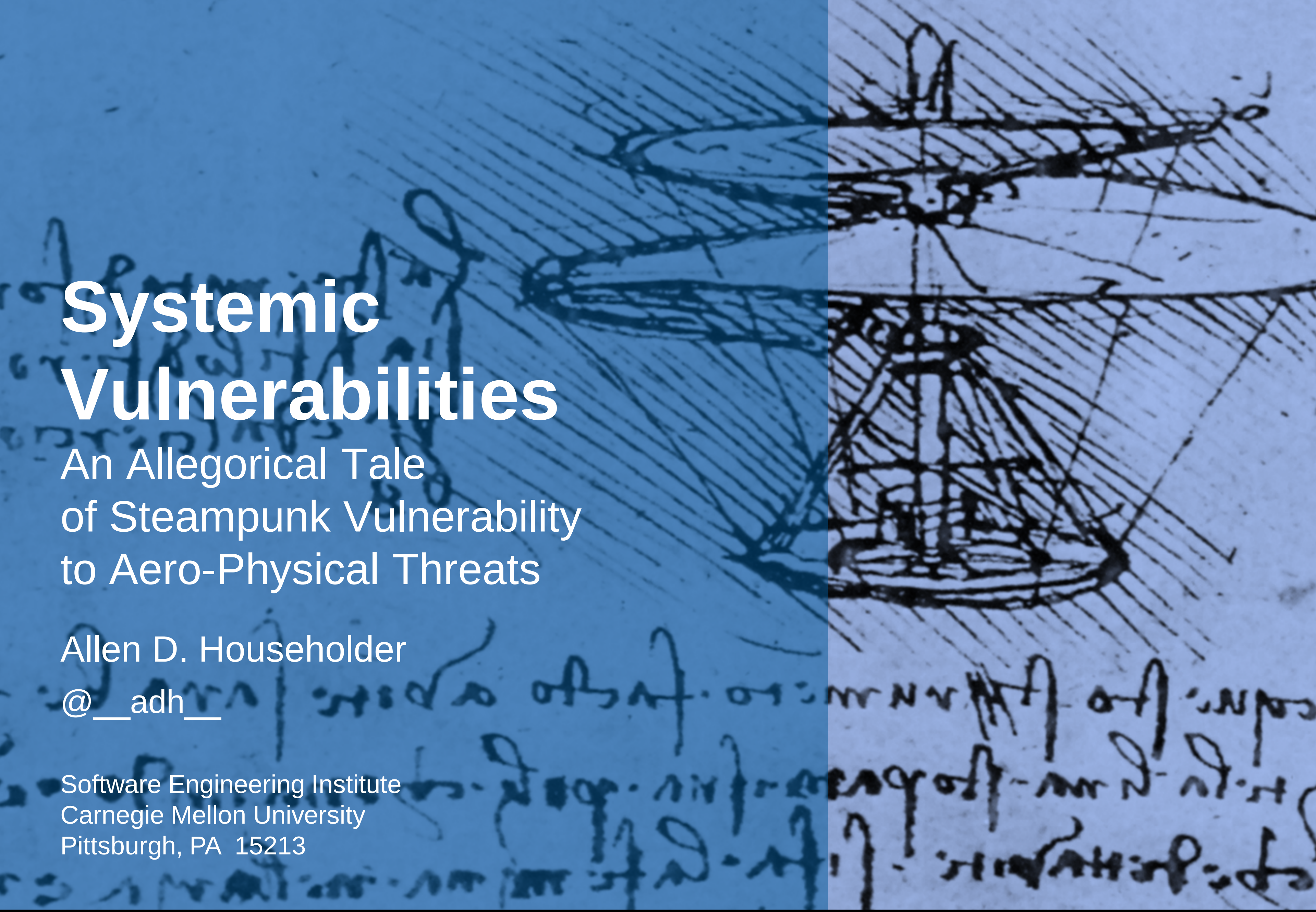


Systemic Vulnerabilities

An Allegorical Tale of Steampunk Vulnerability to Aero-Physical Threats

Allen D. Householder

@__adh__

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0001744

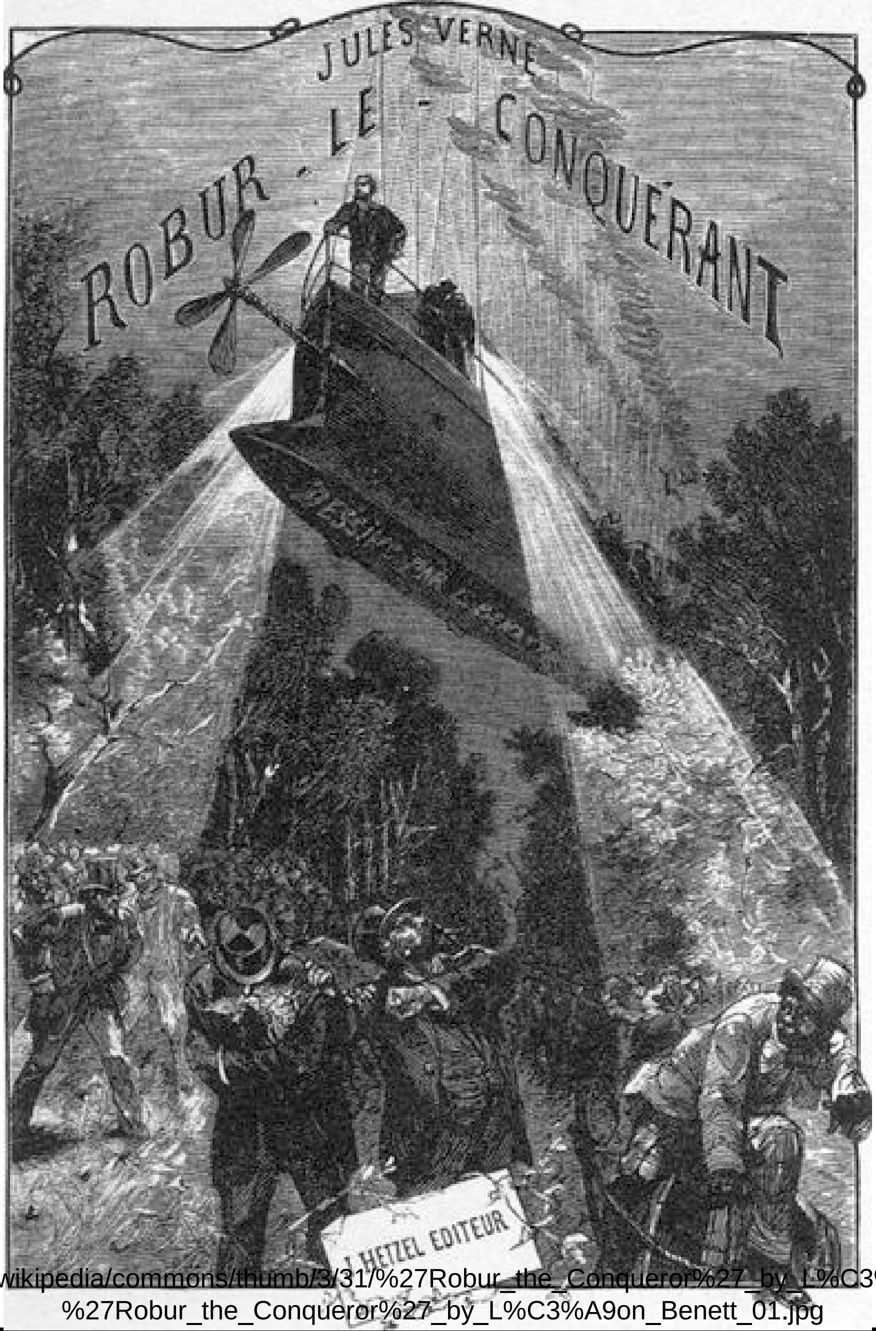
PROLOGUE

The Mind of a Renaissance Man

1878

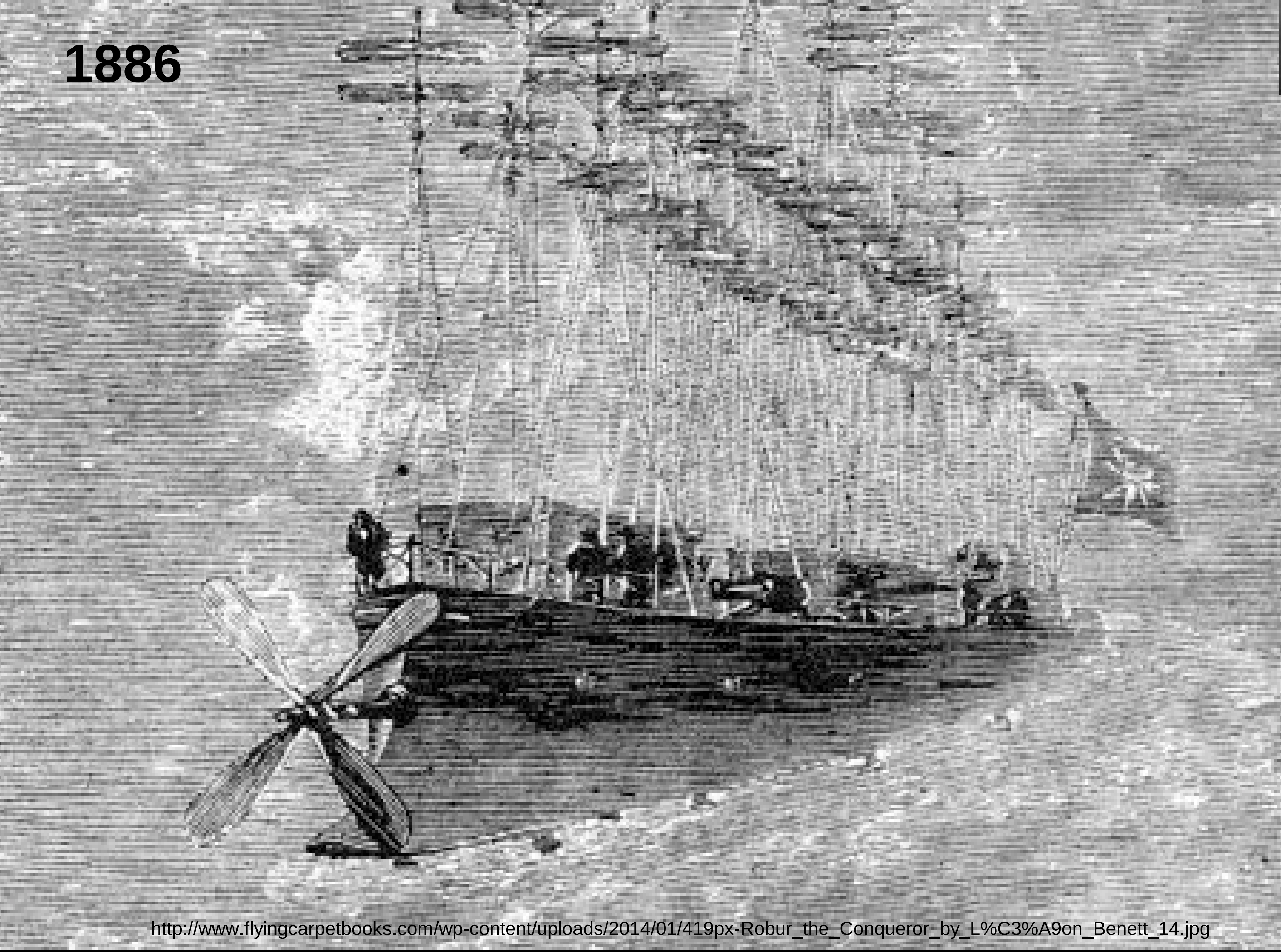
http://en.wikipedia.org/wiki/File:F%C3%A9lix_Nadar_1820-1910_portraits_Jules_Verne_%28restoration%29.jpg

1886



https://upload.wikimedia.org/wikipedia/commons/thumb/3/31/%27Robur_the_Conqueror%27_by_L%C3%A9on_Benett_01.jpg/220px-%27Robur_the_Conqueror%27_by_L%C3%A9on_Benett_01.jpg

1886



http://www.flyingcarpetbooks.com/wp-content/uploads/2014/01/419px-Robur_the_Conqueror_by_L%C3%A9on_Benett_14.jpg

