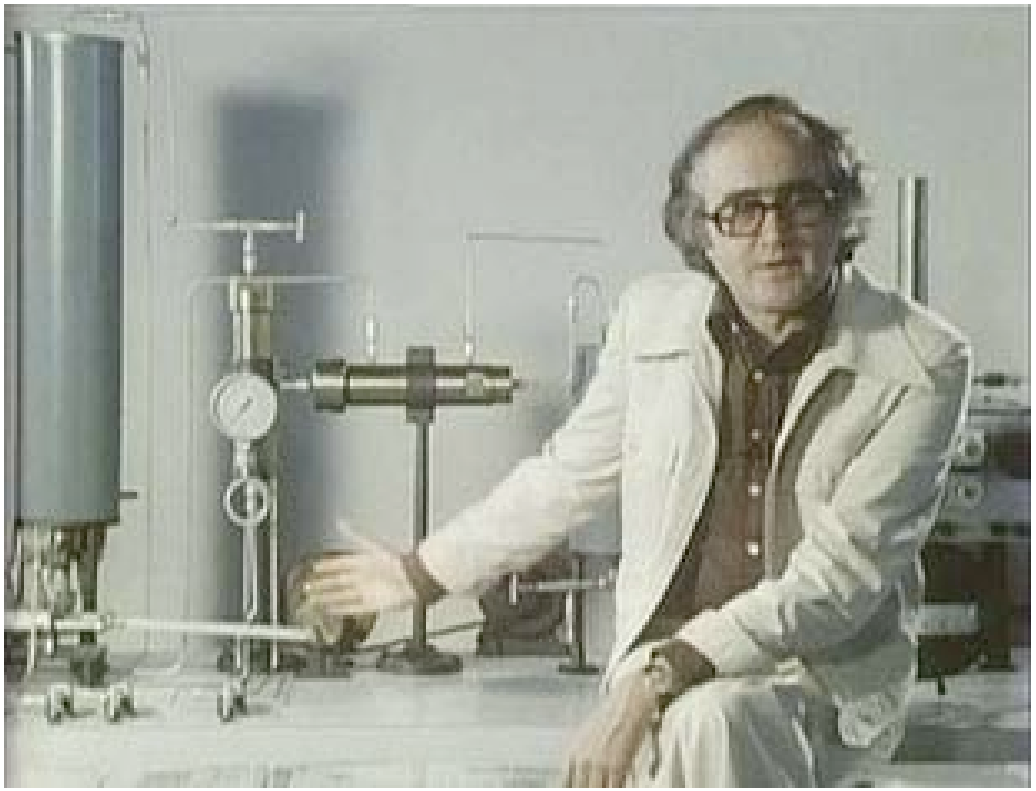
http://ambassadormann.deviantart.com/art/Steampunk-Goggles-number-2-127699287

Prologue: 1979

"Why should we look to the past in order to prepare for the future? Because there is nowhere else to look."

James Burke,

Connections



http://upload.wikimedia.org/wikipedia/en/archive/2/2e/20130124220825!James_Burke_%28historian%29.jpg

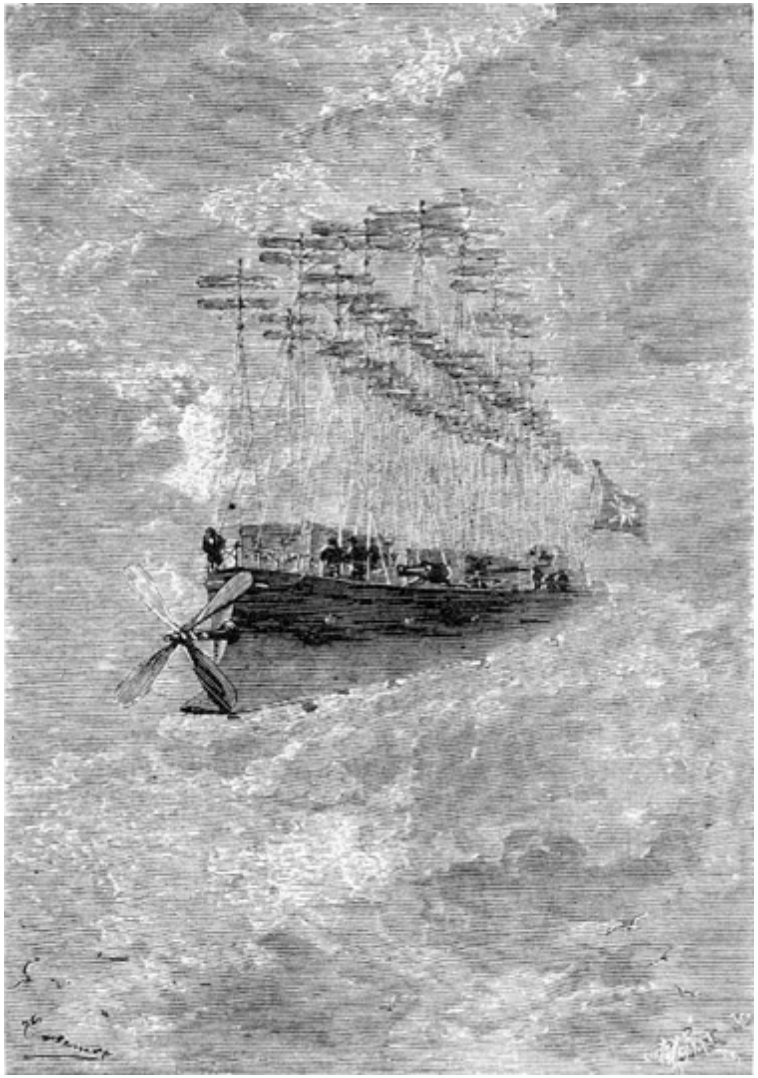
Prologue: 1878

http://en.wikipedia.org/wiki/File:F%C3%A9lix_Nadar_1820-1910_portraits_Jules_Verne_%28restoration%29.jpg

Prologue: 1886

http://en.wikipedia.org/wiki/File:%27Robur_the_Conqueror%27_by_L%C3%A9on_Benett_01.jpg

Prologue: 1886



http://upload.wikimedia.org/wikipedia/commons/3/3d/%27Robur_the_Conqueror%27_by_L%C3%A9on_Benett_14.jpg