ACT I

The Gilded Age

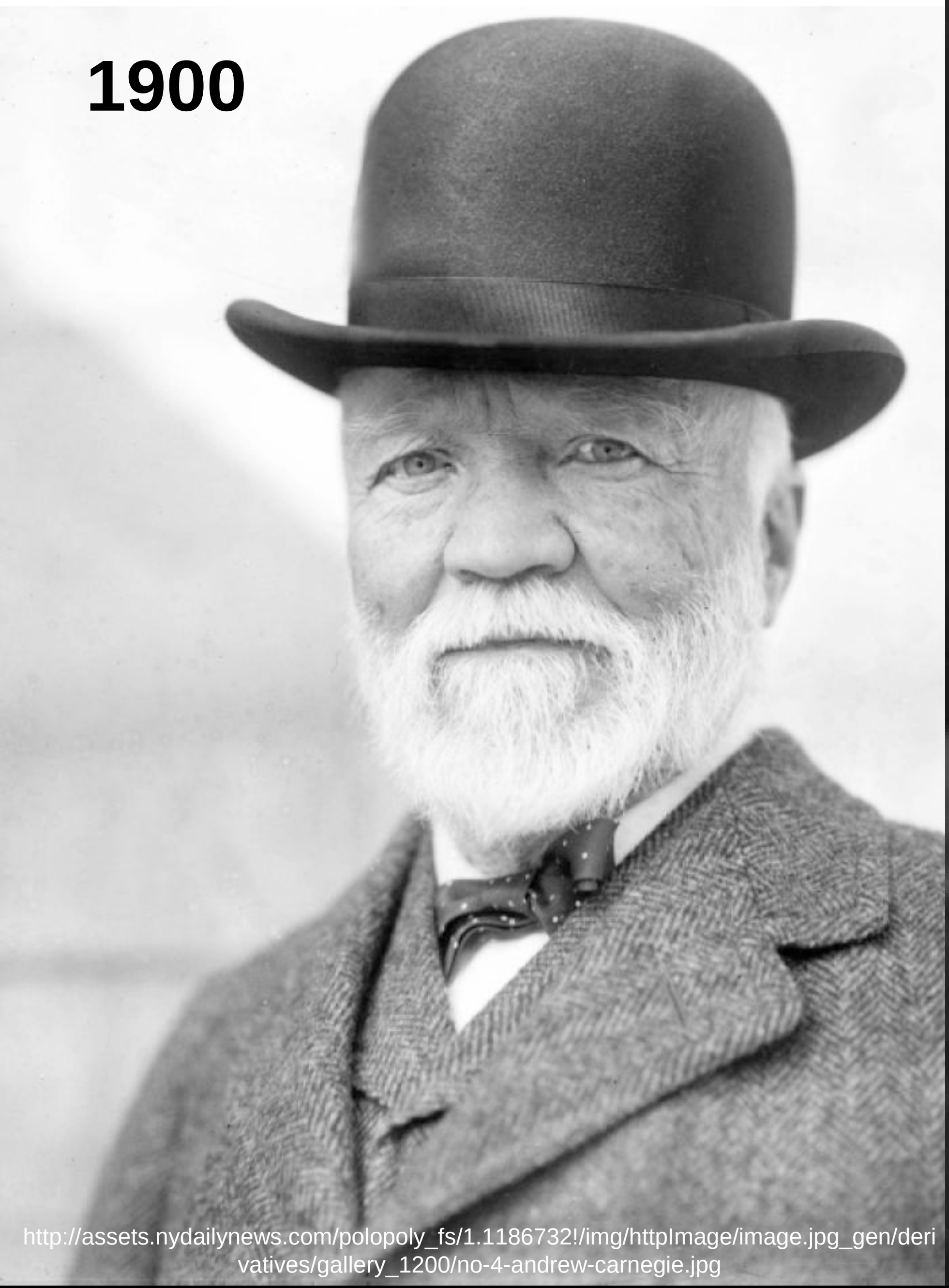
1890

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

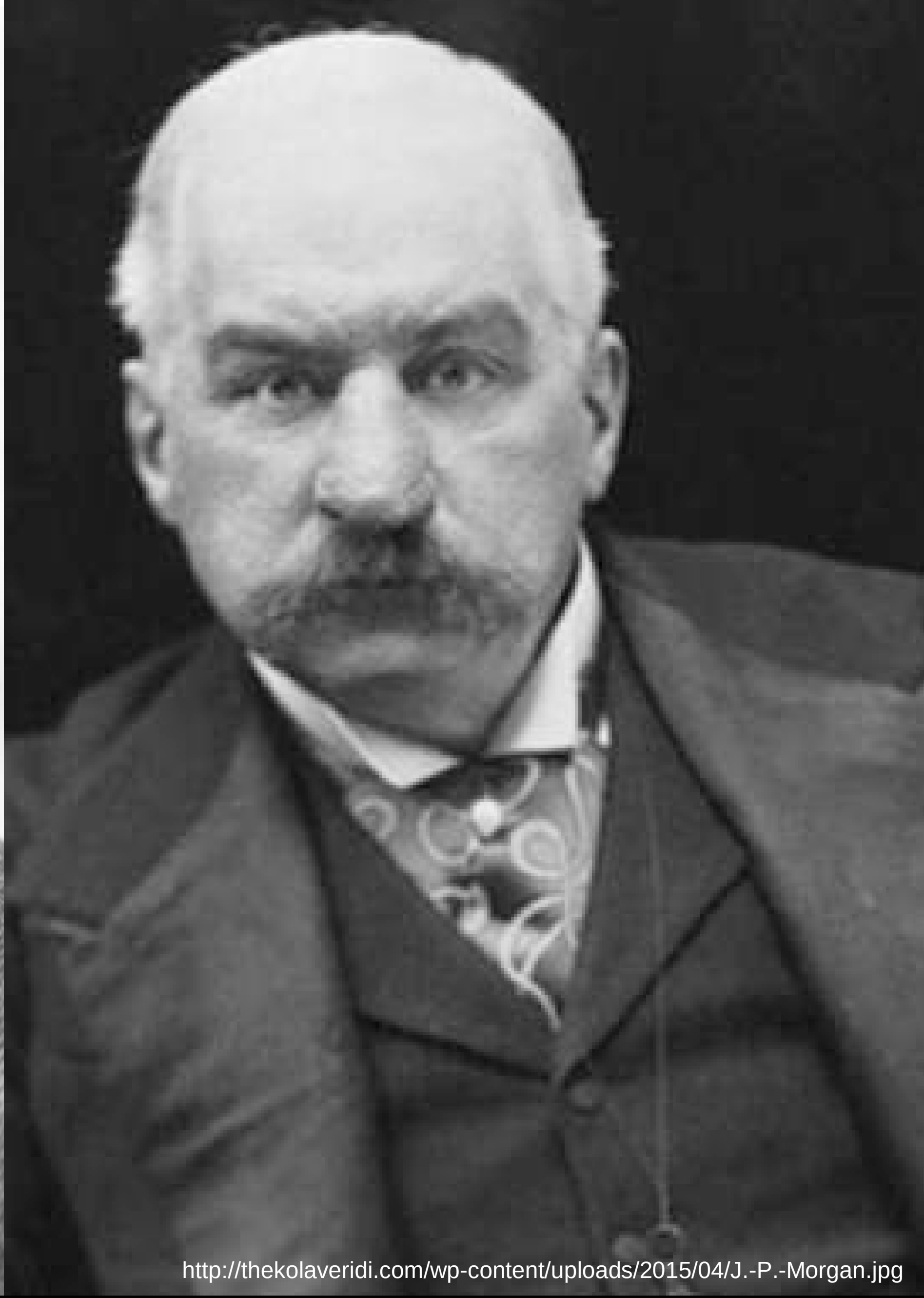
1893

http://burnhamplan100.lib.uchicago.edu/newberryexhibit/images/reforming3-large.jpg

1900

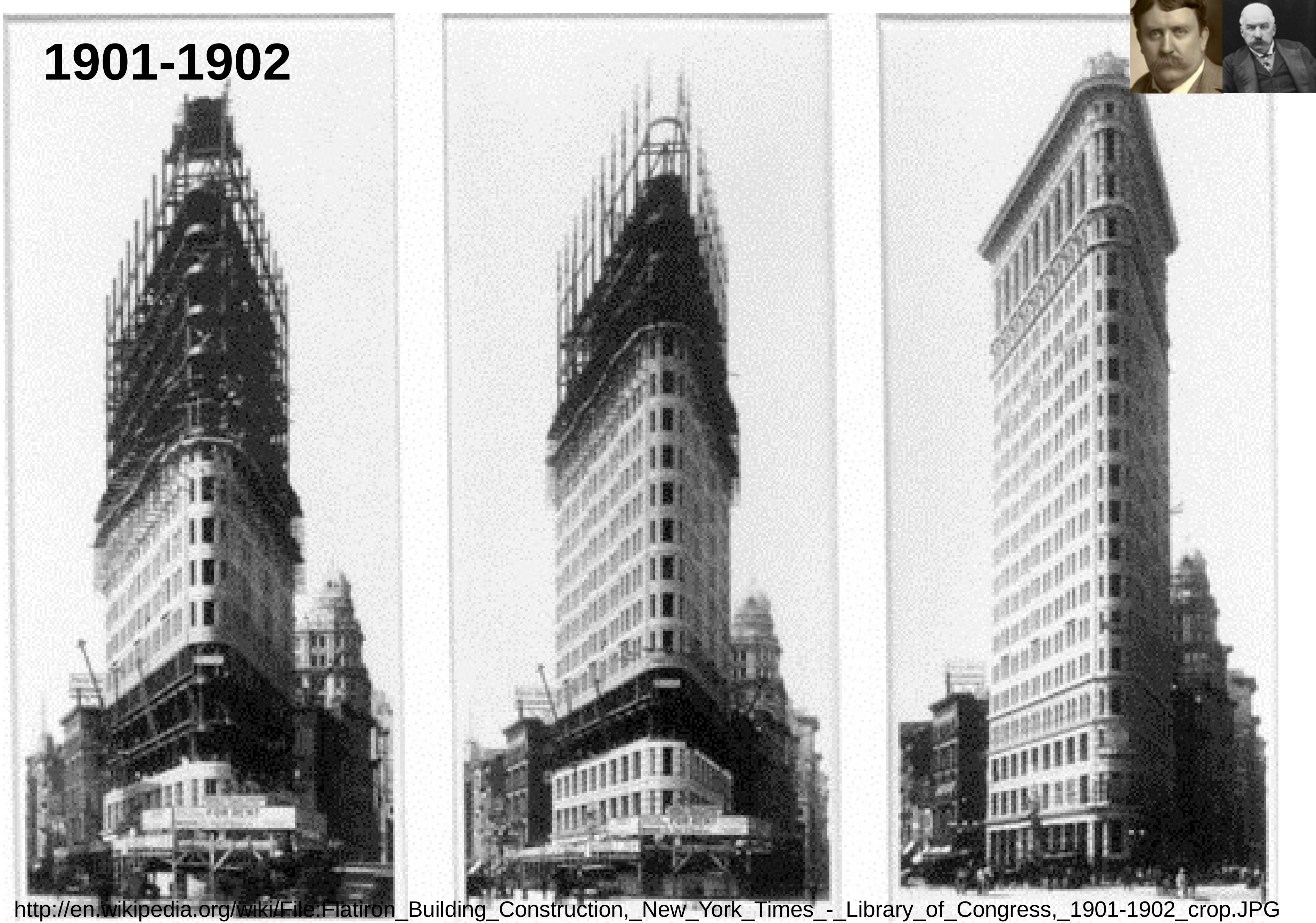


http://assets.nydailynews.com/polopoly_fs/1.1186732!/img/httpImage/image.jpg_gen/derivatives/gallery_1200/no-4-andrew-carnegie.jpg



http://thekolaveridi.com/wp-content/uploads/2015/04/J.-P.-Morgan.jpg

1901-1902

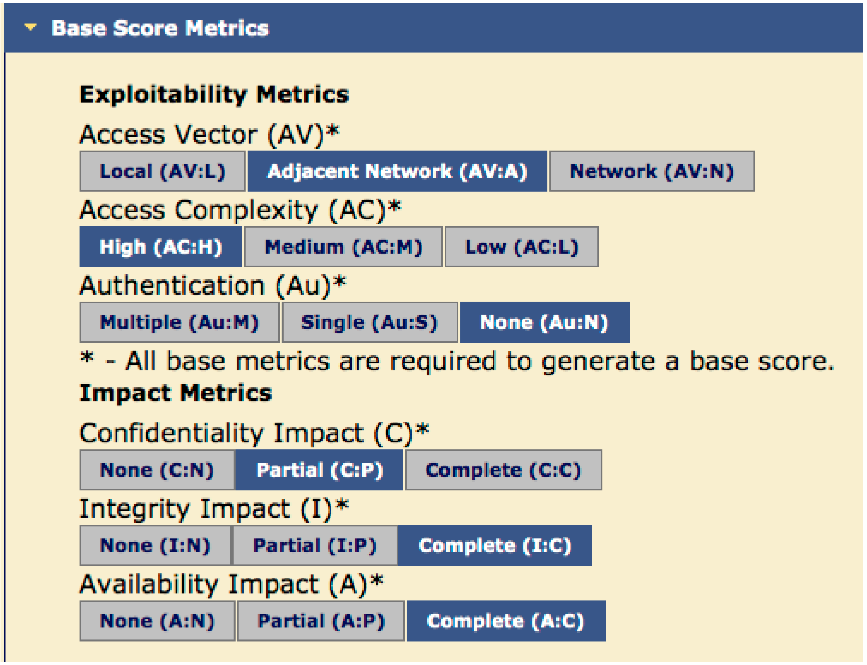


http://en.wikipedia.org/wiki/File:Flatiron_Building_Construction,_New_York_Times_-_Library_of_Congress,_1901-1902_crop.JPG

1902

Dropping 40k Day

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.



▾ Base Score Metrics

Exploitability Metrics

Access Vector (AV)*

Local (AV:L) [✓ Adjacent Network (AV:A)] Network (AV:N)

Access Complexity (AC)*

[✓ High (AC:H)] Medium (AC:M) Low (AC:L)

Authentication (Au)*

Multiple (Au:M) Single (Au:S) [✓ None (Au:N)]

* - All base metrics are required to generate a base score.

Impact Metrics

Confidentiality Impact (C)*

None (C:N) [✓ Partial (C:P)] Complete (C:C)

Integrity Impact (I)*

None (I:N) Partial (I:P) [✓ Complete (I:C)]

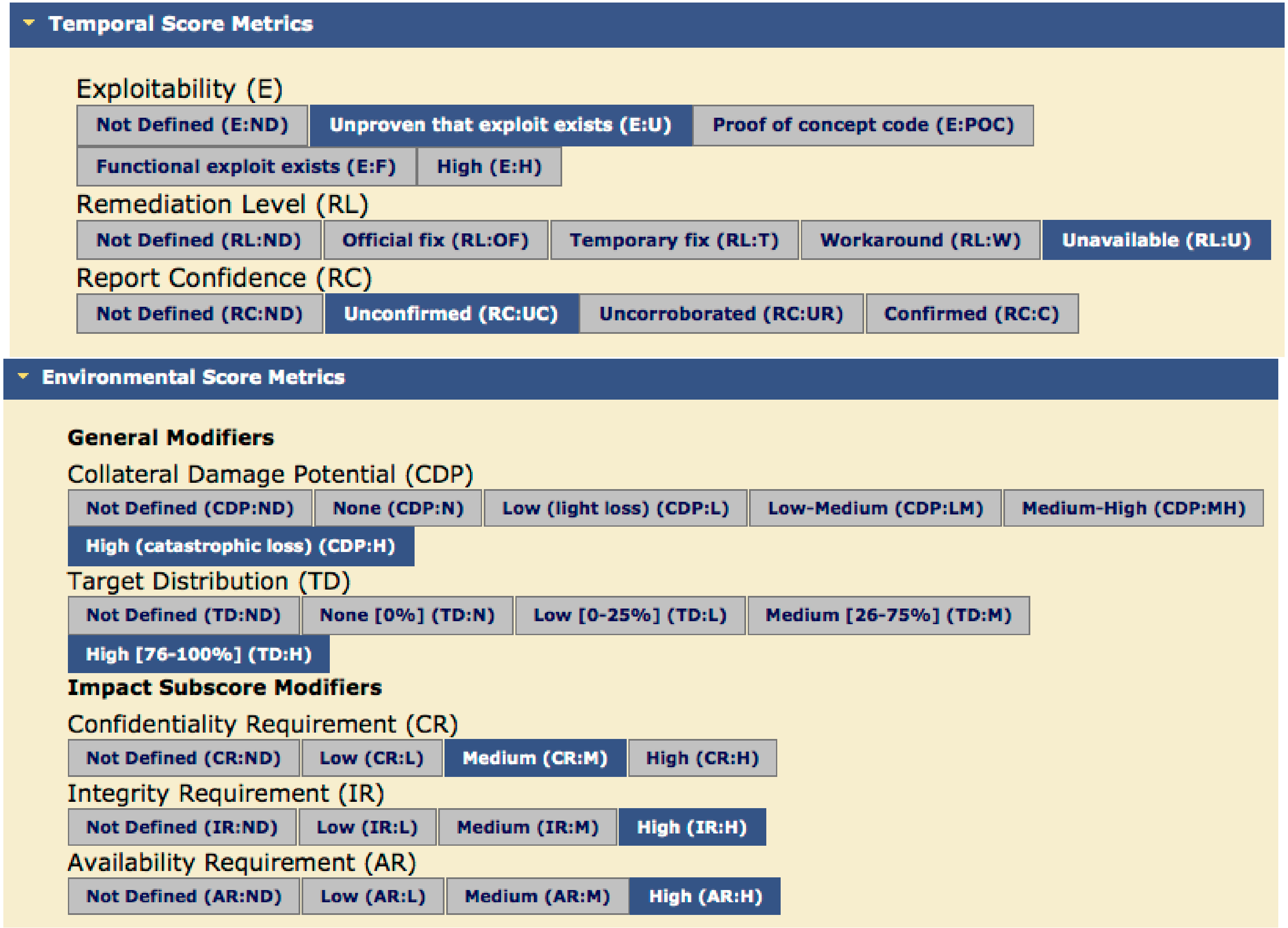
Availability Impact (A)*

None (A:N) Partial (A:P) [✓ Complete (A:C)]