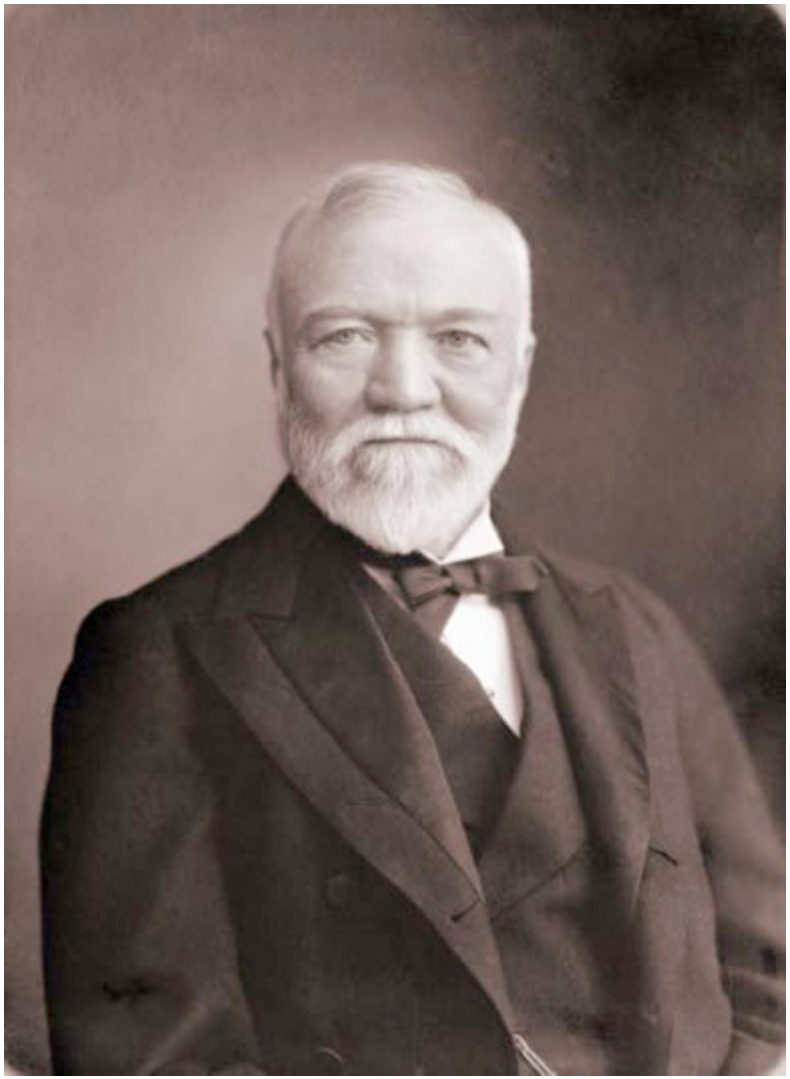
Prologue: 1890

http://en.wikipedia.org/wiki/File:Daniel_Burnham_c1890.jpeg

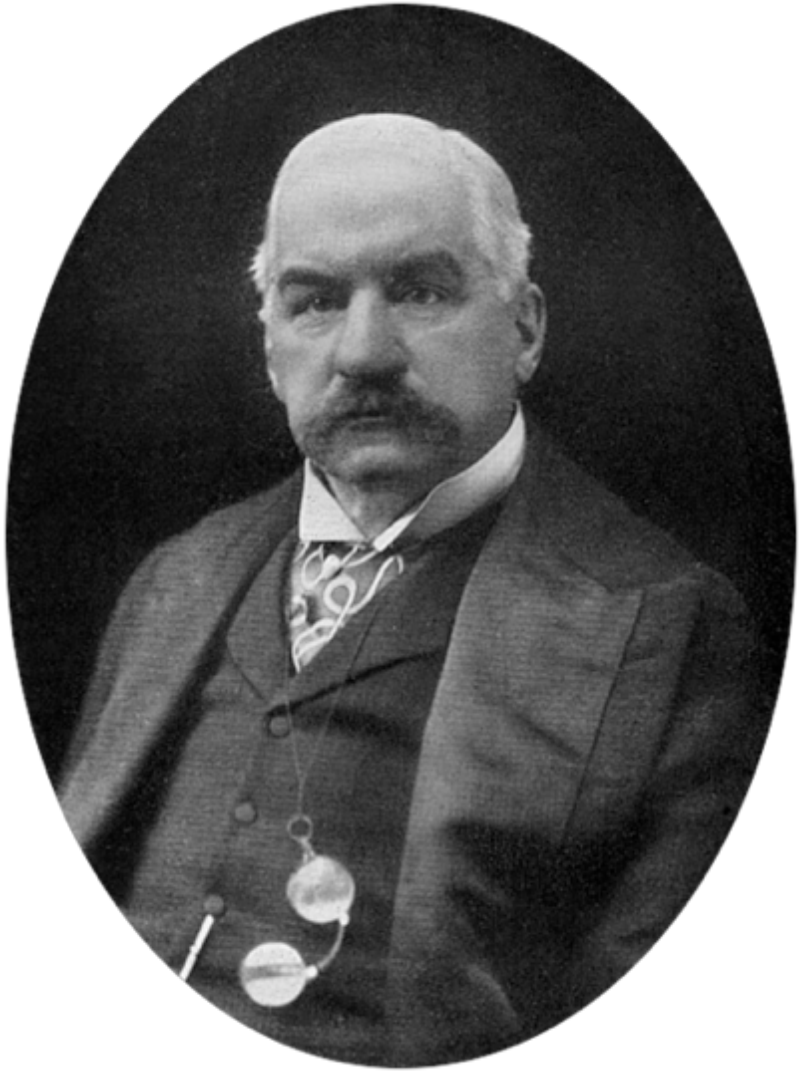
Prologue: 1893

http://www.bc.edu/bc_org/avp/cas/fnart/fa267/1893/1893_02.jpg

Prologue: 1900

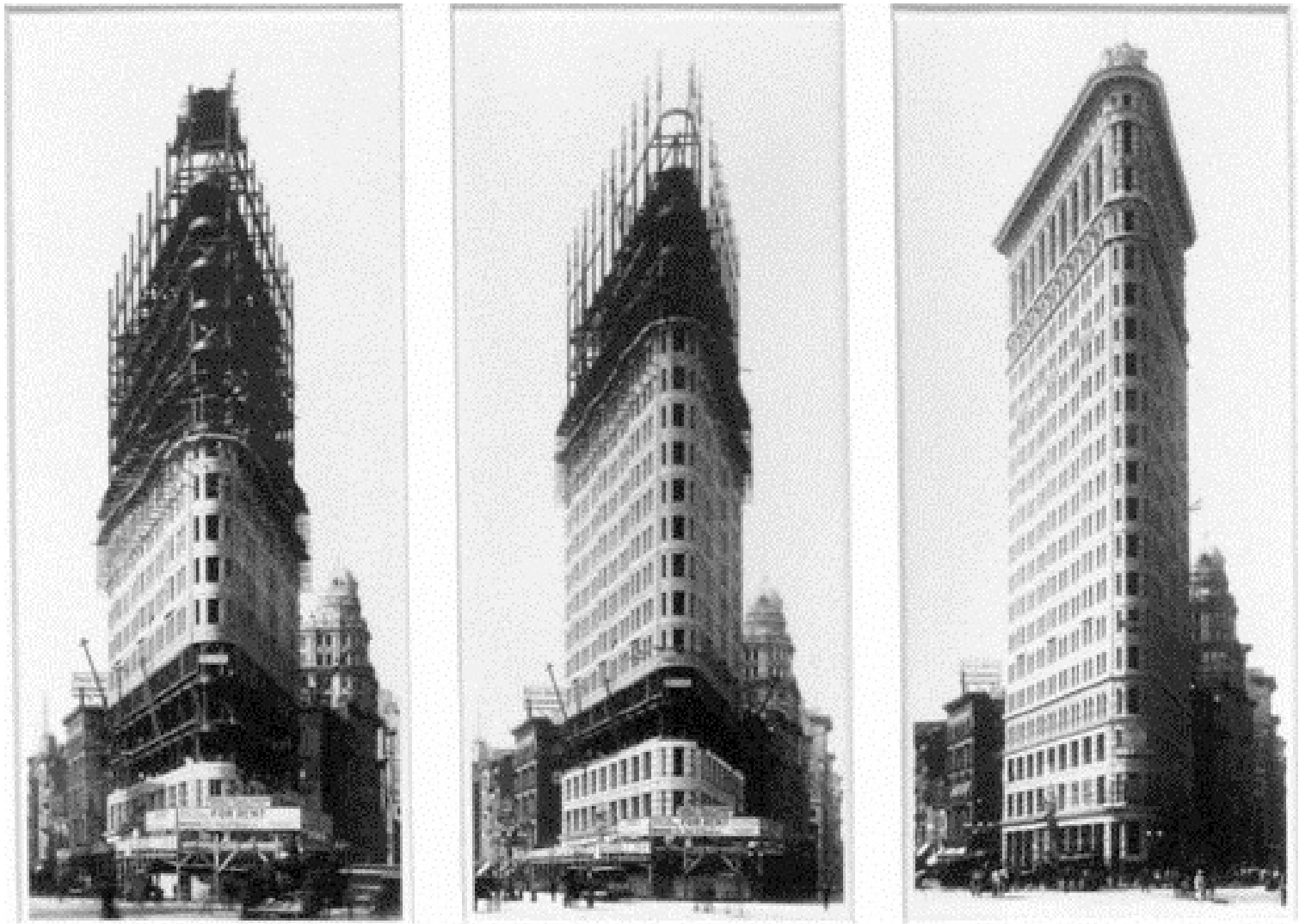


http://explorepahistory.com/displayimage.php?imgId=1-2-A46



http://en.wikipedia.org/wiki/File:JohnPierpontMorgan.png

1901-1902



http://en.wikipedia.org/wiki/File:Flatiron_Building_Construction,_New_York_Times_-_Library_of_Congress,_1901-1902_crop.JPG

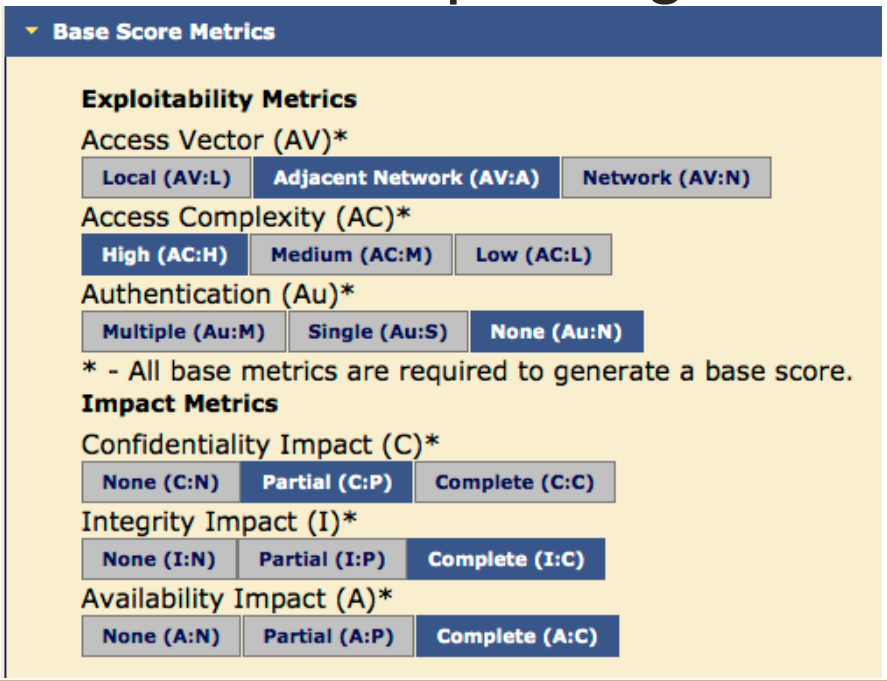
1902

Dropping 40kDay

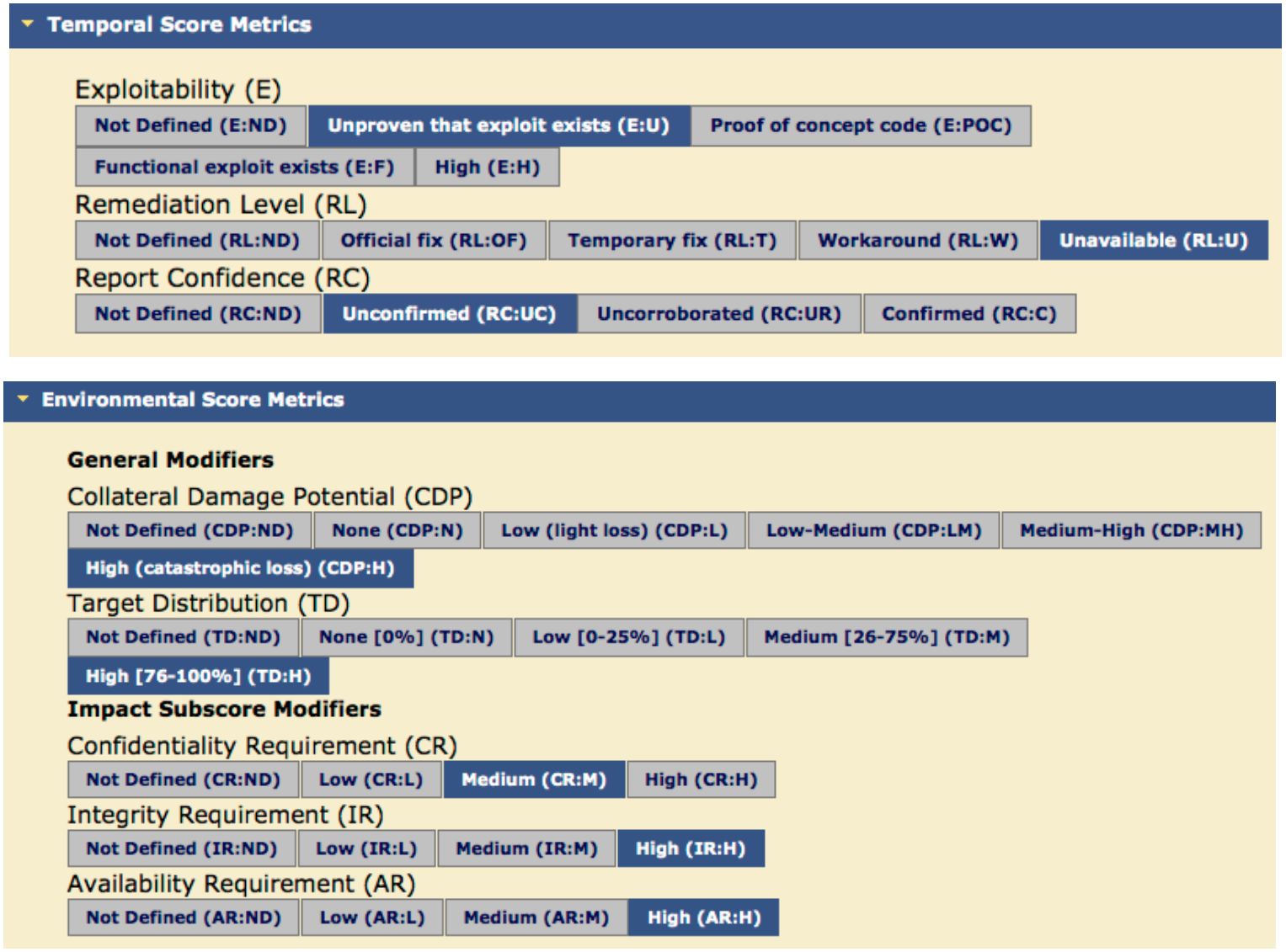
The Flat Iron Building in New York City is vulnerable to denial of service or complete system destruction due to inadequate defenses against the kinetic and chemical energy of 315,000 lbs of aluminum containing 16,000 gallons of kerosene impacting at 500 mph.