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)

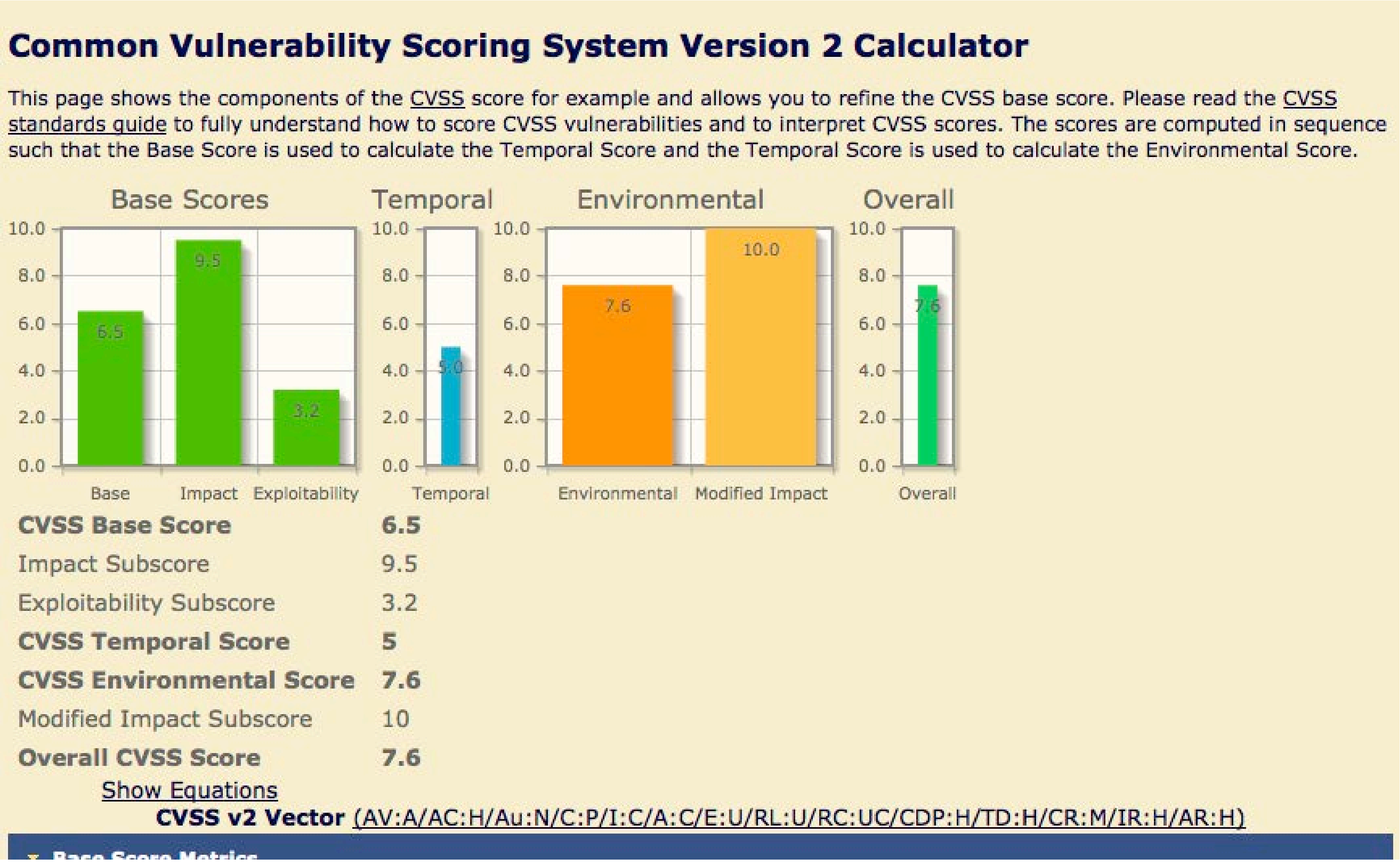
Integrity Requirement (IR)

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)

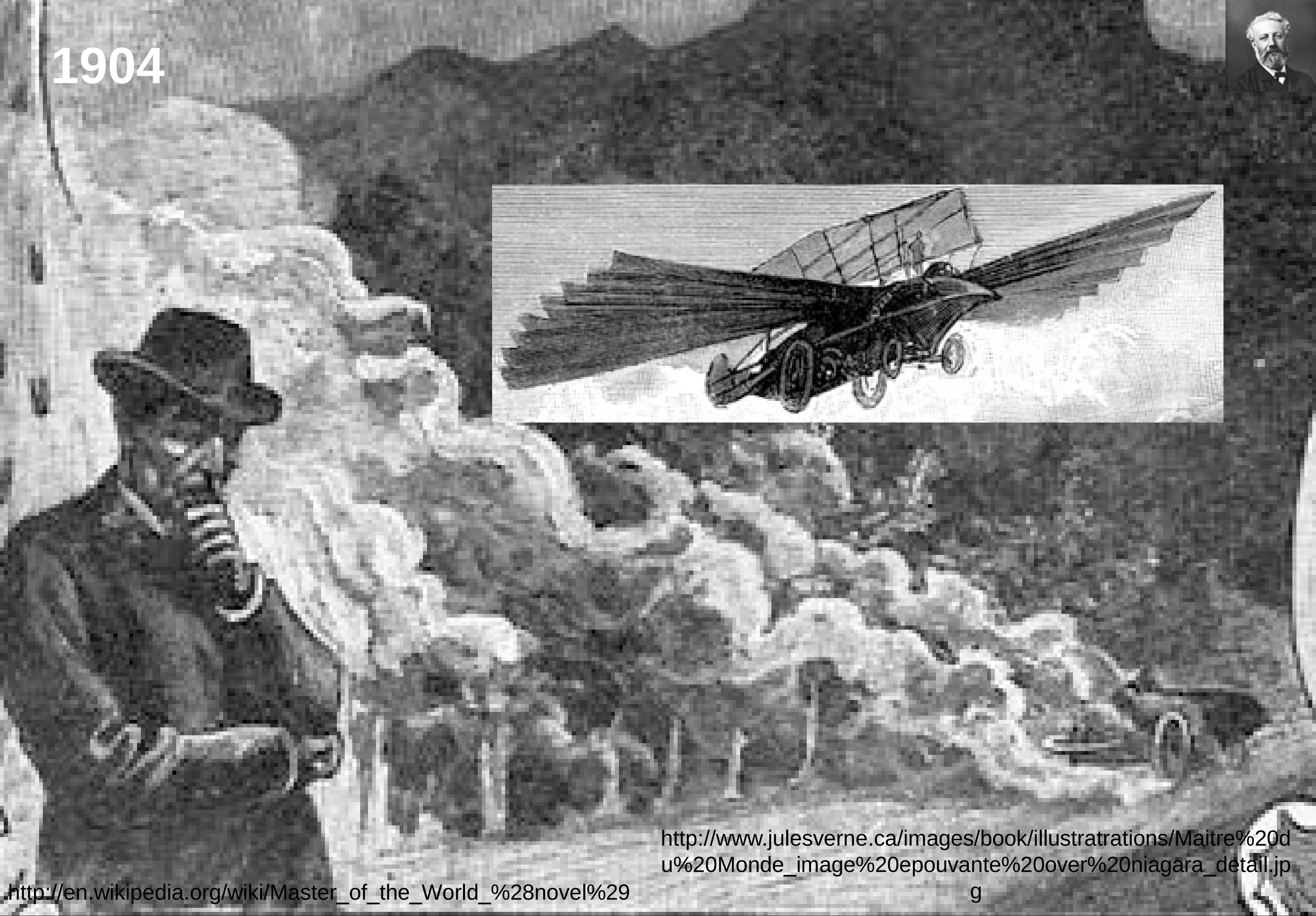
▼ Base Score Metrics

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

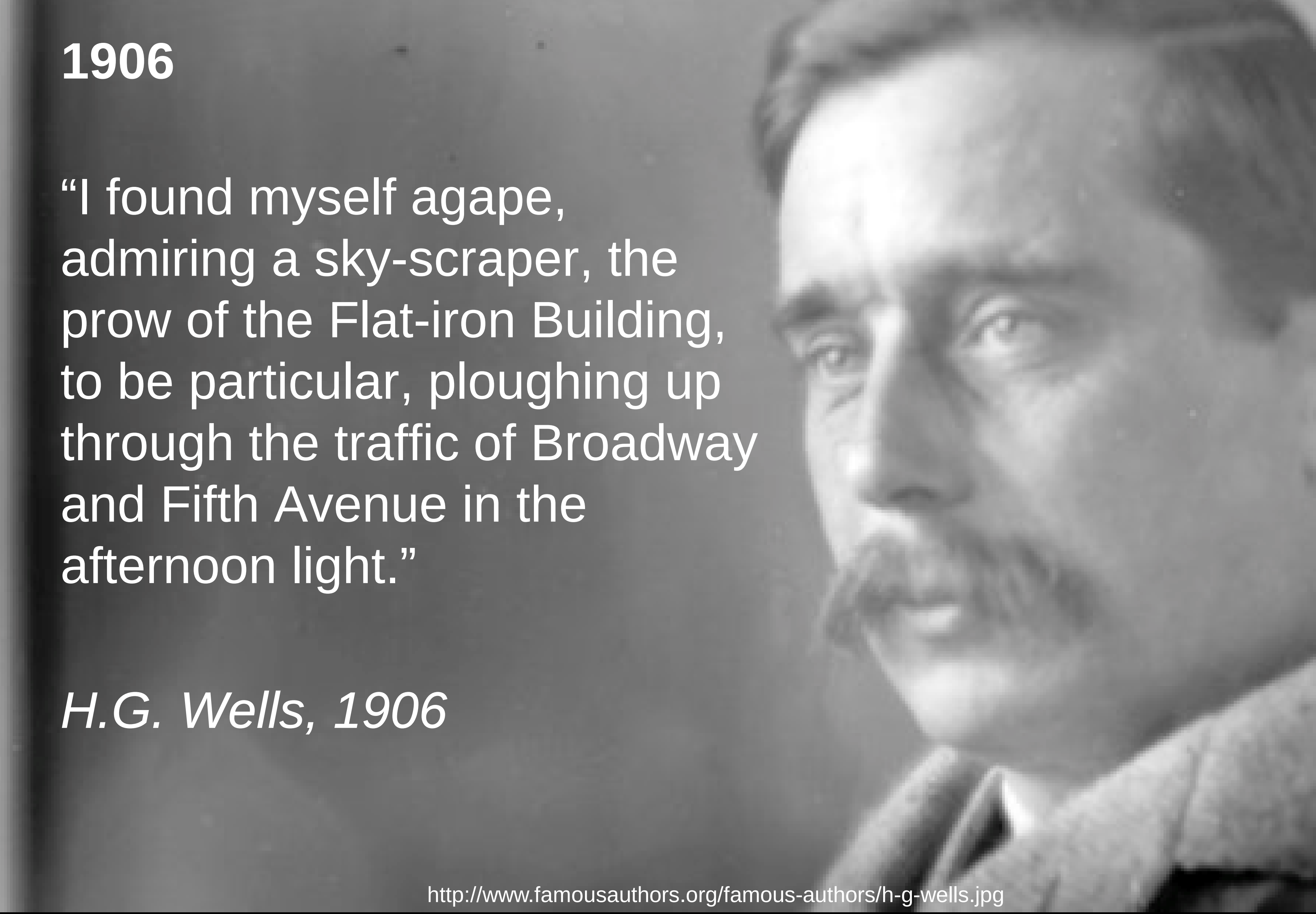
1904



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

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

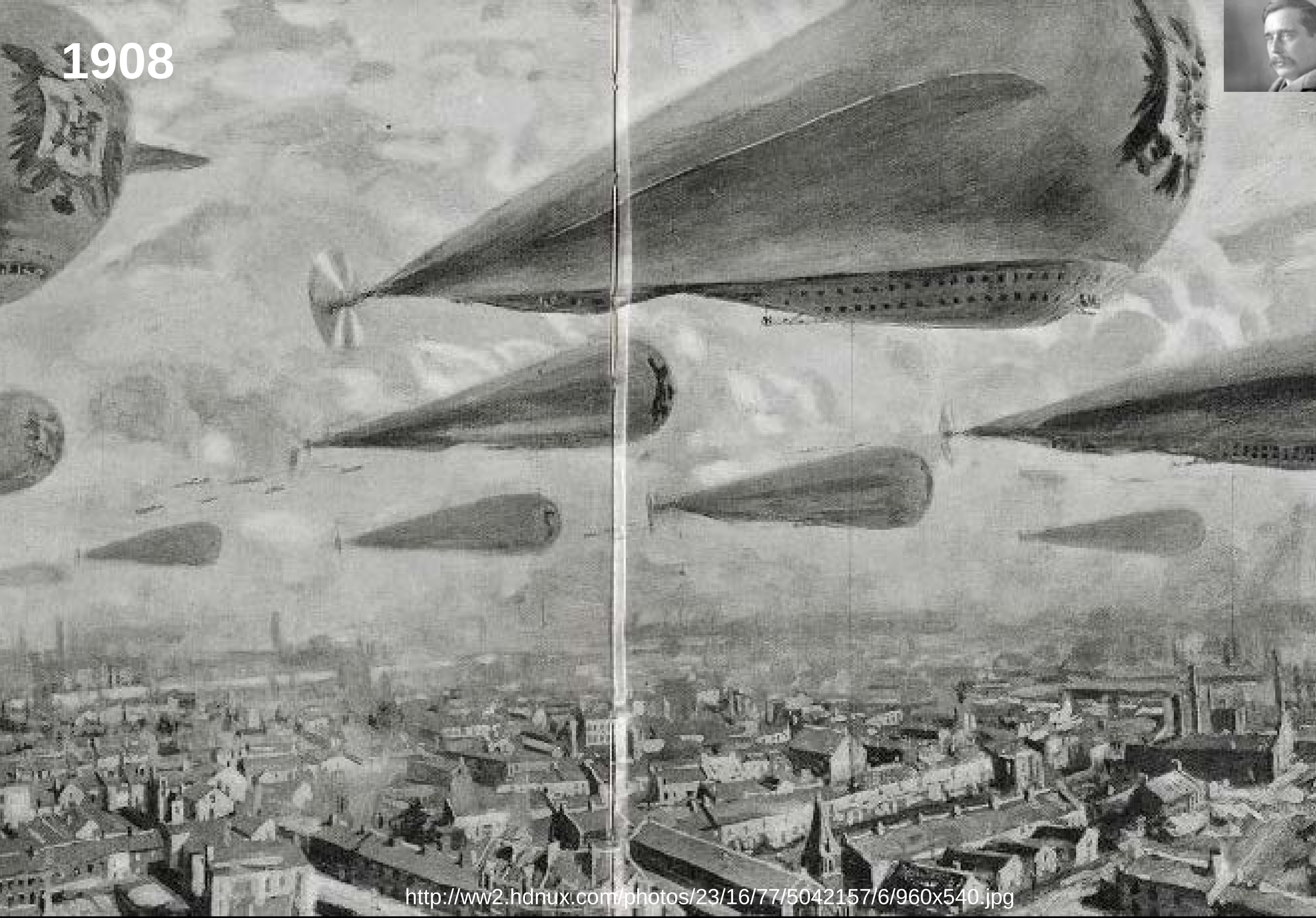
1906



“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://www.famousauthors.org/famous-authors/h-g-wells.jpg



1908

http://ww2.hdnux.com/photos/23/16/77/5042157/6/960x540.jpg

1915

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

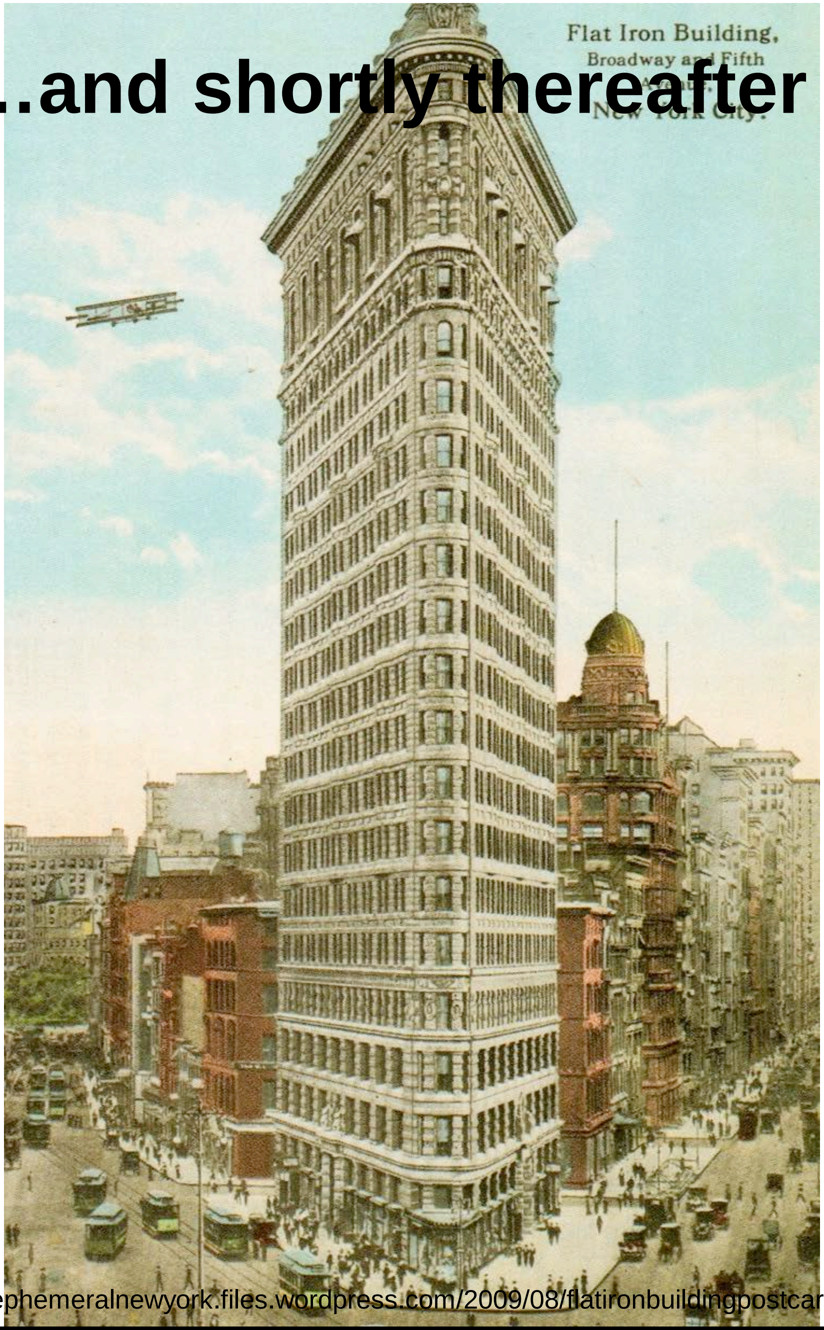
Meanwhile, back in NYC…

1915

Flat Iron Building,
Broadway and Fifth Avenue,
New York City.

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

…and 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

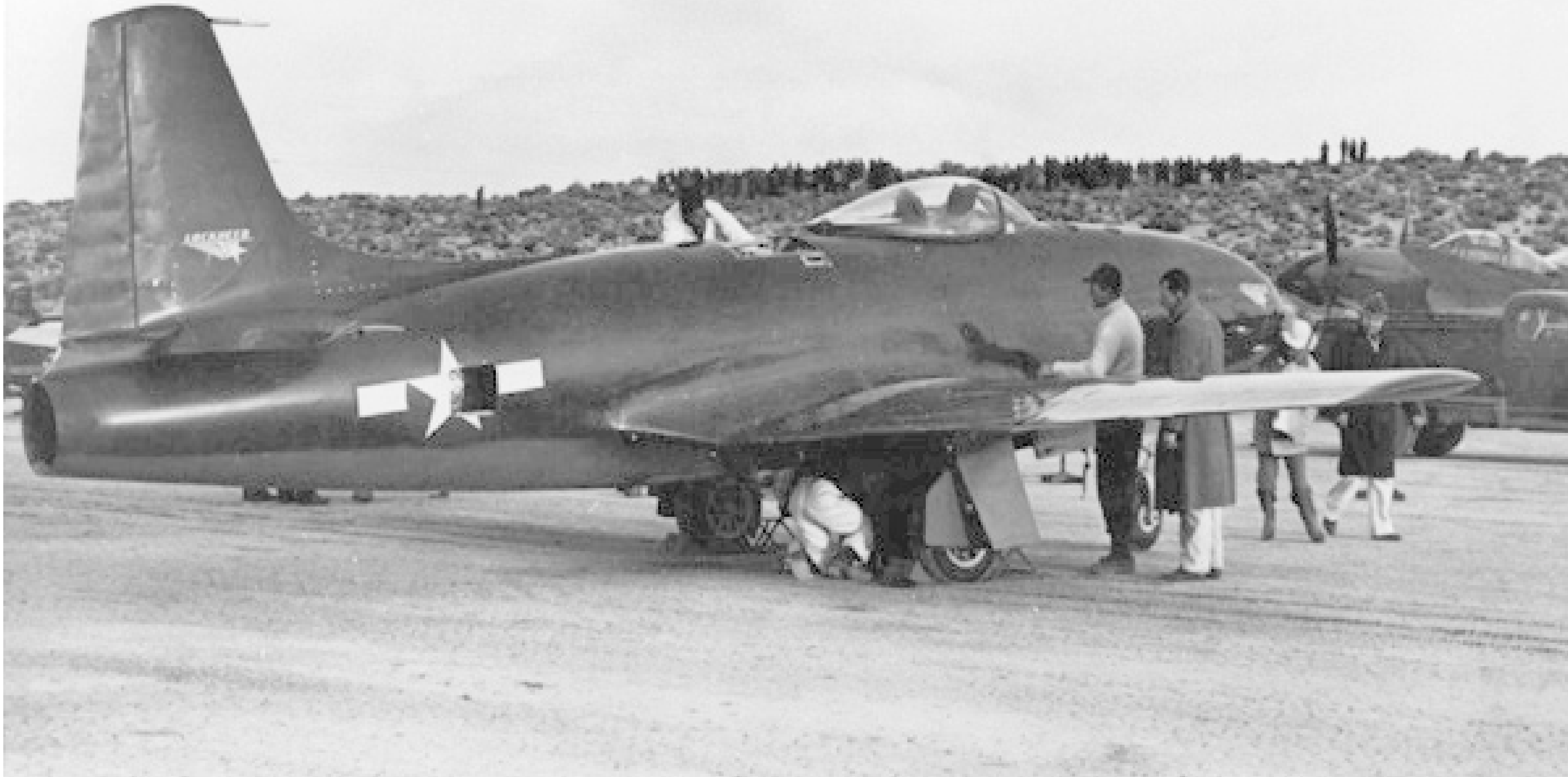
1939

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

Empire State Building

Flatiron Building

1946

VOL. XCV No. 32,259.

LANE HITS WALL ST. TOWER;
IN ARMY CRAFT ARE KILLED;
IG HOLE TORN IN 58TH FLOOR

MINE SE
OPERA
OF UN

Facing
and
T

UMW

Rai
Ac

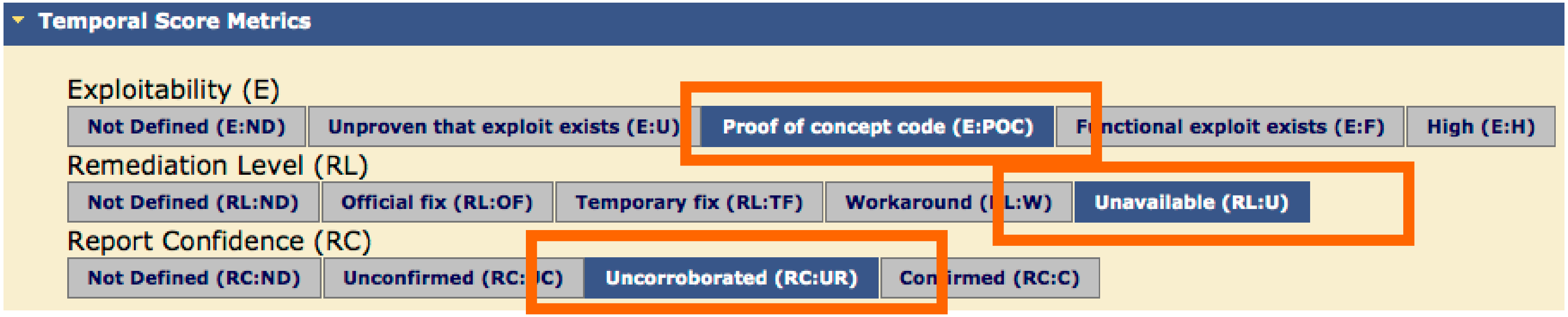
LOT LOST IN FOG

n Route to N
From the South-
Officer a Vic

DEBRIS FALLS

SCENE OF PLANE CRASH LAST NIGHT

CVSS v2 1946



Temporal Score Metrics

Exploitability (E)

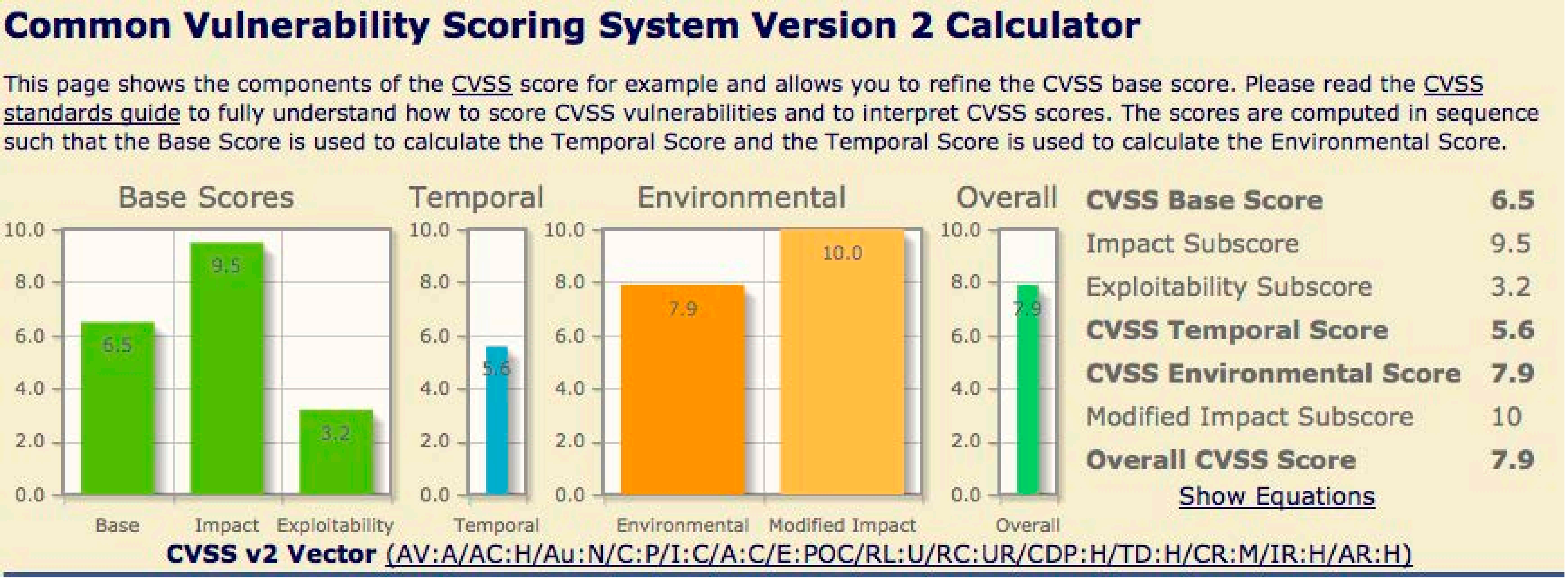
Not Defined (E:ND) | Unproven that exploit exists (E:U) | **Proof of concept code (E:POC)** | Functional exploit exists (E:F) | High (E:H)

Remediation Level (RL)

Not Defined (RL:ND) | Official fix (RL:OF) | Temporary fix (RL:TF) | 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.