CVSS Base Score: 6.5

(AV:A/AC:H/Au:N/C:P/I:C/A:C)



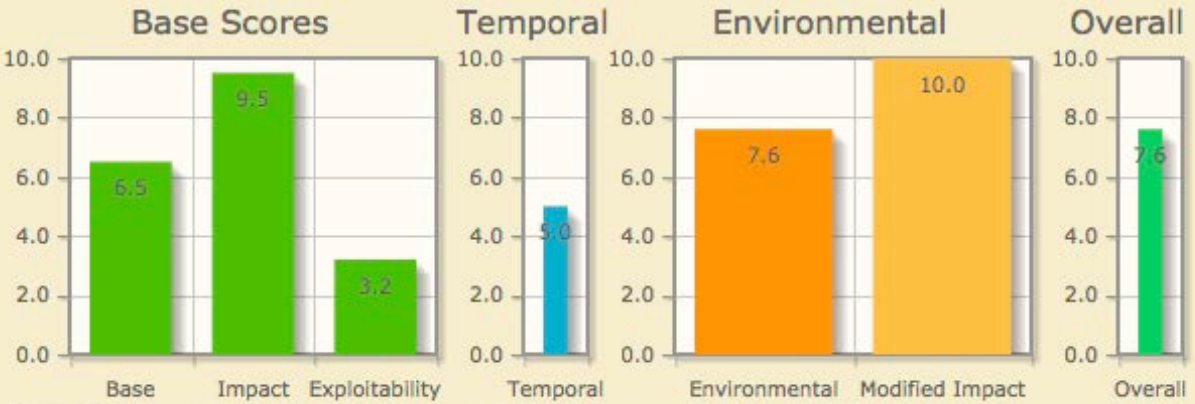
CVSS v2 1902


Temporal Score Metrics
Exploitability (E)
Not Defined (E:ND)
Unproven that exploit exists (E:U)
Proof of concept code (E:POC)
Functional exploit exists (E:F)
High (E:H)
Remediation Level (RL)
Not Defined (RL:ND)
Official fix (RL:OF)
Temporary fix (RL:T)
Workaround (RL:W)
Unavailable (RL:U)
Report Confidence (RC)
Not Defined (RC:ND)
Unconfirmed (RC:UC)
Uncorroborated (RC:UR)
Confirmed (RC:C)
Environmental Score Metrics
General Modifiers
Collateral Damage Potential (CDP)
Not Defined (CDP:ND)
None (CDP:N)
Low (light loss) (CDP:L)
Low-Medium (CDP:LM)
Medium-High (CDP:MH)
High (catastrophic loss) (CDP:H)
Target Distribution (TD)
Not Defined (TD:ND)
None [0%] (TD:N)
Low [0-25%] (TD:L)
Medium [26-75%] (TD:M)
High [76-100%] (TD:H)
Impact Subscore Modifiers
Confidentiality Requirement (CR)
Not Defined (CR:ND)
Low (CR:L)
Medium (CR:M)
High (CR:H)
Integrity Requirement (IR)
Not Defined (IR:ND)
Low (IR:L)
Medium (IR:M)
High (IR:H)
Availability Requirement (AR)
Not Defined (AR:ND)
Low (AR:L)
Medium (AR:M)
High (AR:H)

CVSS v2 1902

Common Vulnerability Scoring System Version 2 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score	**6.5**
Impact Subscore	9.5
Exploitability Subscore	3.2
CVSS Temporal Score	**5**
CVSS Environmental Score	**7.6**
Modified Impact Subscore	10
Overall CVSS Score	**7.6**

Show Equations

CVSS v2 Vector (AV:A/AC:H/Au:N/C:P/I:C/A:C/E:U/RL:U/RC:UC/CDP:H/TD:H/CR:M/IR:H/AR:H)

Base Score Metrics

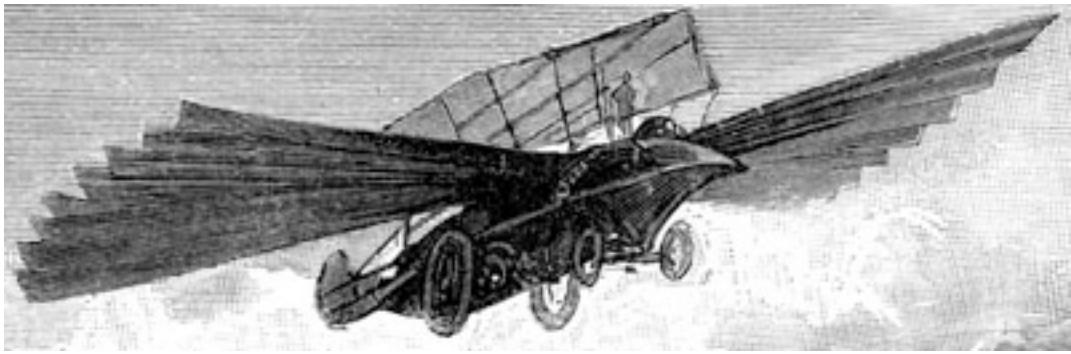
http://nvd.nist.gov/cvss.cfm?calculator&version=2&vector=(AV:A/AC:H/Au:N/C:P/I:C/A:C/E:U/RL:U/RC:UC/CDP:H/TD:H/CR:M/IR:H/AR:H)

1903

http://en.wikipedia.org/wiki/File:First_flight2.jpg

1904

http://en.wikipedia.org/wiki/Master_of_the_World_%28novel%29



http://www.julesverne.ca/images/book/illustratrations/Maitre%20du%20Monde_image%20epouvante%20over%20niagara_detail.jpg

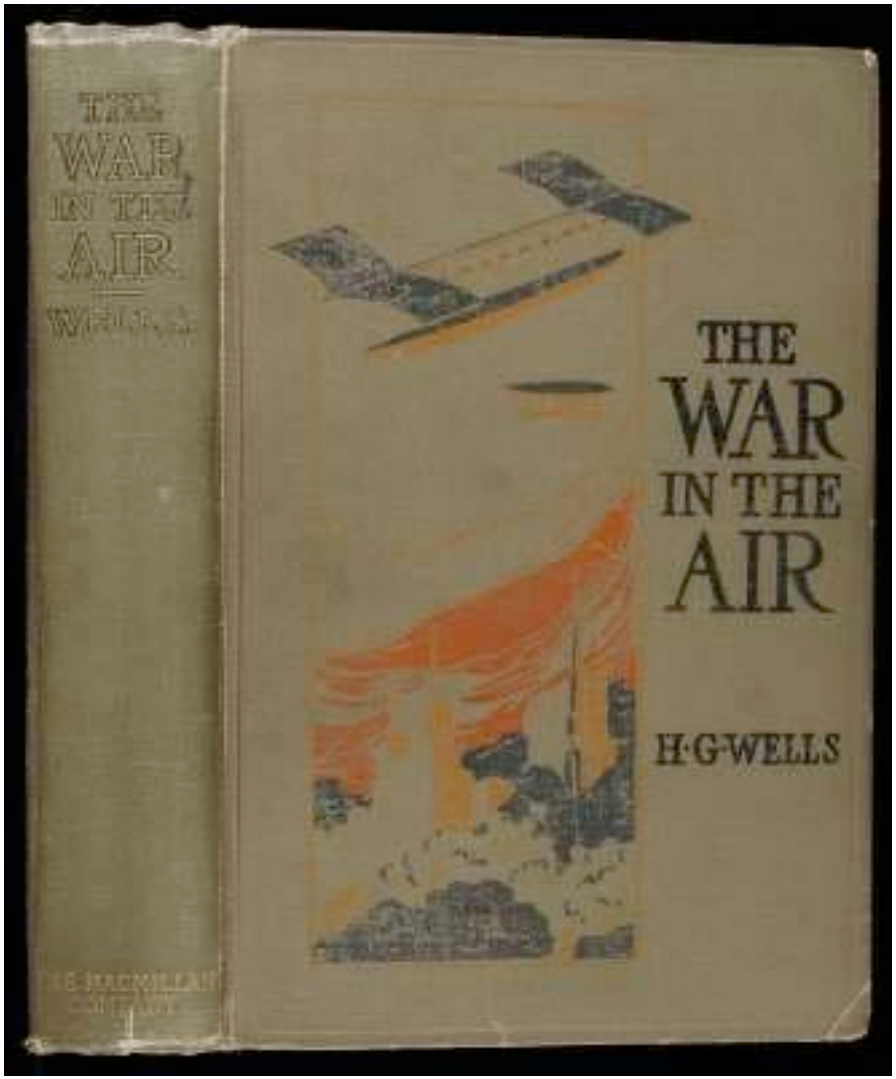
1906

I found myself agape, admiring a sky-scraper, the prow of the Flat-iron Building, to be particular, ploughing up through the traffic of Broadway and Fifth Avenue in the afternoon light.

H.G. Wells, 1906

http://en.wikipedia.org/wiki/File:H_G_Wells_-_Sandgate_-_Project_Gutenberg_eText_13715.png

1908



1915

http://www.pinterest.com/pin/432275264204090218/

Shortly thereafter

http://ephemeralnewyork.files.wordpress.com/2009/08/flatironbuildingpostcard.jpg

1918

http://en.wikipedia.org/wiki/File:Hannover_CL_IIIa,_Forest_of_Argonne,_France,_1918_%28restored%29.jpg

1939

http://en.wikipedia.org/wiki/File:B-25G_Mitchell,_AAF_TAC_Center,_Florida_-_040315-F-9999G-005.jpg

1939

http://www.nationalmuseum.af.mil/shared/media/photodb/photos/060720-F-1234P-001.jpg

1943

http://en.wikipedia.org/wiki/File:Lulu-Belle_af.jpg

1945

http://en.wikipedia.org/wiki/File:Empirestate540.jpg

The view from here

1946


VOL. XCV No. 32,259.

PLANE HITS WALL ST. TOWER;
5 IN ARMY CRAFT ARE KILLED;
BIG HOLE TORN IN 58TH FLOOR

PILOT LOST IN FOG

Route to Newark
om the South—Wac
Officer a Victim

DEBRIS FALLS

SCENE OF PLANE CRASH LAST NIGHT

http://images.rarenewspapers.com/ebayimgs/5.5.2010/image028.jpg

CVSS v2 1946

Temporal Score Metrics

Exploitability (E)

Not Defined (E:ND) | Unproven that exploit exists (E:U | Proof of concept code (E:POC) | Functional exploit exists (E:F) | High (E:H)

Remediation Level (RL)

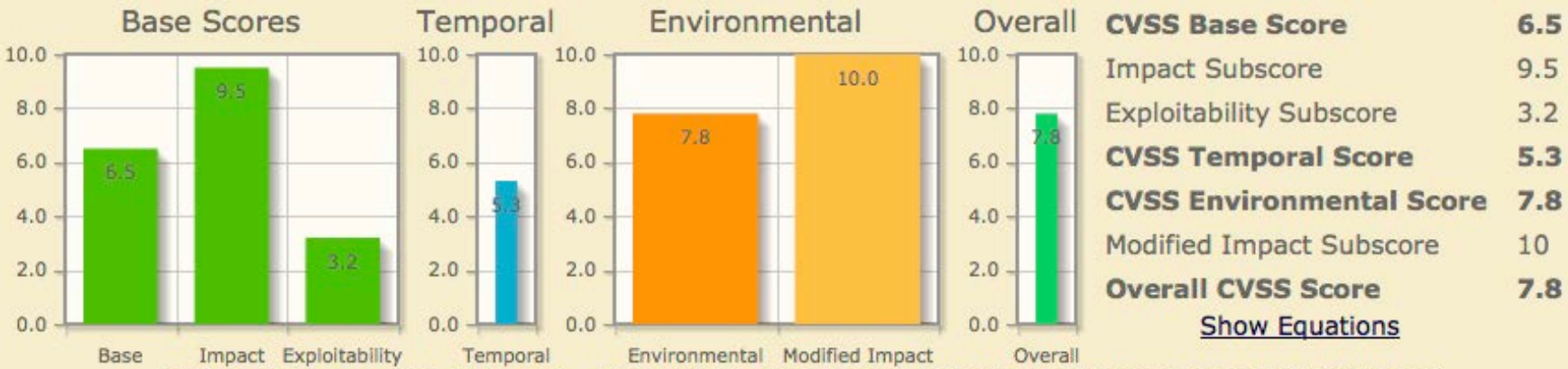
Not Defined (RL:ND) | Official fix (RL:OF) | Temporary fi (RL:T) | Workaround (RL:W) | Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:ND) | Unconfirmed (RC:C) | Uncorroborated (RC:UR) | Confirmed (RC:C)

Common Vulnerability Scoring System Version 2 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score	**6.5**
Impact Subscore	9.5
Exploitability Subscore	3.2
CVSS Temporal Score	**5.3**
CVSS Environmental Score	**7.8**
Modified Impact Subscore	10
Overall CVSS Score	**7.8**

Show Equations

CVSS v2 Vector (AV:A/AC:H/Au:N/C:P/I:C/A:C/E:POC/RL:W/RC:UR/CDP:H/TD:H/CR:M/IR:H/AR:H)

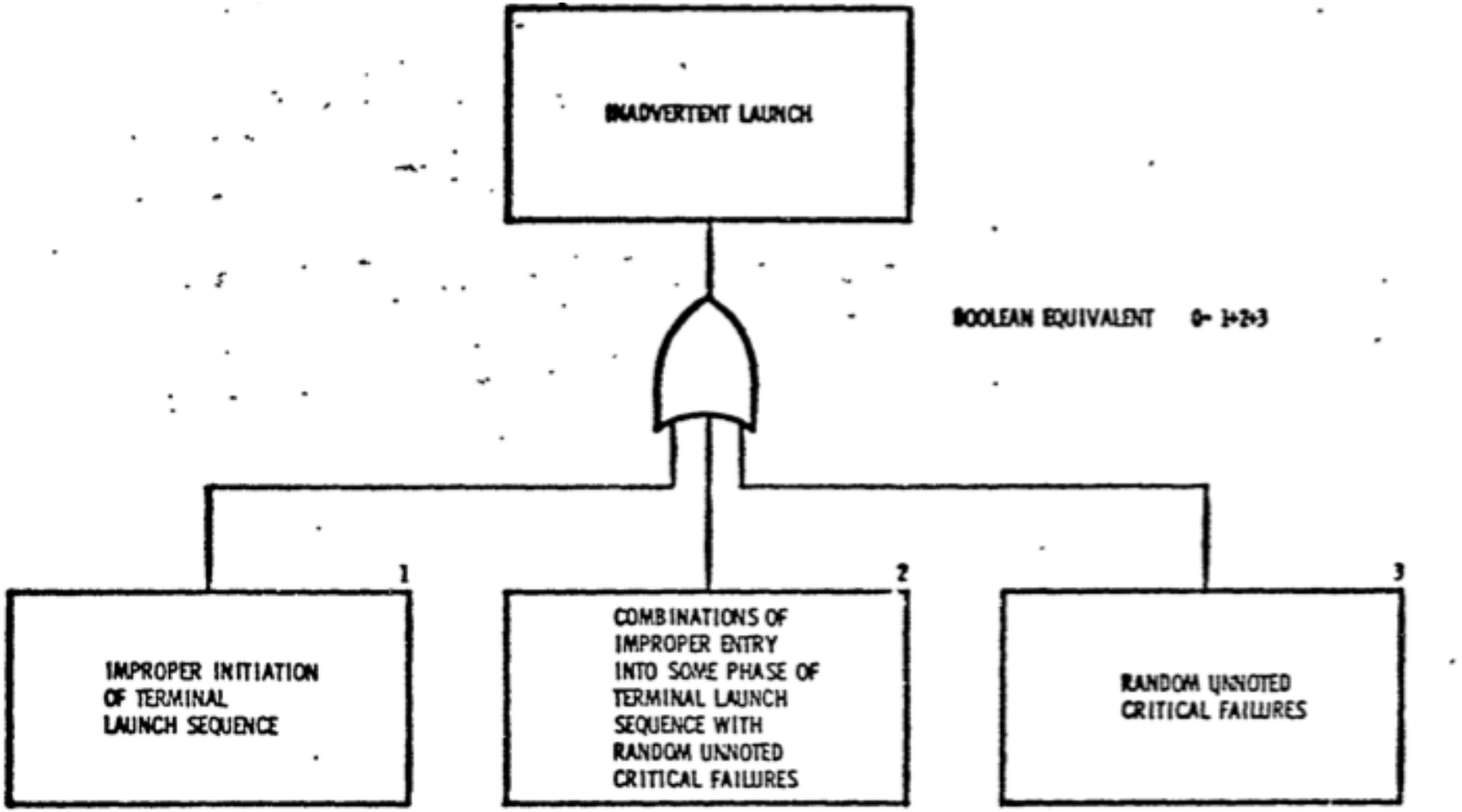
Disclaiming Responsibility for the Fire
(Verses 1-4 go here)

http://eil.com/shop/moreinfo.asp?catalogid=76681

1962

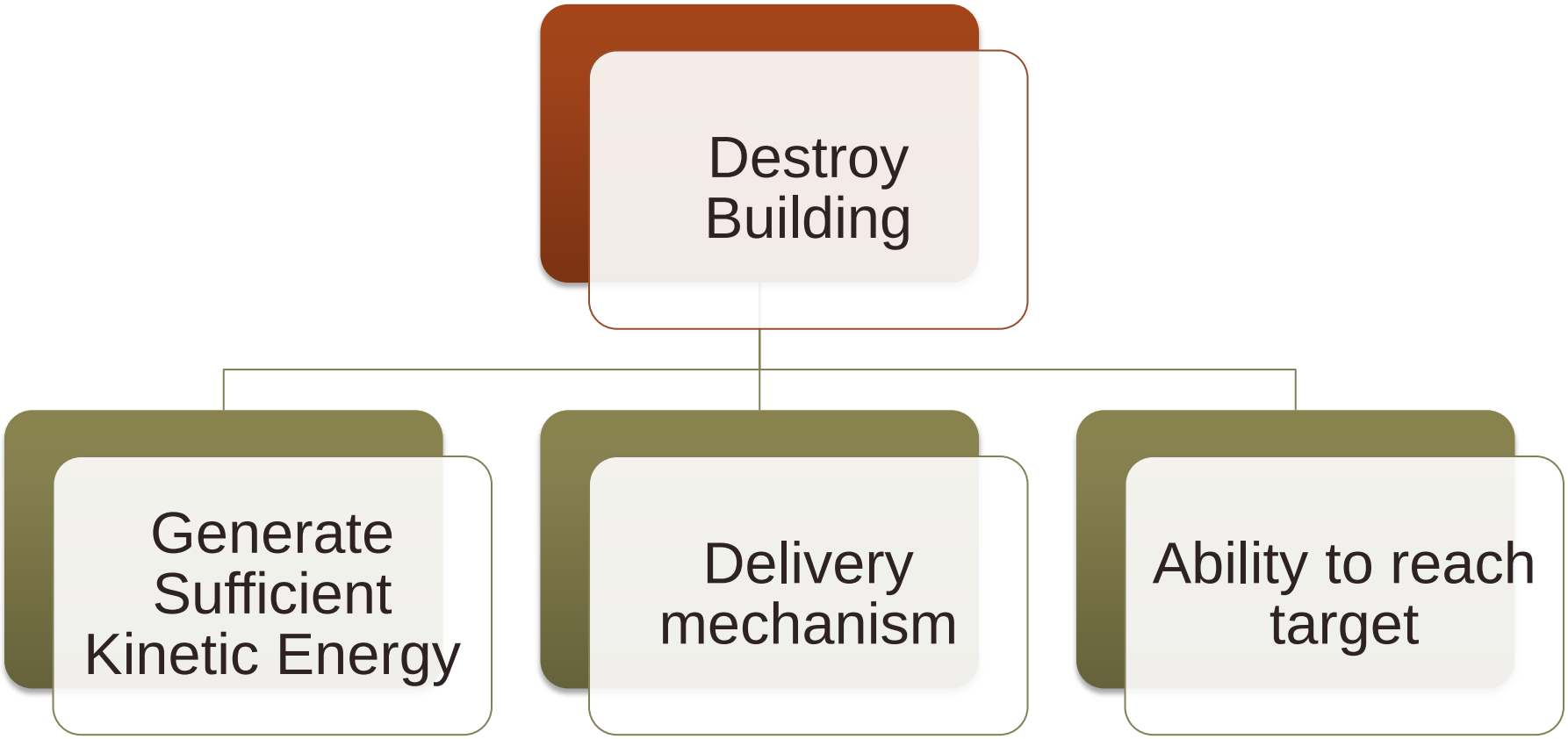
http://en.wikipedia.org/wiki/LGM-30_Minuteman#mediaviewer/File:Minuteman_I.jpg