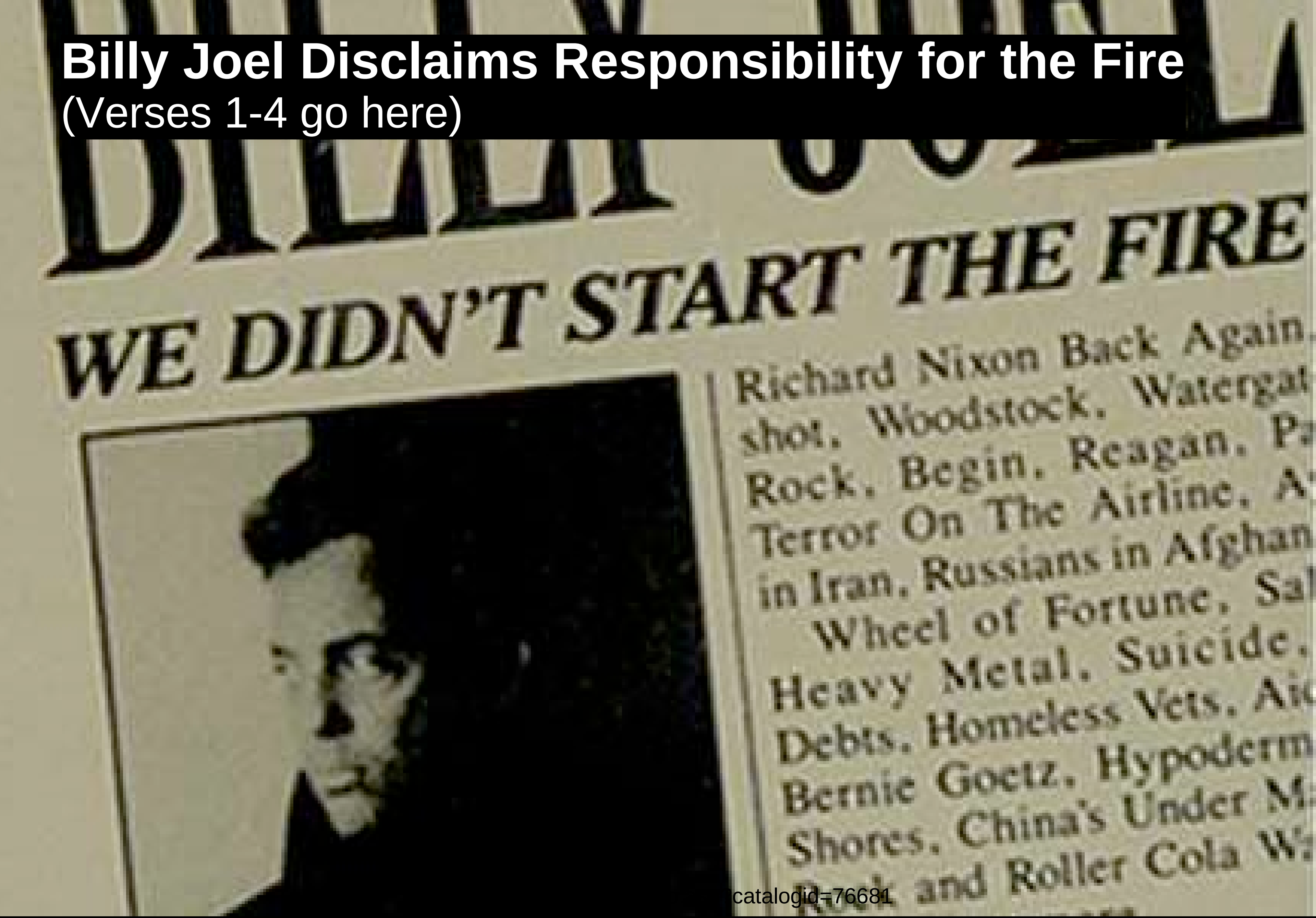
CVSS Base Score	**6.5**
Impact Subscore	9.5
Exploitability Subscore	3.2
CVSS Temporal Score	**5.6**
CVSS Environmental Score	**7.9**
Modified Impact Subscore	10
Overall CVSS Score	**7.9**

Show Equations

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

Billy Joel Disclaims Responsibility for the Fire

(Verses 1-4 go here)



BILLY JOEL

WE DIDN'T START THE FIRE

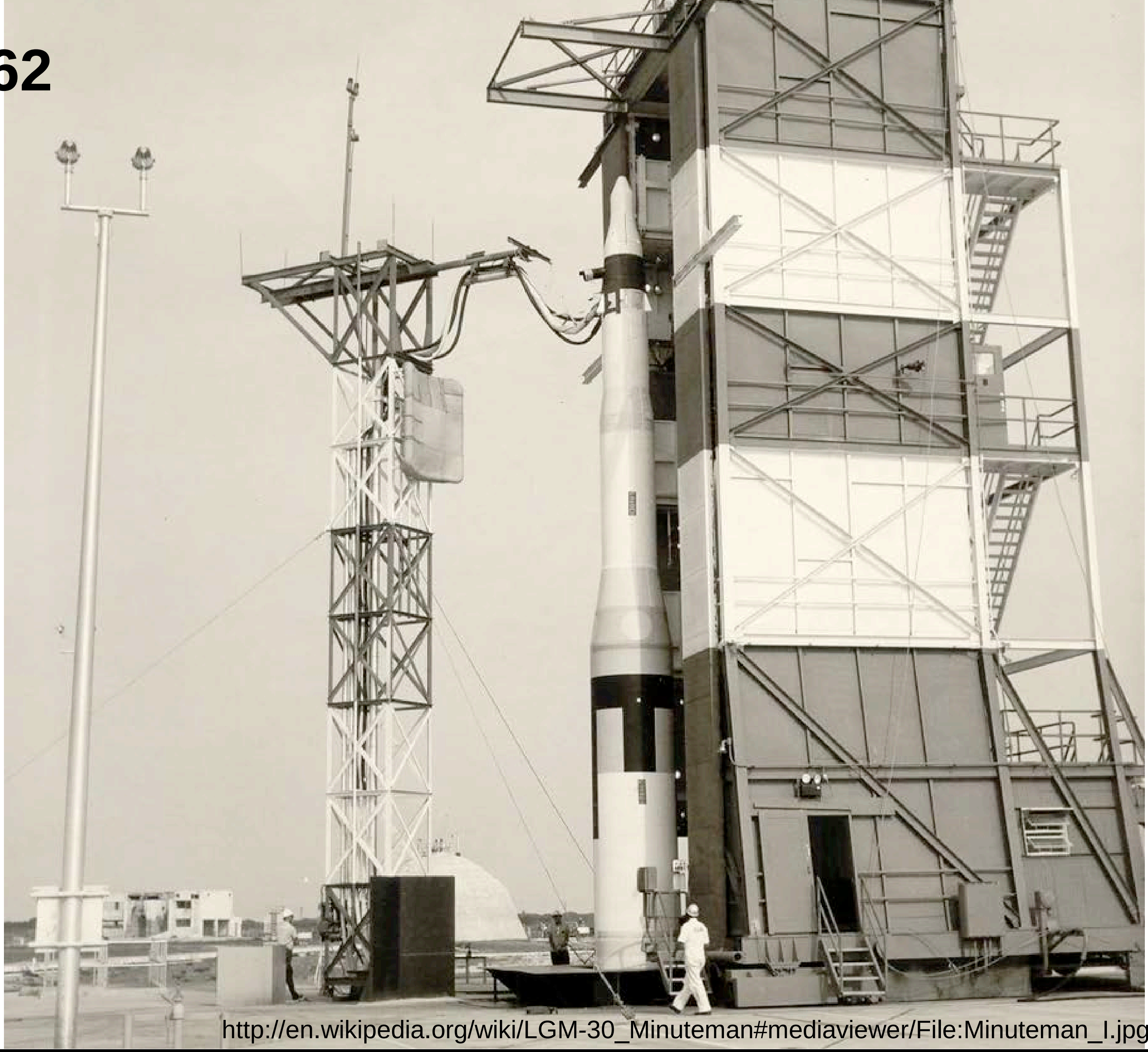
Richard Nixon Back Again.
shot. Woodstock. Watergat
Rock. Begin. Reagan. Pa
Terror On The Airline. A
in Iran. Russians in Afghan
Wheel of Fortune. Sal
Heavy Metal. Suicide.
Debts. Homeless Vets. Aic
Bernie Goetz. Hypoderm
Shores. China's Under M
Rock and Roller Cola W

catalogid=76681

ACT II

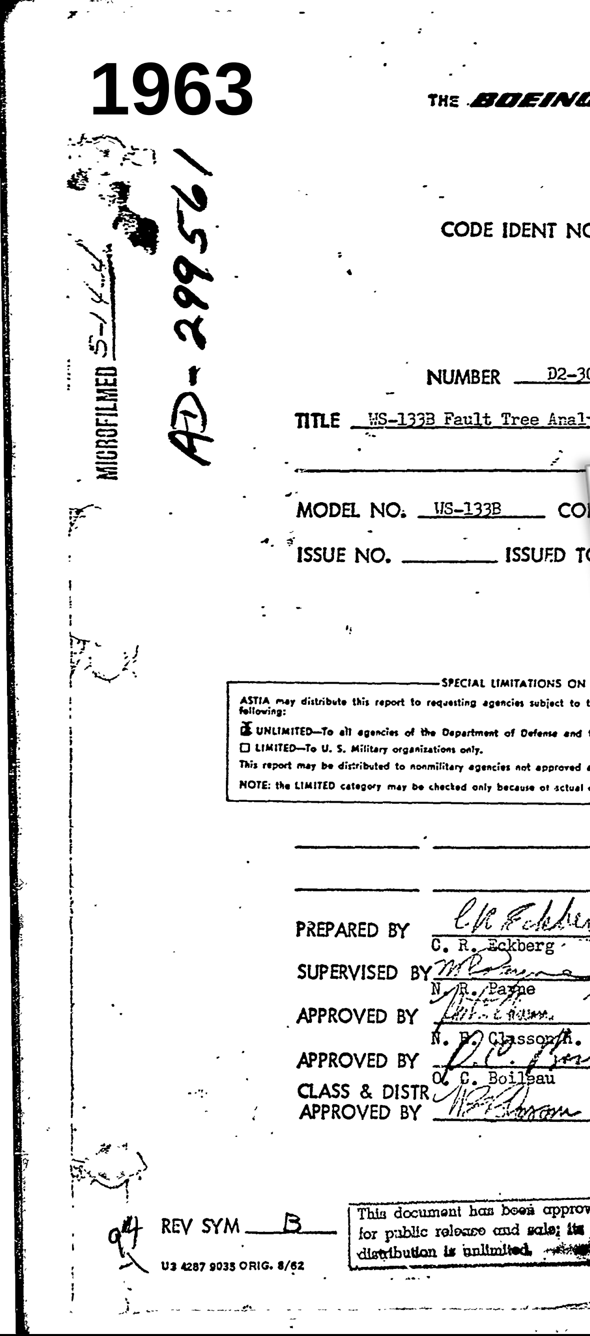
The Dawn of the Space Age

1962



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

1963



THE BOEING COMPANY

CODE IDENT NO. 81205

MICROFILMED 5-1-64

AD-299561

NUMBER D2-30207-1

TITLE WS-133B Fault Tree Analysis Program Plan (U)

MODEL NO. WS-133B CO

ISSUE NO. ________ ISSUED TO

SPECIAL LIMITATIONS ON AS

ASTIA may distribute this report to requesting agencies subject to their following:

☒ UNLIMITED—To all agencies of the Department of Defense and their

☐ LIMITED—To U. S. Military organizations only.

This report may be distributed to nonmilitary agencies not approved above

NOTE: the LIMITED category may be checked only because of actual or pot

PREPARED BY C. R. Eckberg

SUPERVISED BY N. R. Payne

APPROVED BY N. B. Classon R. K. Heb

APPROVED BY O. C. Boileau

CLASS & DISTR APPROVED BY

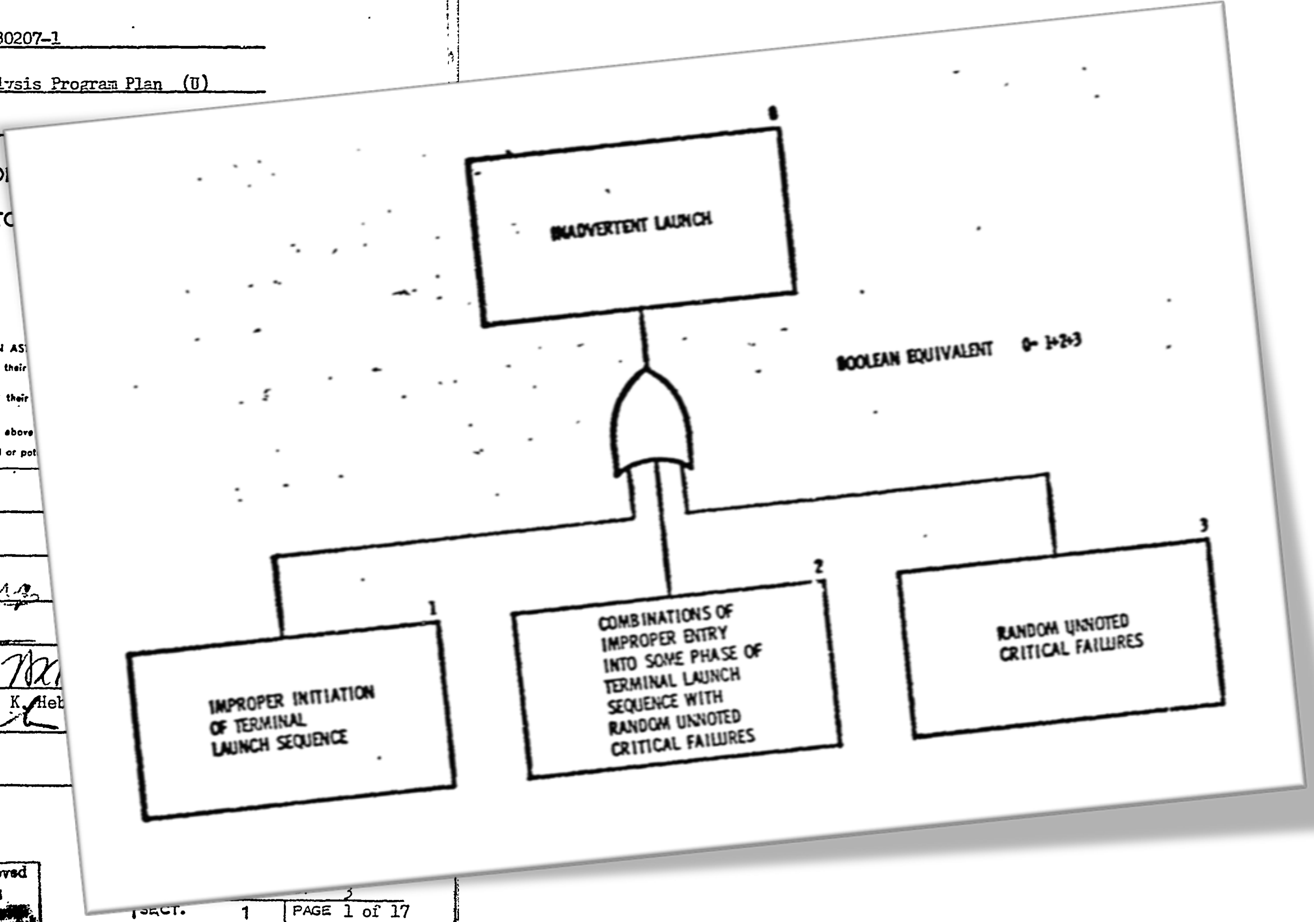
REV SYM B

This document has been approved for public release and sale; its distribution is unlimited.

U3 4287 9035 ORIG. 8/62

SECT. 1 PAGE 1 of 17

2-5142-2

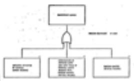

0
INADVERTENT LAUNCH
BOOLEAN EQUIVALENT 0= 1+2+3
1
IMPROPER INITIATION OF TERMINAL LAUNCH SEQUENCE
2
COMBINATIONS OF IMPROPER ENTRY INTO SOME PHASE OF TERMINAL LAUNCH SEQUENCE WITH RANDOM UNNOTED CRITICAL FAILURES
3
RANDOM UNNOTED CRITICAL FAILURES

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

1967

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

1968



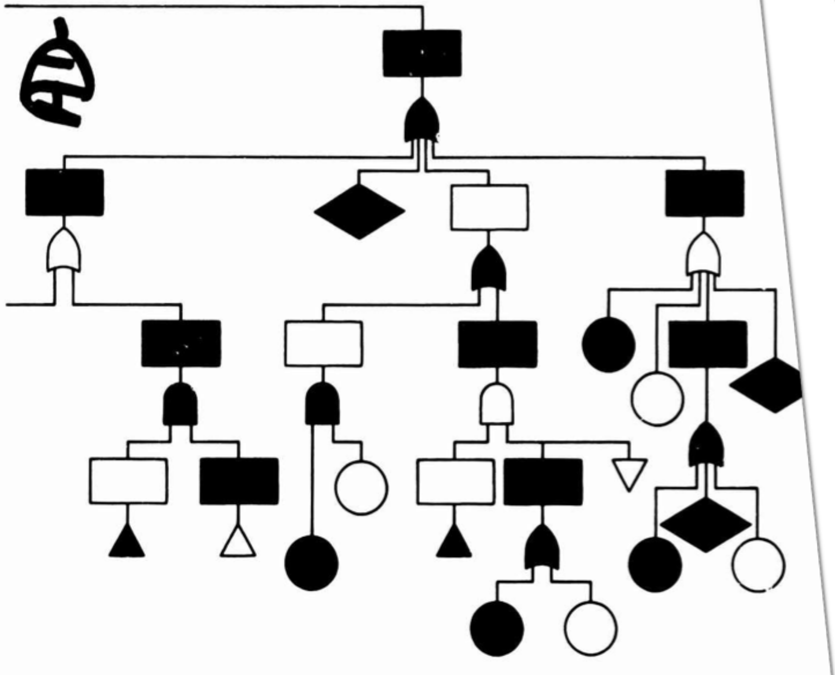
BOEING AEROSPACE COMPANY

RESEARCH AND ENGINEERING DIVISION

SEATTLE,

AD-8470

FAULT TREE FOR SAFETY



SUPPORT SYSTEMS ENGINEERING

Beginning with the most undesired (top) event, the fault tree graphically depicts the paths that lead to each succeeding lower level of the display. This does not imply that each descending fault path has a "higher probability of occurrence"; in fact, in many instances, the opposite may be the case. However, a series of "little things," each with a relatively low probability of occurrence, may trigger an event at the next higher level. This is depicted in the fault tree as a progression of events through the logic gates.

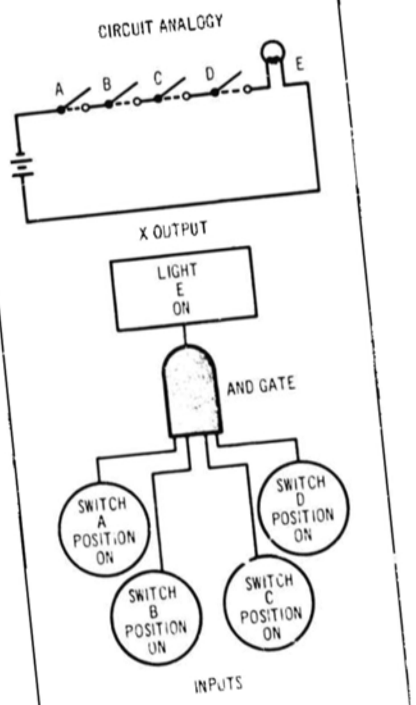
For example: A failed antiskid unit combined with a slippery runway and a severe crosswind could logically lead to divergence off the runway upon landing. If we carry this fault path higher in the display, we may find that a failed engine prohibits correcting the divergence. In this case, the multiple factors did not cause the engine to fail, but the fact that it did fail at a critical moment prevented the pilot from completing corrective action. Suppose, however, the engine failed prior to touchdown. Obviously, the pilot would have planned his approach to compensate for the power loss. Certainly, he would have been more cautious of the slippery runway and, as a consequence, better prepared to cope with the failed antiskid at the first indication of failure or malfunction. Thus, the fault tree analyst must foresee not only grossly probable events but many possible events.

BASIC LOGIC GATES

Three basic symbols, or logic gates, are used in constructing a fault tree: the AND, the OR, and the INHIBIT gates. These are illustrated in Figs. 1, 2, and 3.

AND and OR Gates

These gates represent the fundamental Boolean functions that form the basis for all logic analysis. The decision on which gate, the AND or OR, to use can be explained by the following



The AND gate performs the logic function that requires the co-existence of all gate inputs (A, B, C, D) events in order to realize an output (X) event.

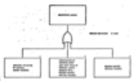
Figure 1. Use of "AND" Gate

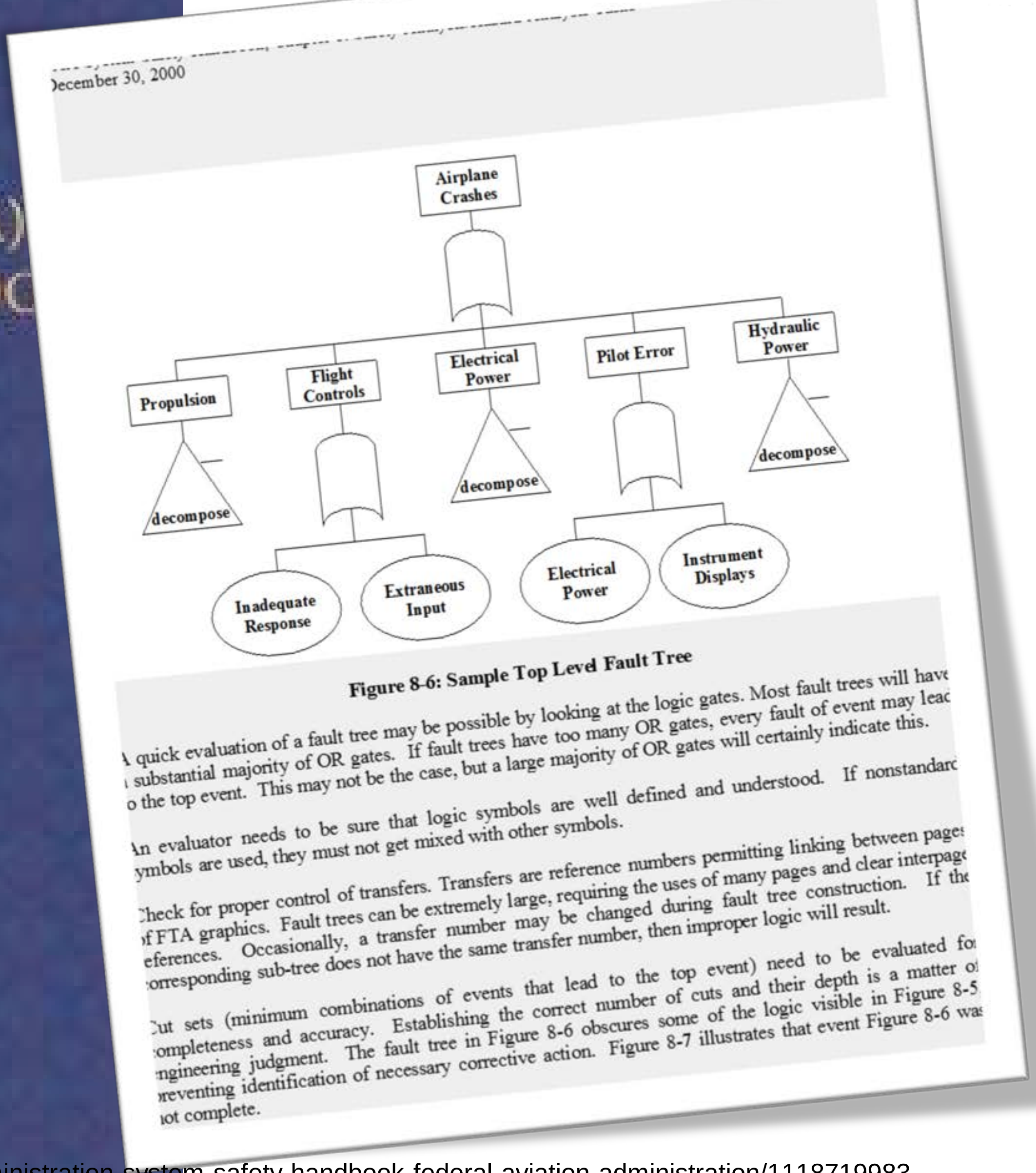
3

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

1970

FEDERAL AVIATION ADMINISTRATION (FAA) SYSTEM SAFETY HANDBOO





ecember 30, 2000

Airplane Crashes
Propulsion
Flight Controls
Electrical Power
Pilot Error
Hydraulic Power
decompose
decompose
decompose
Inadequate Response
Extraneous Input
Electrical Power
Instrument Displays

Figure 8-6: Sample Top Level Fault Tree

quick evaluation of a fault tree may be possible by looking at the logic gates. Most fault trees will have substantial majority of OR gates. If fault trees have too many OR gates, every fault of event may leac o the top event. This may not be the case, but a large majority of OR gates will certainly indicate this.

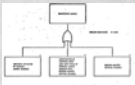
n evaluator needs to be sure that logic symbols are well defined and understood. If nonstandarc ymbols are used, they must not get mixed with other symbols.

heck for proper control of transfers. Transfers are reference numbers permitting linking between pages f FTA graphics. Fault trees can be extremely large, requiring the uses of many pages and clear interpage eferences. Occasionally, a transfer number may be changed during fault tree construction. If the orresponding sub-tree does not have the same transfer number, then improper logic will result.

ut sets (minimum combinations of events that lead to the top event) need to be evaluated for ompleteness and accuracy. Establishing the correct number of cuts and their depth is a matter of ngineering judgment. The fault tree in Figure 8-6 obscures some of the logic visible in Figure 8-5 reventing identification of necessary corrective action. Figure 8-7 illustrates that event Figure 8-6 was ot complete.

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

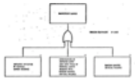
1979



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

1981

NUREG-0492



Fault Tree Handbook

U.S. Nuclear Regulatory Commission

CHAPTER III – FAULT TREE ANALYSIS – BASIC CONCEPTS

1. **Orientation**

In Chapter I we introduced two approaches to system analysis: inductive an deductive. Chapter II described the major inductive methods. Chapter III present the basic concepts and definitions necessary for an understanding of the deductiv Fault Tree Analysis approach, which is the subject of the remainder of this text.

2. **Failure vs. Success Models**

The operation of a system can be considered from two standpoints: we ca enumerate various ways for system success, or we can enumerate various ways fo system failure. We have already seen an example of this in Chapter II, section 8 Figure III-1 depicts the Failure/Success space concept.

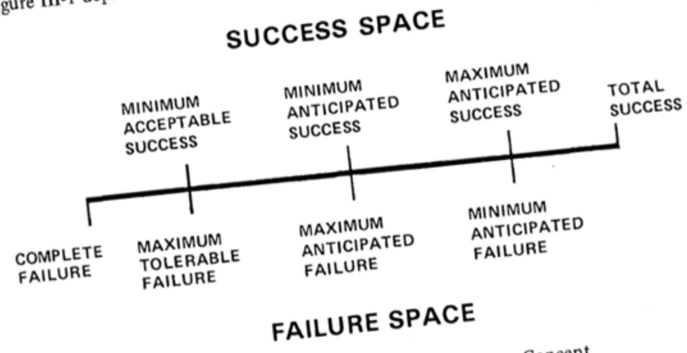

SUCCESS SPACE
MINIMUM ACCEPTABLE SUCCESS
MINIMUM ANTICIPATED SUCCESS
MAXIMUM ANTICIPATED SUCCESS
TOTAL SUCCESS
COMPLETE FAILURE
MAXIMUM TOLERABLE FAILURE
MAXIMUM ANTICIPATED FAILURE
MINIMUM ANTICIPATED FAILURE
FAILURE SPACE

Figure III-1. The Failure Space–Success Space Concept

It is interesting to note that certain identifiable points in success space coincide with certain analogous points in failure space. Thus, for instance, "maximum anticipated success" in success space can be thought of as coinciding with "minimum anticipated failure" in failure space. Although our first inclination might be to select the optimistic view of our system–success–rather than the pessimistic one–failure–, we shall see that this is not necessarily the most advantageous one.