1963

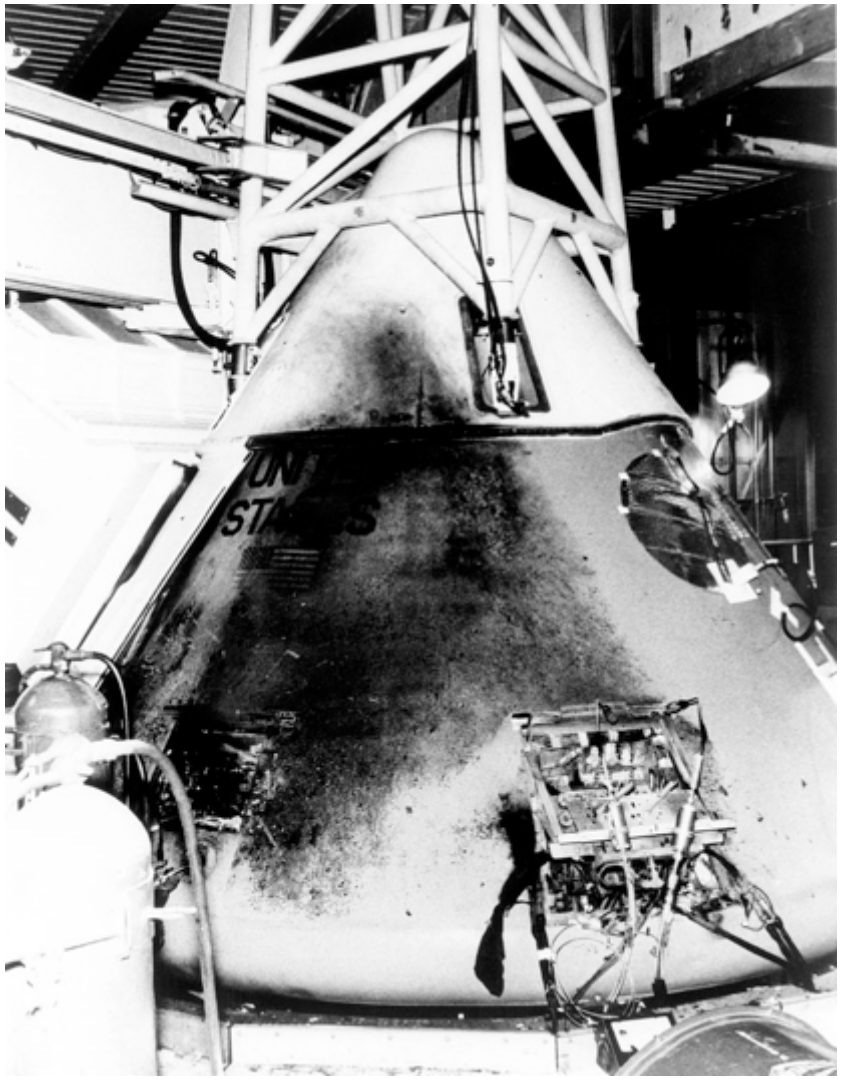


http://www.dtic.mil/get-tr-doc/pdf?AD=AD0299561

Basic attack tree

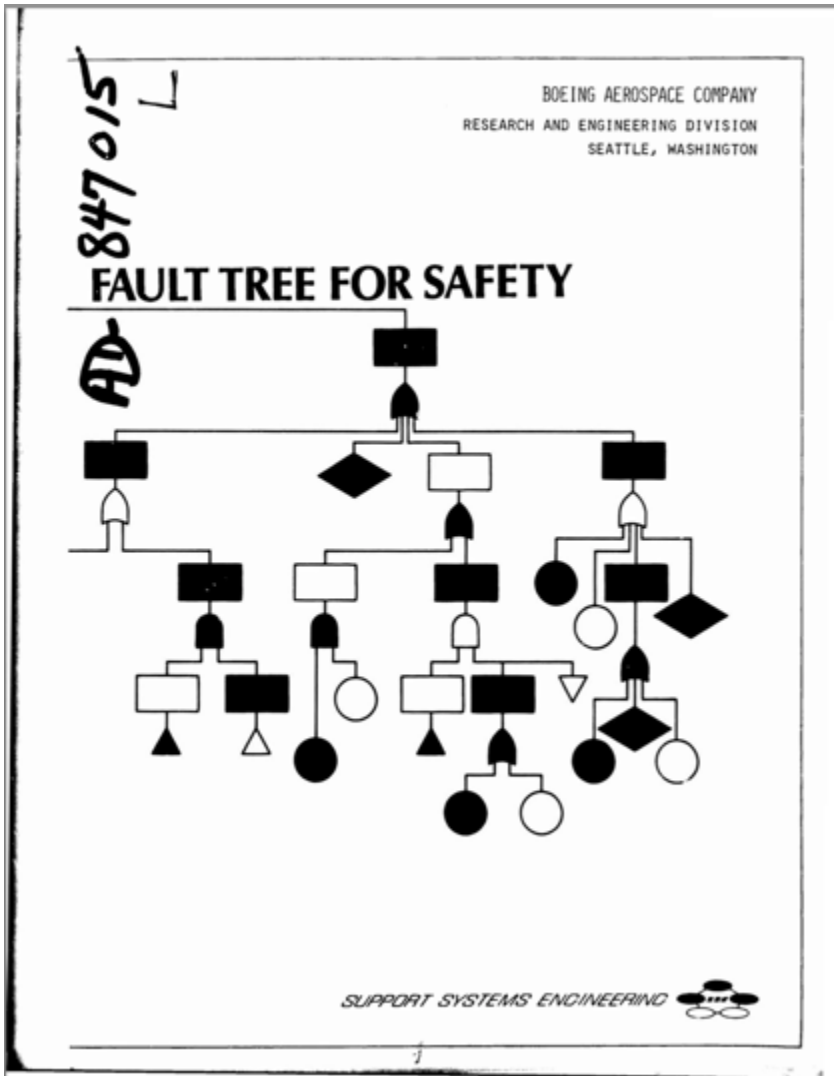


1967



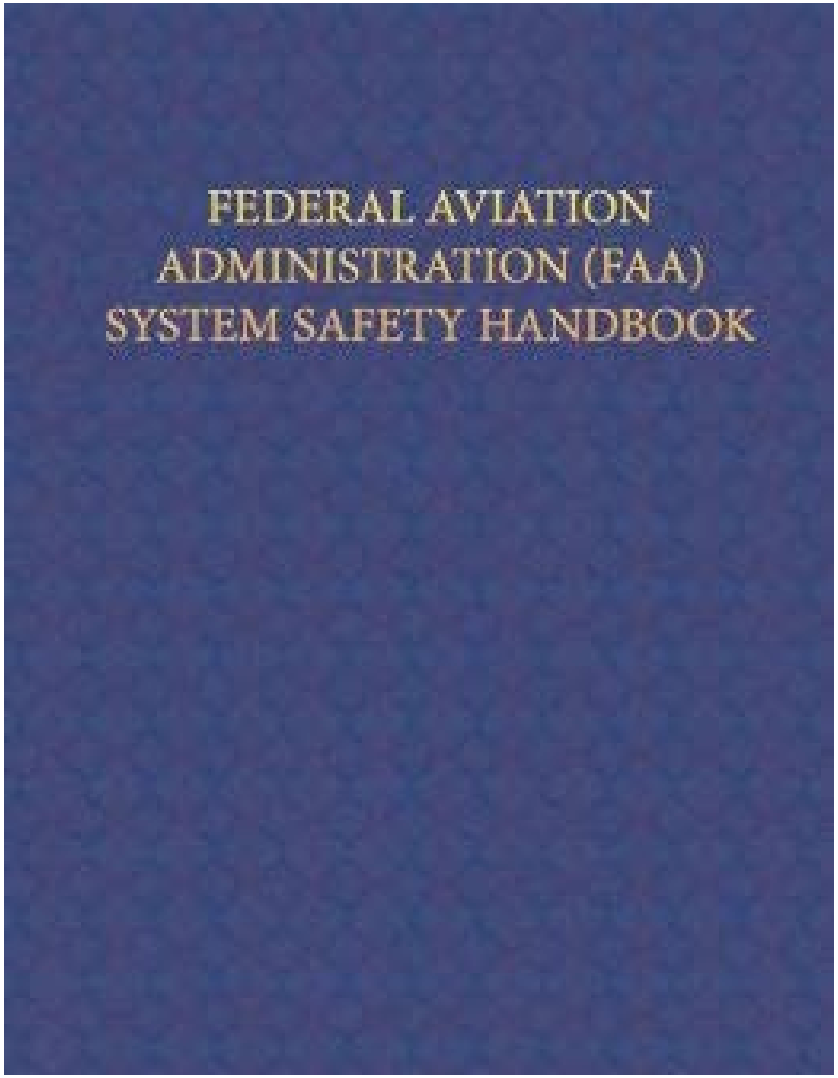
http://en.wikipedia.org/wiki/Apollo_1#mediaviewer/File:Apollo_1%27s_Command_Module_-_GPN-2003-00057.jpg

1968



http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=AD0847015

1970



http://www.barnesandnoble.com/w/federal-aviation-administration-system-safety-handbook-federal-aviation-administration/1118719983

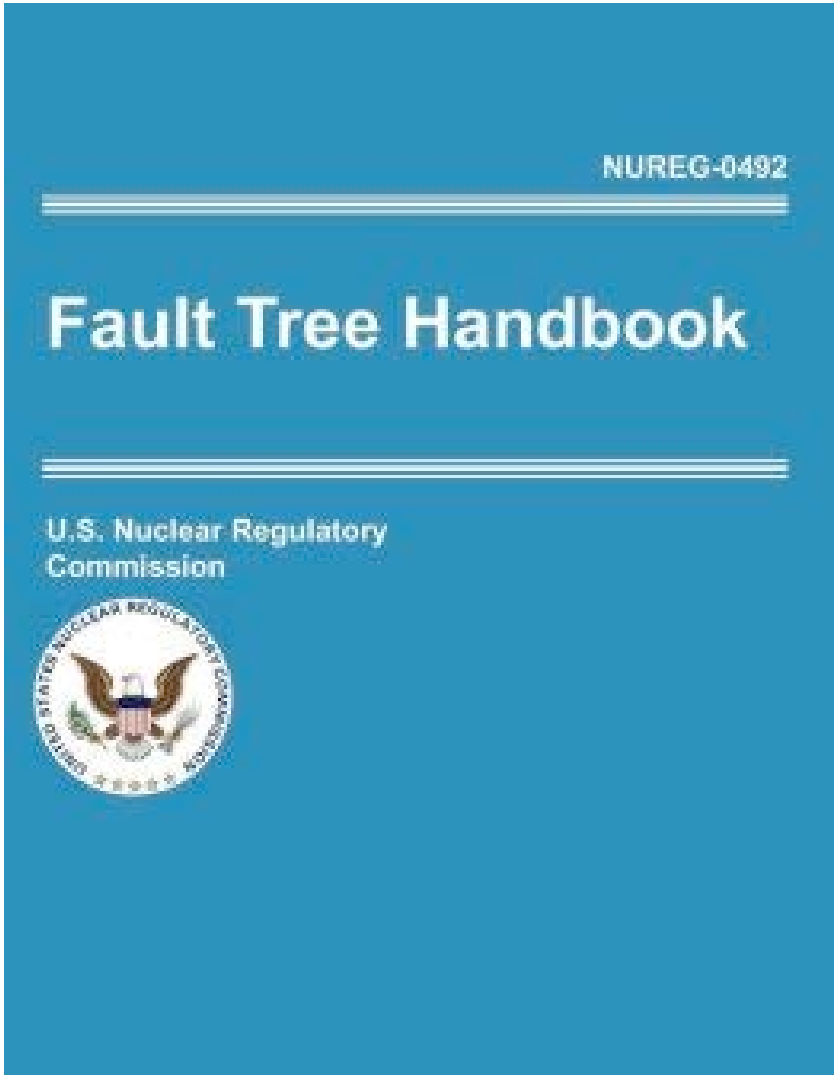
1978

http://www.boeing.com/boeing/commercial/767family/

1979

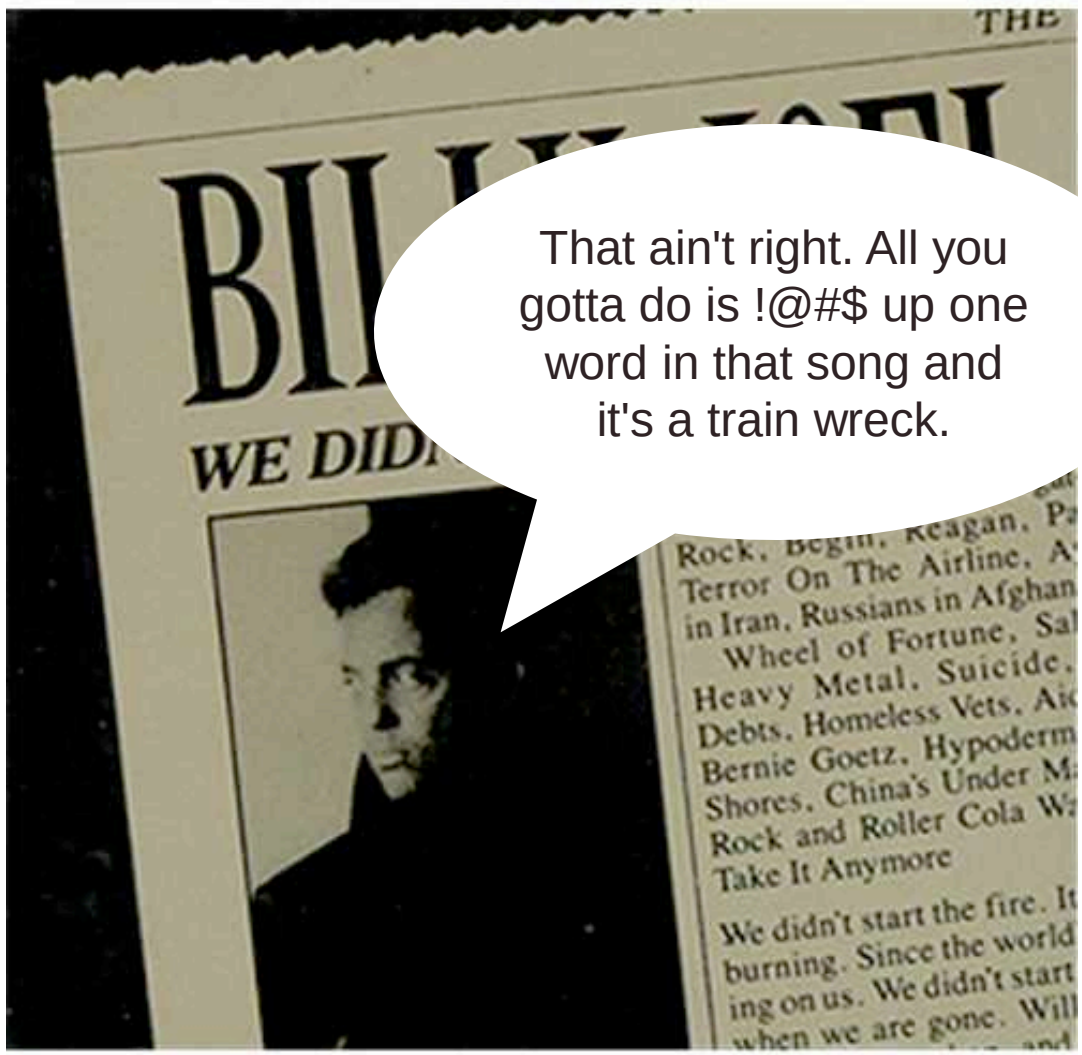
http://phil.cdc.gov/phil/details.asp?pid=1194

1981



http://www.barnesandnoble.com/w/fault-tree-handbook-us-nuclear-regulatory-commission/1113865485