From an analytical standpoint, there are several overriding advantages that accru to the failure space standpoint. First of all, it is generally easier to attain concurrenc on what constitutes failure than it is to agree on what constitutes success. We may desire an airplane that flies high, travels far without refueling, moves fast and carries a big load. When the final version of this aircraft rolls off the production line, some of these features may have been compromised in the course of making the usual

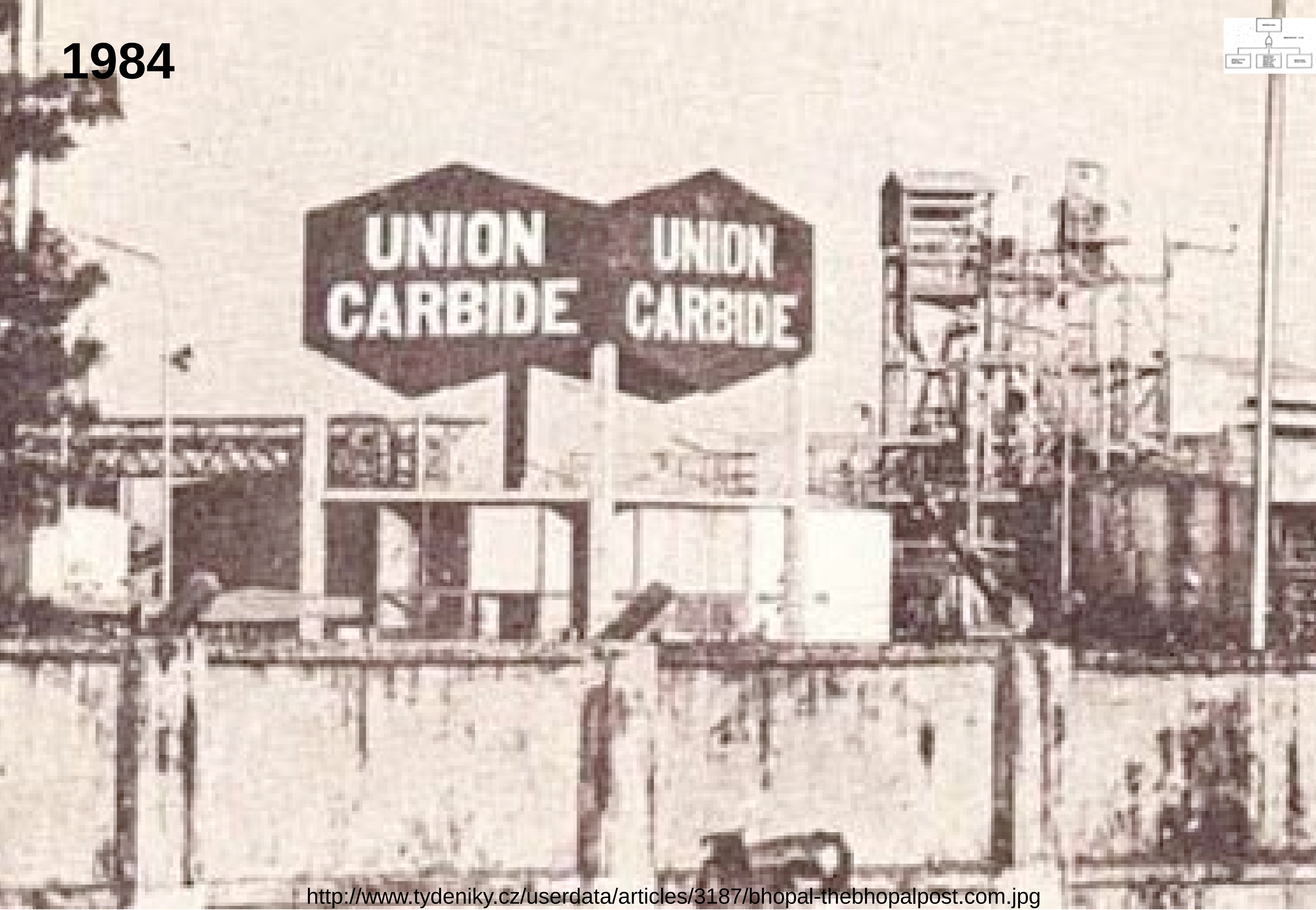
III-1

http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/sr0492.pdf

1982

http://media.web.britannica.com/eb-media/52/103452-004-7DA0E924.jpg

1984



http://www.tydeniky.cz/userdata/articles/3187/bhopal-thebhopalpost.com.jpg

1986

> "…the fault tree method was not applied to the rocket boosters before the accident and is just now being used to check whether the agency missed any potential causes of failure"

http://www.nytimes.com/1986/02/05/us/shuttle-inquiry-exploring-key-wreckage-nasa-s-risk-assessment-isn-t-most.html

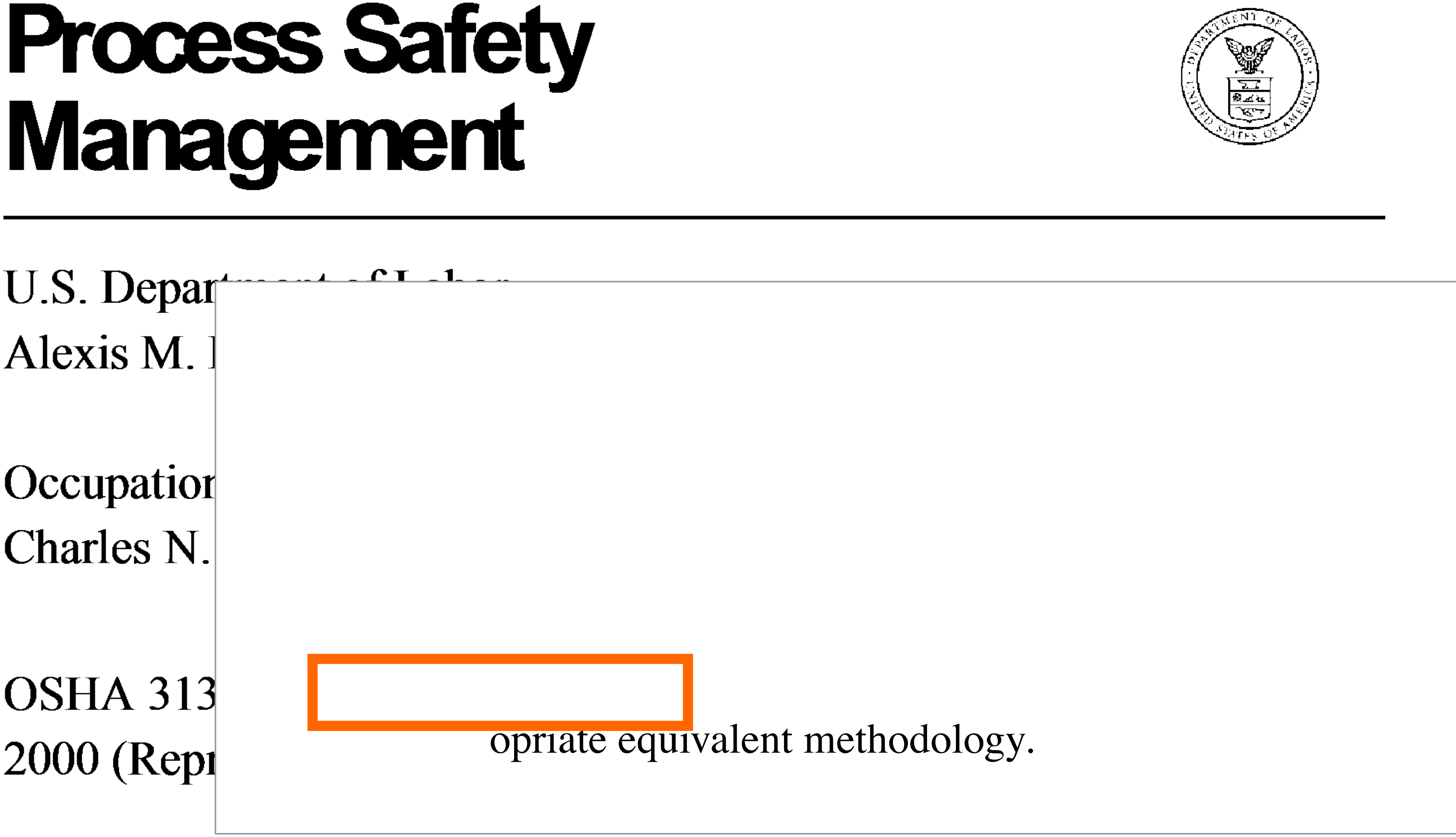
http://commons.wikimedia.org/wiki/File:Space_Shuttle_Challenger_(04-04-1983).JPEG

1988

http://firesafetynation.com

http://i.dailymail.co.uk/i/pix/2013/07/06/article-0-1A8FAA3F000005DC-107_634x769.jpg

1992



Process Safety Management

U.S. Depar

Alexis M. I

Occupation

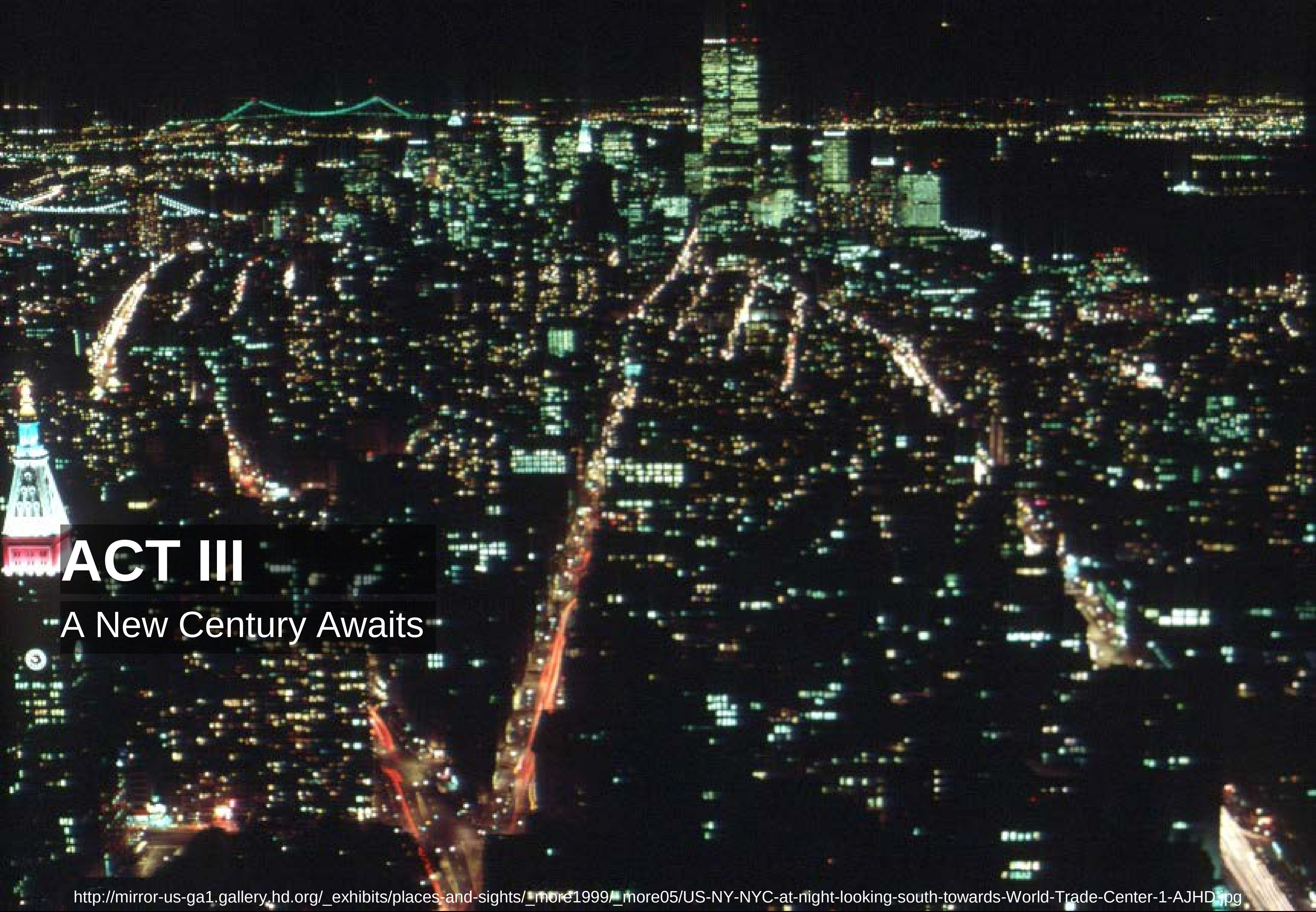
Charles N.