Rock and Roller Cola Wars…



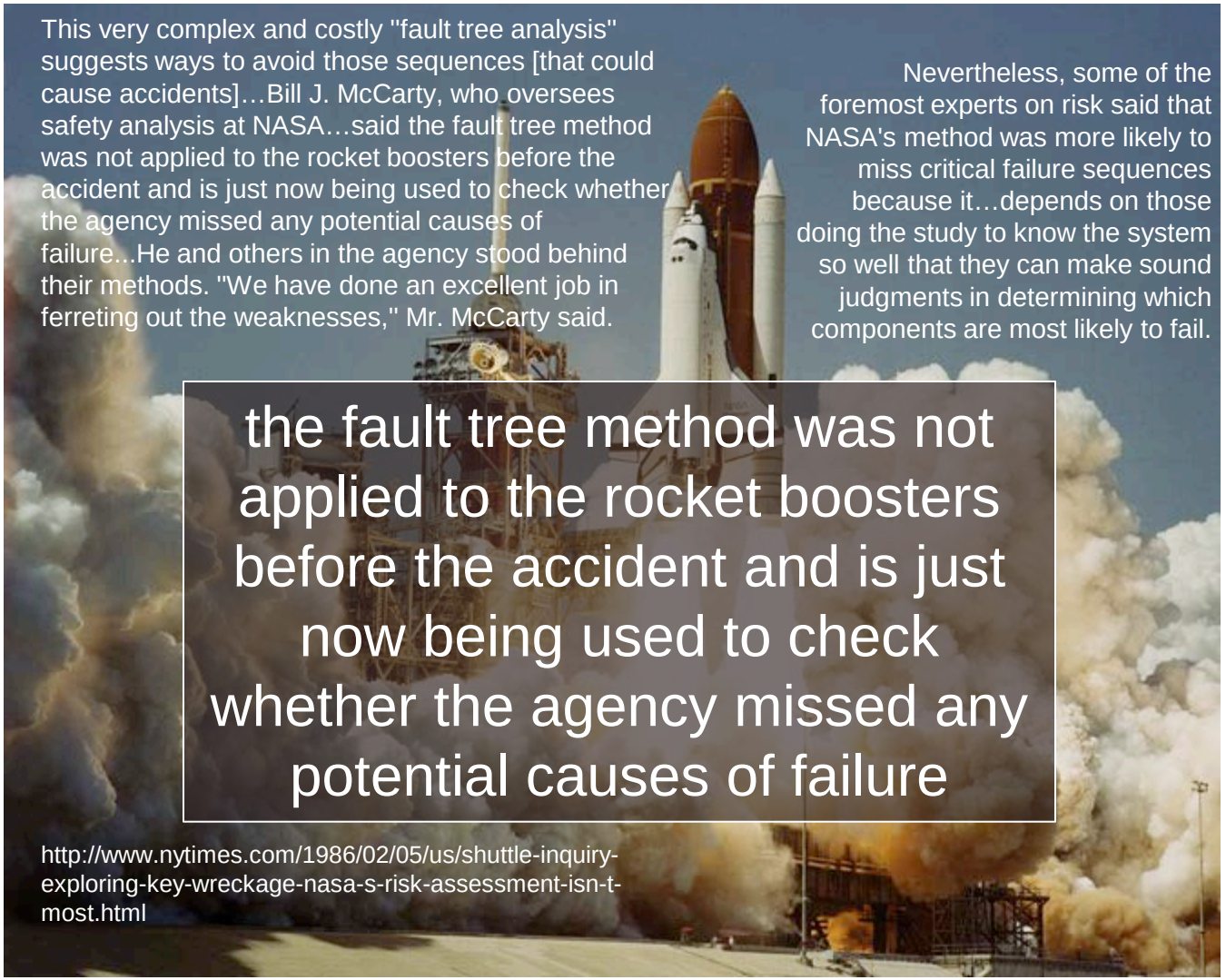
http://eil.com/shop/moreinfo.asp?catalogid=76681

http://www.rollingstone.com/music/videos/watch-billy-joel-forget-the-lyrics-to-we-didnt-start-the-fire-20140314

1984

http://www.bhopal.net/what-happened-in-bhopal/

1986

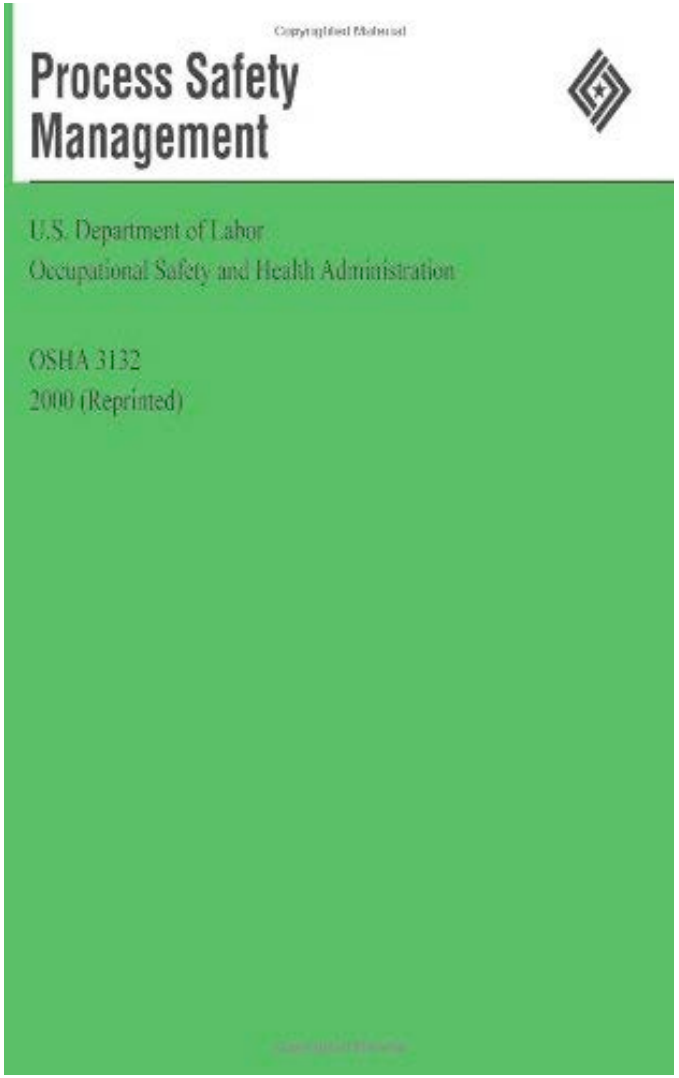


http://commons.wikimedia.org/wiki/File:Space_Shuttle_Challenger_(04-04-1983).JPEG

1988

http://firesafetynation.com/images/2%281%29.jpg http://i.dailymail.co.uk/i/pix/2013/07/06/article-0-1A8FAA3F000005DC-107_634x769.jpg

1992



http://www.amazon.com/Process-Safety-Management-Department-Labor/dp/1478114207

1999

Attack Trees

Dr. Dobb's Journal December 1999

Modeling security threats

By Bruce Schneier

Few people truly understand computer security, as illustrated by computer-security company marketing literature that touts "hacker proof software," "triple-DES security," and the like. In truth, unbreakable security is broken all the time, often in ways its designers never imagined. Seemingly strong cryptography gets broken, too. Attacks thought to be beyond the ability of mortal men become commonplace. And as newspapers report security bug after security bug, it becomes increasingly clear that the term "security" doesn't have meaning unless also you know things like "Secure from whom?" or "Secure for how long?"

Clearly, what we need is a way to model threats against computer systems. If we can understand all the different ways in which a system can be attacked, we can likely design countermeasures to thwart those attacks. And if we can understand who the attackers are -- not to mention their abilities, motivations, and goals -- maybe we can install the proper countermeasures to deal with the real threats.

Enter Attack Trees

Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks. Basically, you represent attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes.

https://www.schneier.com/paper-attacktrees-ddj-ft.html

2001

"This technical note describes and illustrates an approach for documenting attack information in a structured and reusable form.

We expect that security analysts can use this approach to document and identify commonly occurring attack patterns, and that information system designers and analysts can use these patterns to develop more survivable information systems."

Technical Note
CMU/SEI-2001-TN-001

Attack Modeling for Information Security and Survivability

Andrew P. Moore
Robert J. Ellison
Richard C. Linger

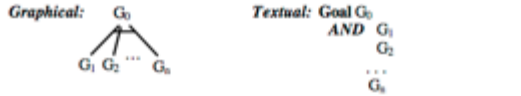
March 2001

2.1 Structure and Semantics

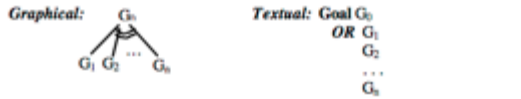
We decompose a node of an attack tree either as

- a set of attack sub-goals, all of which must be achieved for the attack to succeed, that are represented as an AND-decomposition, or
- a set of attack sub-goals, any one of which must be achieved for the attack to succeed, that are represented as an OR-decomposition.

Attack trees can be represented graphically or textually. We represent an AND-decomposition as follows:



This represents a goal G_0 that can be achieved if the attacker achieves each of G_1 through G_n. We represent an OR-decomposition similarly:



This represents a goal G_0 that can be achieved if the attacker achieves any one of G_1 through G_n. Generally we use the textual representation in this paper, since the graphical representation tends to be awkward for non-trivial attack trees.

2001

http://en.wikipedia.org/wiki/File:World_Trade_Center,_New_York_City_-_aerial_view_%28March_2001%29.jpg

CVSS v2 2001

Temporal Score Metrics

Exploitability (E)

Not Defined (E:ND) | Unproven that exploit exists (E:U) | Proof of concept code (E:POC) | **Functional exploit exists (E:F)** | High (E:H)

Remediation Level (RL)

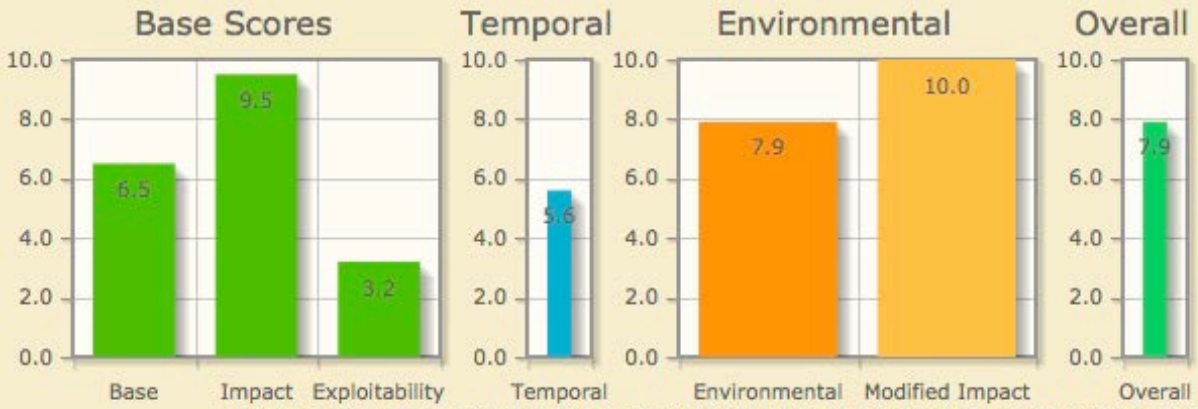
Not Defined (RL:ND) | Official fix (RL:OF) | **Temporary fix (RL:T)** | Workaround (RL:W) | Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:ND) | Unconfirmed (RC:UC) | Uncorroborated (RC:UR) | **Confirmed (RC:C)**

Common Vulnerability Scoring System Version 2 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score	**6.5**
Impact Subscore	9.5
Exploitability Subscore	3.2
CVSS Temporal Score	**5.6**
CVSS Environmental Score	**7.9**
Modified Impact Subscore	10
Overall CVSS Score	**7.9**

Show Equations

CVSS v2 Vector (AV:A/AC:H/Au:N/C:P/I:C/A:C/E:F/RL:T/RC:C/CDP:H/TD:H/CR:M/IR:H/AR:H)

2002

http://www.afhso.af.mil/shared/media/photodb/photos/110802-D-LN615-001.jpg http://www.afhso.af.mil/topics/factsheets/factsheet.asp?id=18593

CVSS v2 2002

Temporal Score Metrics

Exploitability (E)

Not Defined (E:ND)	Unproven that exploit exists (E:U)	Proof of concept code (E:POC)	Functional exploit exists (E:F)	High (E:H)

Remediation Level (RL)

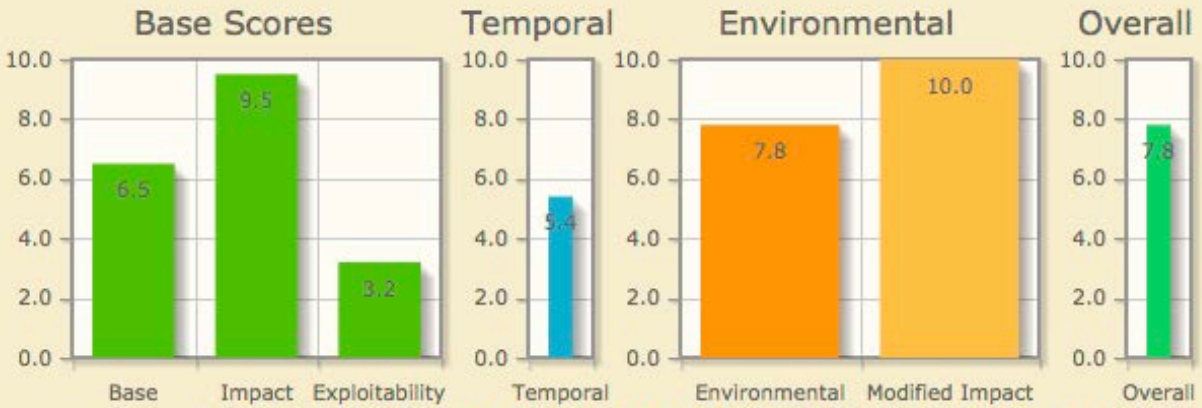
Not Defined (RL:ND)	Official fix (RL:OF)	Temporary fix (RL:T)	Workaround (RL:W)	Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:ND)	Unconfirmed (RC:UC)	Uncorroborated (RC:UR)	Confirmed (RC:C)

Common Vulnerability Scoring System Version 2 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score	**6.5**
Impact Subscore	9.5
Exploitability Subscore	3.2
CVSS Temporal Score	**5.4**
CVSS Environmental Score	**7.8**
Modified Impact Subscore	10
Overall CVSS Score	**7.8**

Show Equations

CVSS v2 Vector (AV:A/AC:H/Au:N/C:P/I:C/A:C/E:F/RL:OF/RC:C/CDP:H/TD:H/CR:M/IR:H/AR:H)

2003

Veterans of the Challenger experience say that it sounds cautious and logical to argue that all potential causes of the disaster should be examined and eliminated, one by one. Ron D. Dittemore, the shuttle program manager, made that argument again today, saying that he would construct a "fault tree," and that the question of whether insulating foam fatally damaged the heat-shedding tiles would be one branch of that tree.

http://www.nytimes.com/2003/02/07/us/loss-shuttle-search-for-answers-learning-lessons-challenger-inquiry.html

…would construct a "fault tree," and that the question of whether insulating foam fatally damaged the heat-shedding tiles would be one branch of that tree.

http://static.ddmcdn.com/gif/shuttle-columbia-launch-660x433-130201-1.jpg

2009: NASA on Fault Tree Analysis

Fault Tree Analysis (FTA) is one of the most important logic and probabilistic techniques used in Probability Risk Assessment (PRA) and system reliability assessment today. PRA and its underlying techniques, including FTA, has become a useful and respected methodology for safety assessment. Because of its logical, systematic and comprehensive approach, PRA and FTA have been repeatedly proven **capable of uncovering design and operational weaknesses that escaped even some of the best** deterministic safety and engineering experts.

http://www.hq.nasa.gov/office/codeq/software/ComplexElectronics/techniques/fault-tree.htm

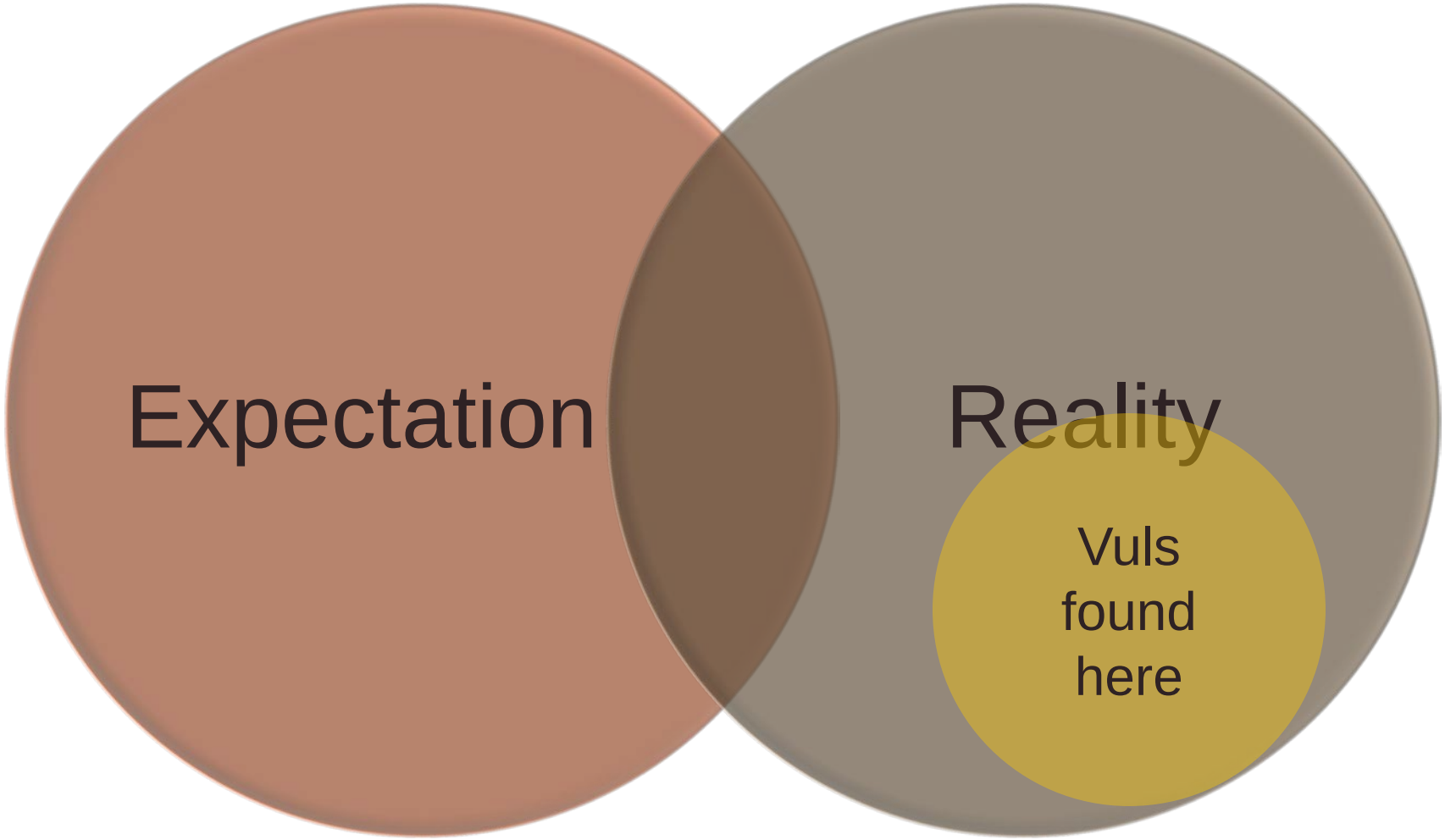
2012: MS Blog on Attack Tree Analysis

"The problem is that attack trees quickly became rather complex. A full attack tree often has hundreds of different paths you can take, making it **difficult to follow visually**. Determining the classification of a threat from attack trees is also far **too labor-intensive**…While the concept of attack trees is sound, the application of this approach is far from it."

The Evolution of Elevation: Threat Modeling in a Microsoft World

- January 17, 2012, Dana Epp, Microsoft MVP - Enterprise and Developer Security
  http://technet.microsoft.com/en-us/security/hh778966.aspx

Vulnerability Discovery



Build security in?

At what stage in the process should the Flat Iron Building developers have incorporated defenses against 500+mph airplanes filled with jet fuel?

How harshly should we judge those who declined to defend against threats that science fiction had barely begun to explore when the system was deployed?

Vulnerabilities can arise because the world changes around the system…

…even if the system itself remains unchanged.

2014

The trendline in the count of critical monocultures seems to be rising and most of these are embedded systems both without a remote management interface and long lived. That combination -- **long lived and not reachable** -- is the trend that must be dealt with, possibly even reversed.

- *Dan Geer, speaking @ NSA on 3/26/14*

Points to ponder

How long will your next refrigerator last?

How about your next car?

http://www.toyota.com/entune/entune-app-suite/prius/

http://corporate.ford.com/news-center/press-releases-detail/ford-acquires-software-company-livio-to-further-advance-in-car-c

Points to ponder

How about your light bulbs?

What's in the Box

Three hue light bulbs; wireless bridge; power adapter; 2-meter Ethernet networ

Specifications

Concentrate	Tested in schools to a tone and brightness that'll keep you t
Bulbs	E26 contact medium screw base fitting, 9 watts; A19 form t
Light output	16 million colors; all shades of white; dimming via RF to 5 p
Lumen output	600 lm @ 4000K; 510 lm @ 3000K; 360 lm @ 2000K; 550 efficacy @ 4000K
Bridge	Supports 50 bulbs per bridge; ZigBee LightLink Protocol 1.0; 2400 - 2483.5 MHz frequency band; desktop or wall mount; measures 3.93 inches in diameter and 0.98 inches tall
Startup	Less than 2 seconds from AC power; less than 0.5 seconds from standby
iOS support	iPhone (3GS, 4, 4S, 5); iPad (1, 2, 3rd generation, 4th generation); iPad mini; iPod touch (4th
	8.9
Warranty	2 years

d and alert

15,000 hours of lifetime use

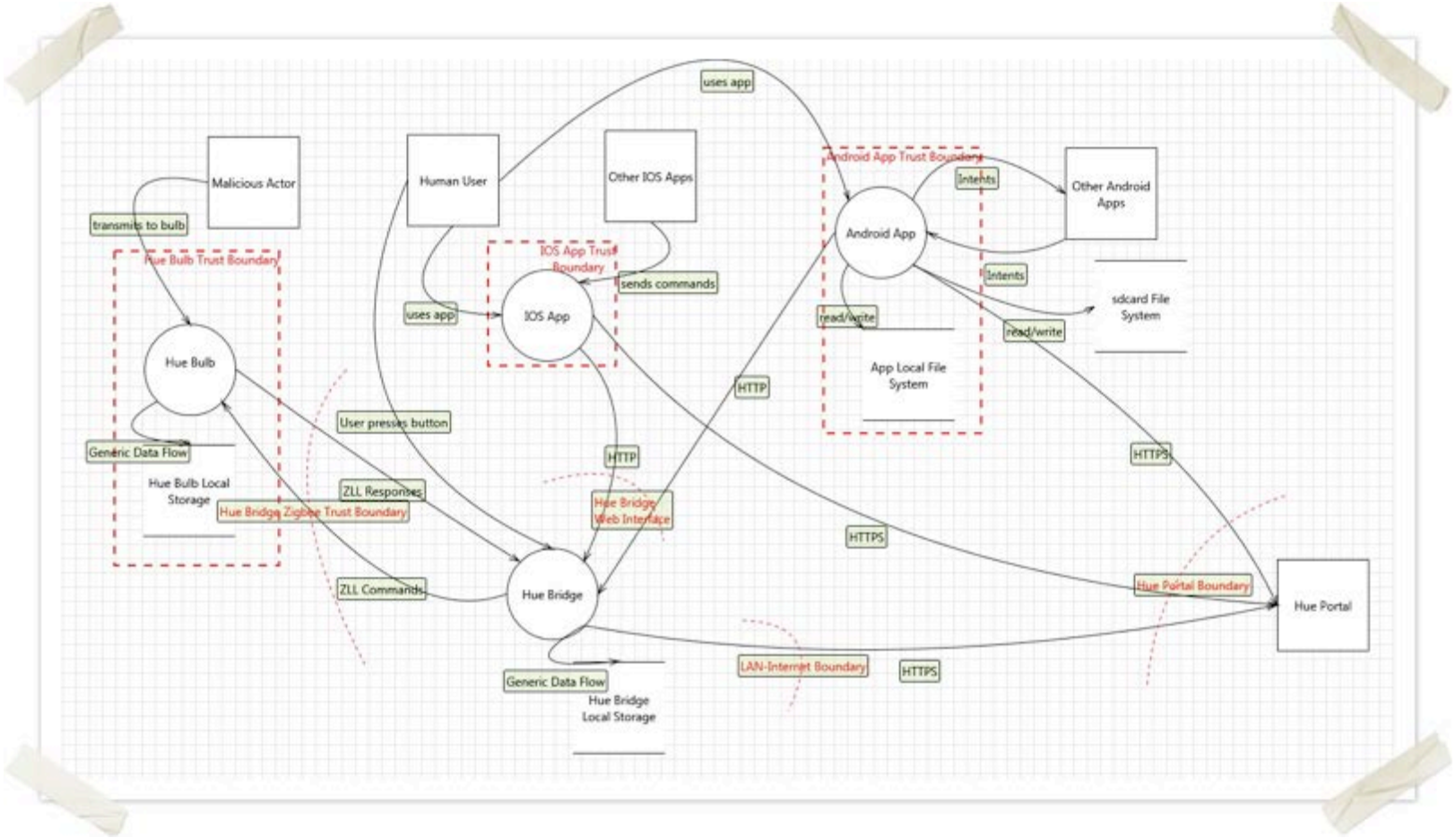
t (no external dimmer)

Note, Galaxy Note 2, Galaxy Ace 2, Galaxy Tablet
HTC One X, Kindle Fire, Kindle Fire HD, Kindle Fire HD

$$\frac{15{,}000\,hrs}{4\,hrs\,/\,day} \approx 10\,years$$

Points to ponder

How long will you be able to get patches for them?



Points to ponder

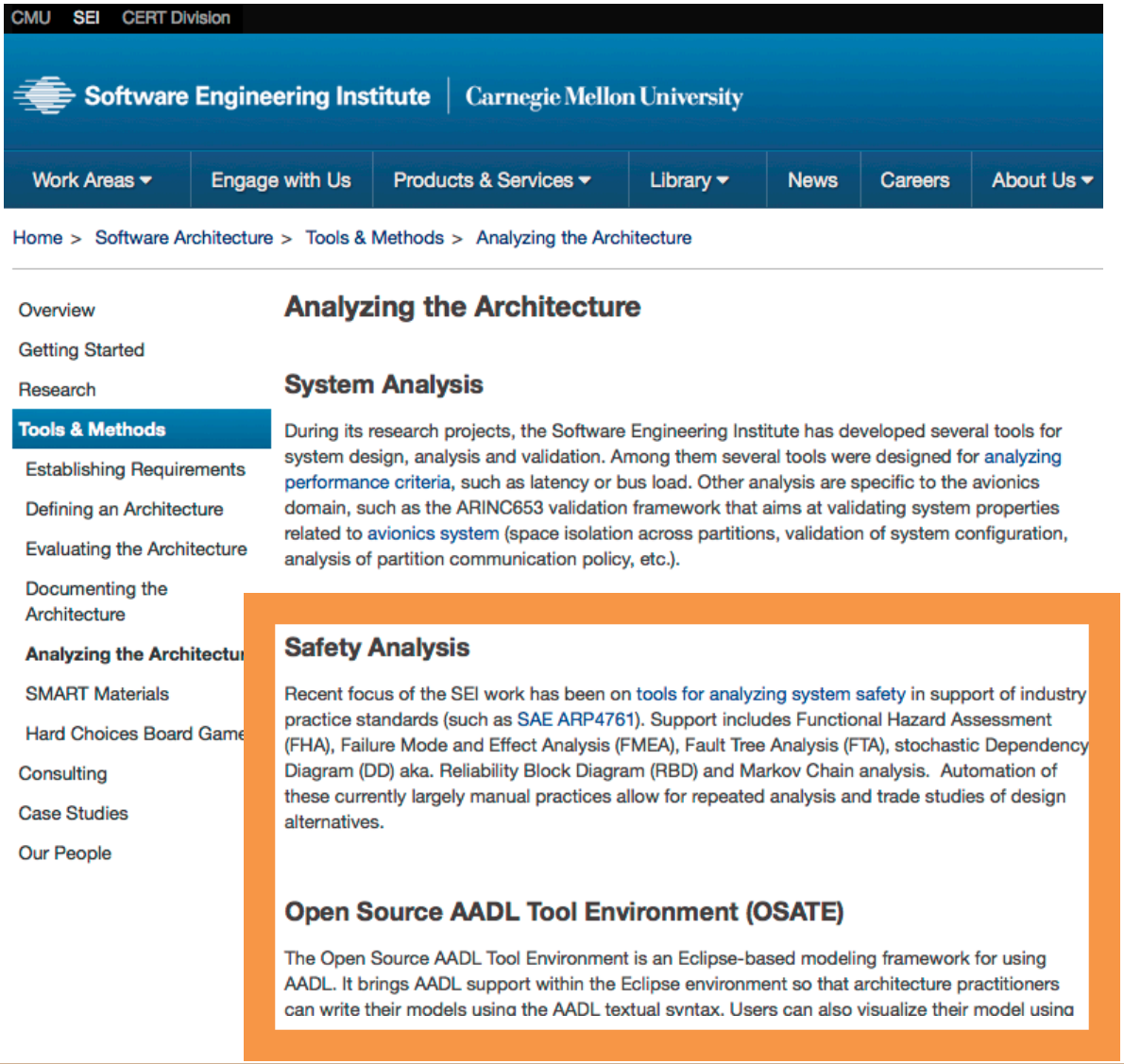
Defense mechanisms

- Field upgradability
- Layered defenses
- Planned obsolescence
- Read more Science Fiction

Design for adaptability to environments that become more hostile over time

Threat modeling and attack tree analysis still have a lot to learn from safety analysis, incl. fault trees

2014


CMU SEI CERT Division
Software Engineering Institute | Carnegie Mellon University
Work Areas
Engage with Us
Products & Services
Library
News
Careers
About Us
Home > Software Architecture > Tools & Methods > Analyzing the Architecture
Overview
Getting Started
Research
Tools & Methods
Establishing Requirements
Defining an Architecture
Evaluating the Architecture
Documenting the Architecture
Analyzing the Architectur
SMART Materials
Hard Choices Board Game
Consulting
Case Studies
Our People
Analyzing the Architecture
System Analysis
During its research projects, the Software Engineering Institute has developed several tools for system design, analysis and validation. Among them several tools were designed for analyzing performance criteria, such as latency or bus load. Other analysis are specific to the avionics domain, such as the ARINC653 validation framework that aims at validating system properties related to avionics system (space isolation across partitions, validation of system configuration, analysis of partition communication policy, etc.).
Safety Analysis
Recent focus of the SEI work has been on tools for analyzing system safety in support of industry practice standards (such as SAE ARP4761). Support includes Functional Hazard Assessment (FHA), Failure Mode and Effect Analysis (FMEA), Fault Tree Analysis (FTA), stochastic Dependency Diagram (DD) aka. Reliability Block Diagram (RBD) and Markov Chain analysis. Automation of these currently largely manual practices allow for repeated analysis and trade studies of design alternatives.
Open Source AADL Tool Environment (OSATE)
The Open Source AADL Tool Environment is an Eclipse-based modeling framework for using AADL. It brings AADL support within the Eclipse environment so that architecture practitioners can write their models using the AADL textual syntax. Users can also visualize their model using

Related work at CERT

Systemic Vulnerability Program (ongoing)

- Extend focus from vulnerabilities within a single application or program to encompass those that may affect a wide range of applications, networks, and systems.
  - Emerging domain outreach, tool development.
  - Supply chain vulnerabilities (CRDb)

Vulnerability Discovery Research (ongoing)

Extending AADL for Security Design Assurance of the Internet of Things Research (2014-2015)

This talk inspired by…

KC-135s from the 171st Air Refueling Wing often circle the Pittsburgh area. From the perspective of my office at CMU looking out at the view seen here, the planes usually fly right above or behind the Cathedral of Learning.

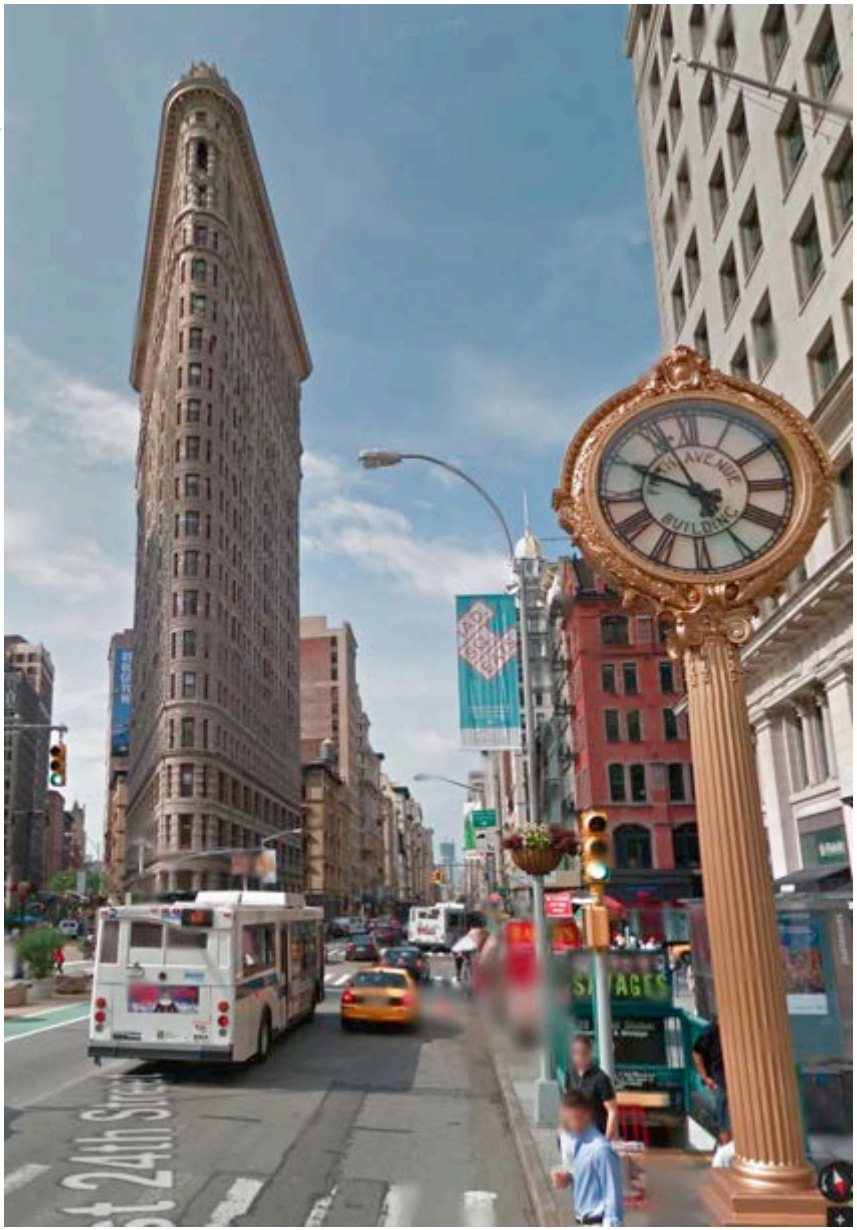
Construction of the Cathedral of Learning was started in 1926. The KC-135 didn't enter service until 1957.

Why didn't Pitt address this vulnerability in design?

http://www.wingsoverpittsburgh.com/Airshow2010/pics/Kc135FlyingDirty.jpg

"What are you going to make your future of, for all your airs?" And then I suppose I shall return to crane my neck at the Flat-Iron Building or the Times sky scraper, and ask all that too, an identical question.

H.G. Wells, 1906



http://archive.org/stream/hgwellsfuture00wellrich/hgwellsfuture00wellrich_djvu.txt

Google Maps Street View, 2014