OSHA 313

2000 (Repr

opriate equivalent methodology.

https://www.osha.gov/Publications/osha3132.pdf

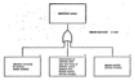


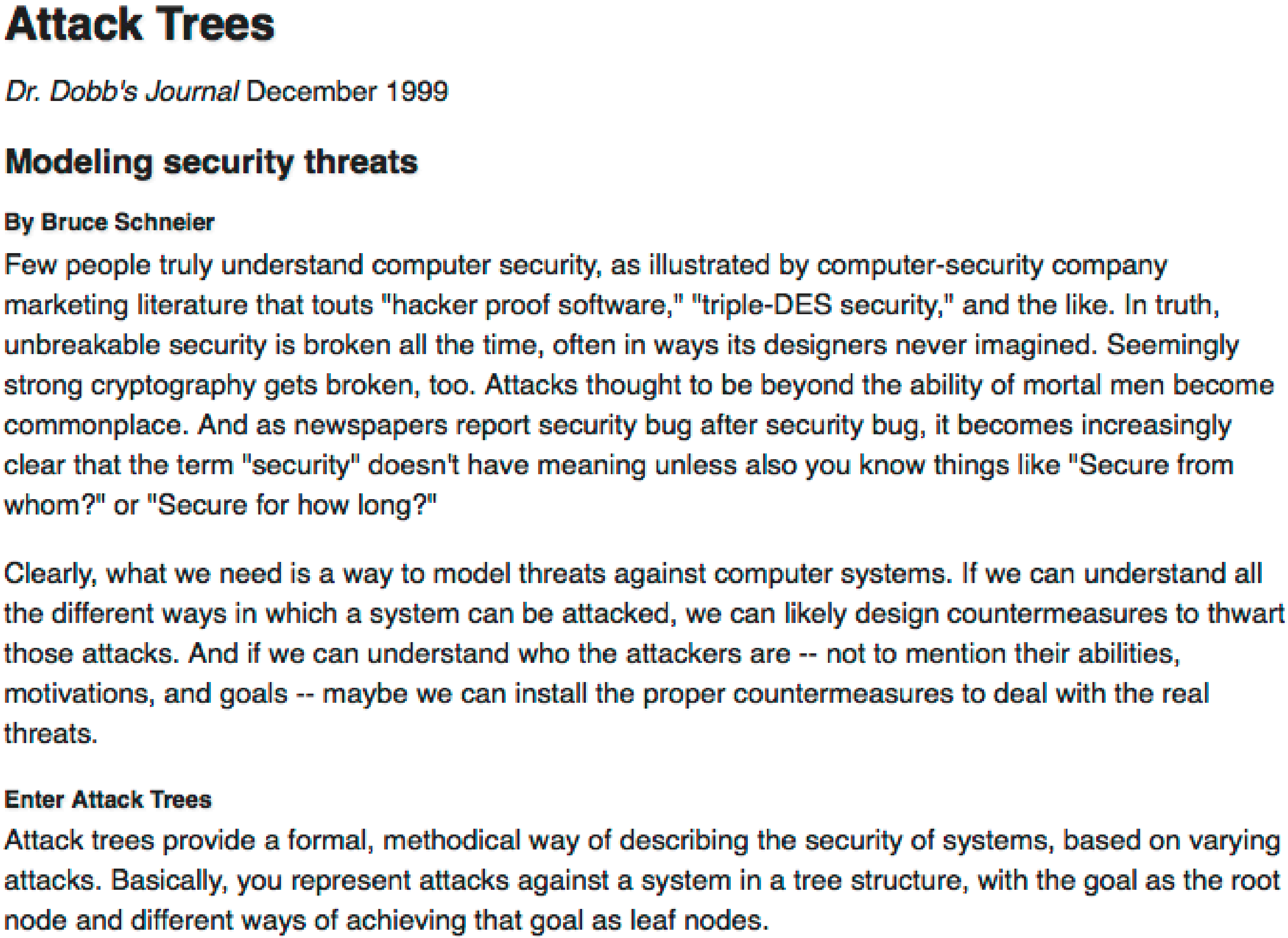
ACT III

A New Century Awaits

http://mirror-us-ga1.gallery.hd.org/_exhibits/places-and-sights/_more1999/_more05/US-NY-NYC-at-night-looking-south-towards-World-Trade-Center-1-AJHD.jpg

1999





Attack Trees

Dr. Dobb's Journal December 1999

Modeling security threats

By Bruce Schneier

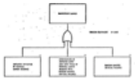
Few people truly understand computer security, as illustrated by computer-security company marketing literature that touts "hacker proof software," "triple-DES security," and the like. In truth, unbreakable security is broken all the time, often in ways its designers never imagined. Seemingly strong 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.

2001



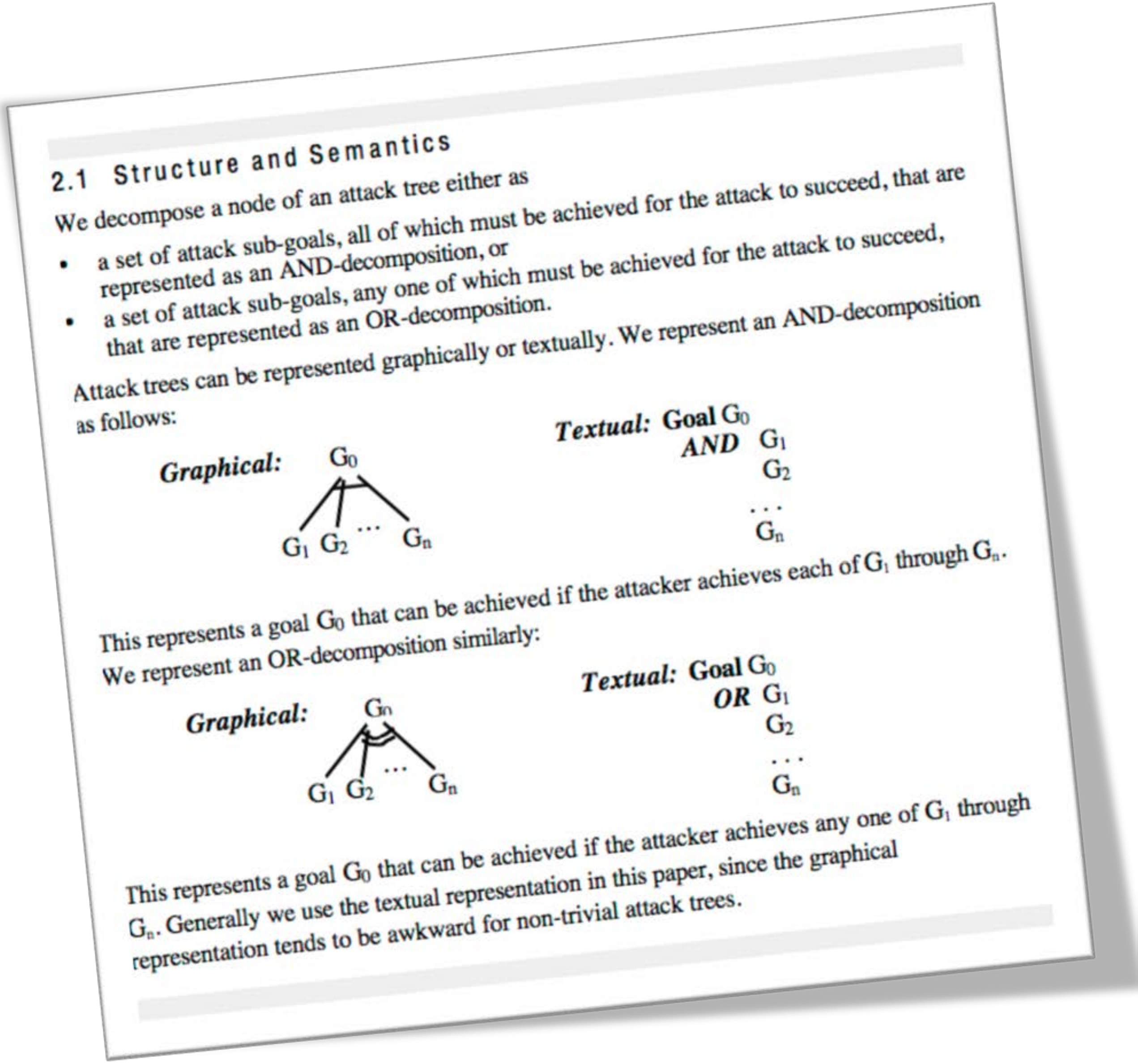
Attack Modeling for Information Security and Survivability

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

March 2001

Survivable Systems

Unlimited distribution subject to the copyright



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:

Graphical:

Textual: **Goal** G_0
AND G_1
G_2
. . .
G_n

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:

Graphical:

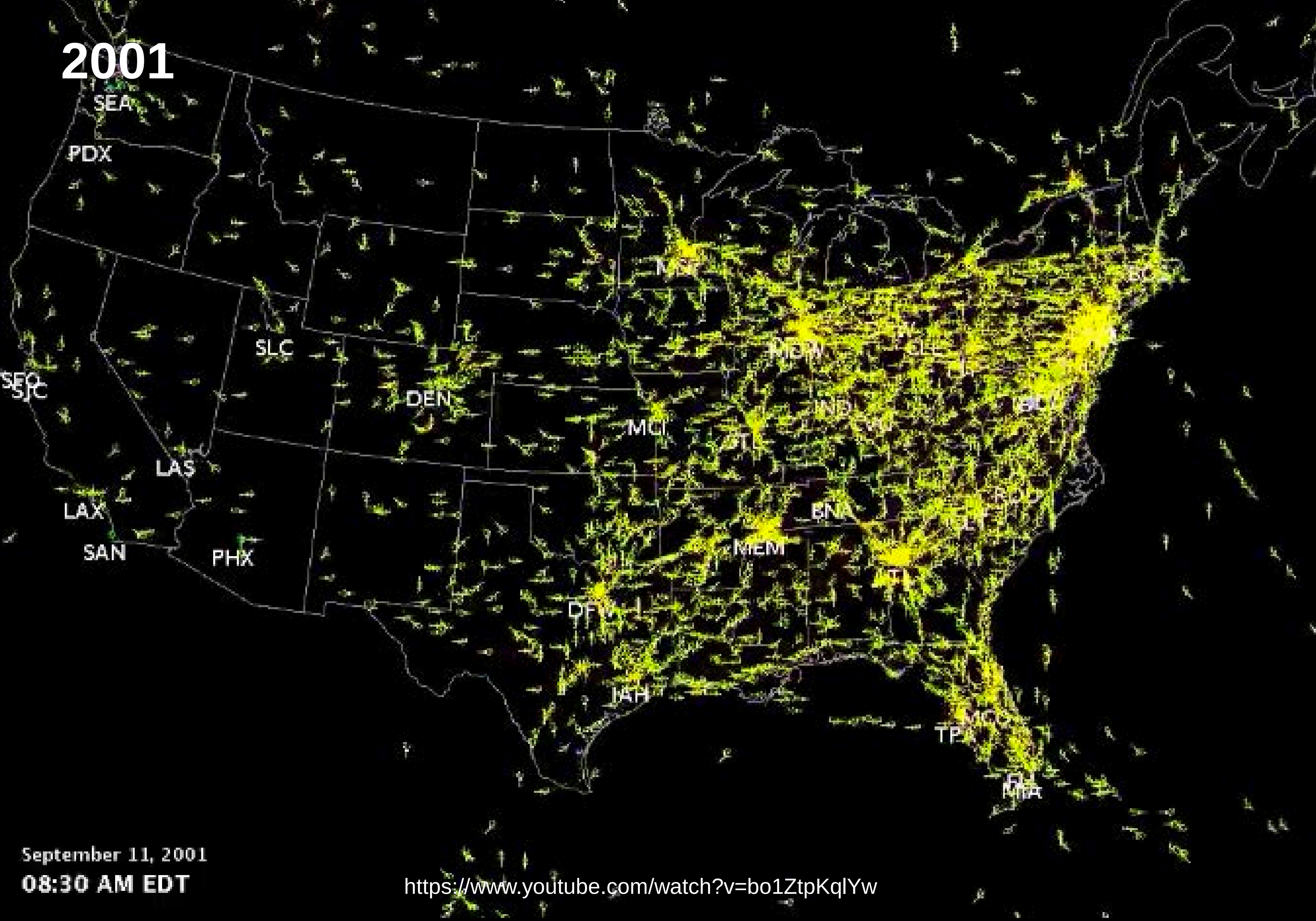
Textual: **Goal** G_0
OR G_1
G_2
. . .
G_n

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

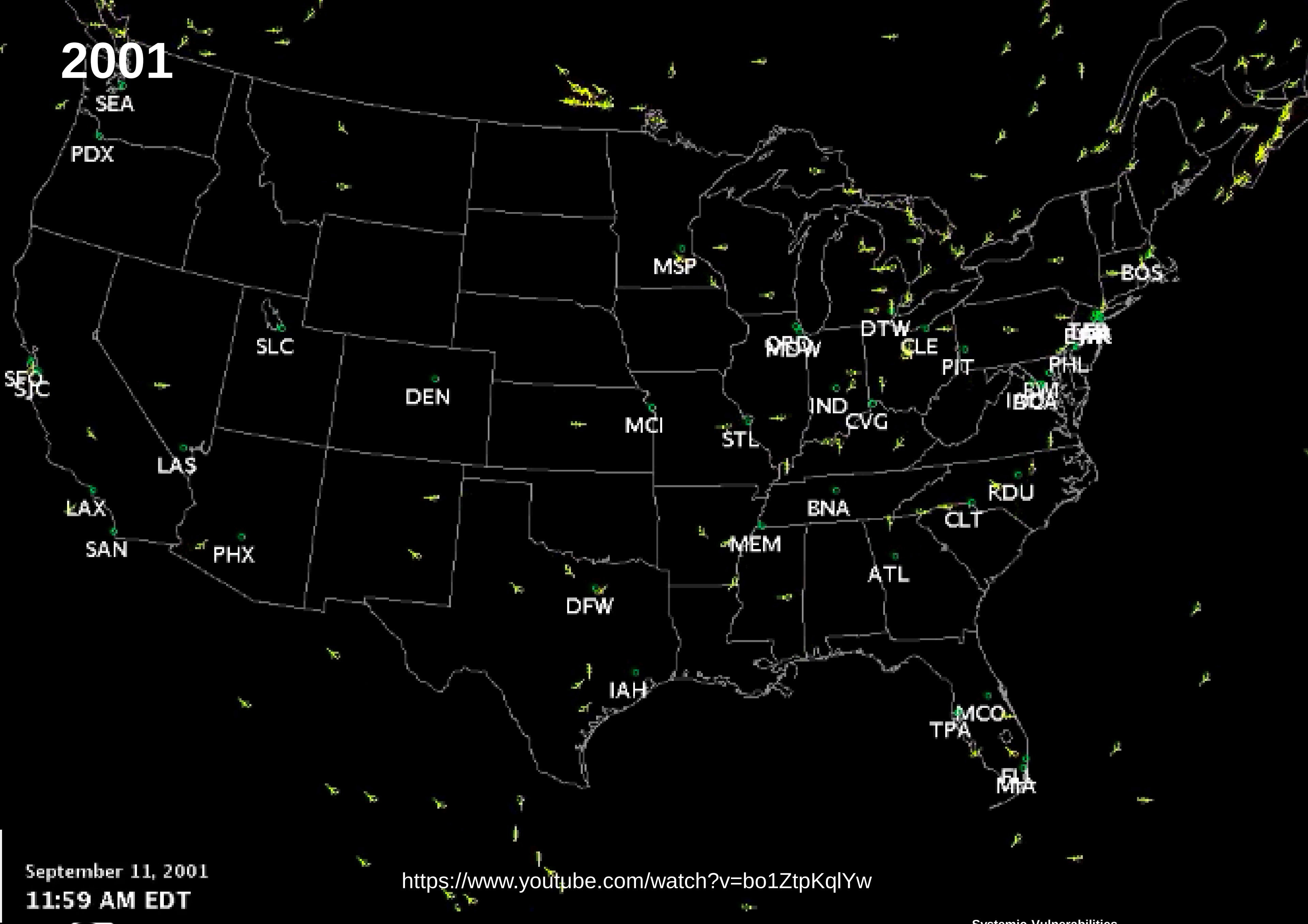
http://en.wikipedia.org/wiki/File:World_Trade_Center,_New_York_City_-_aerial_view_%28March_2001%29.jpg

2001



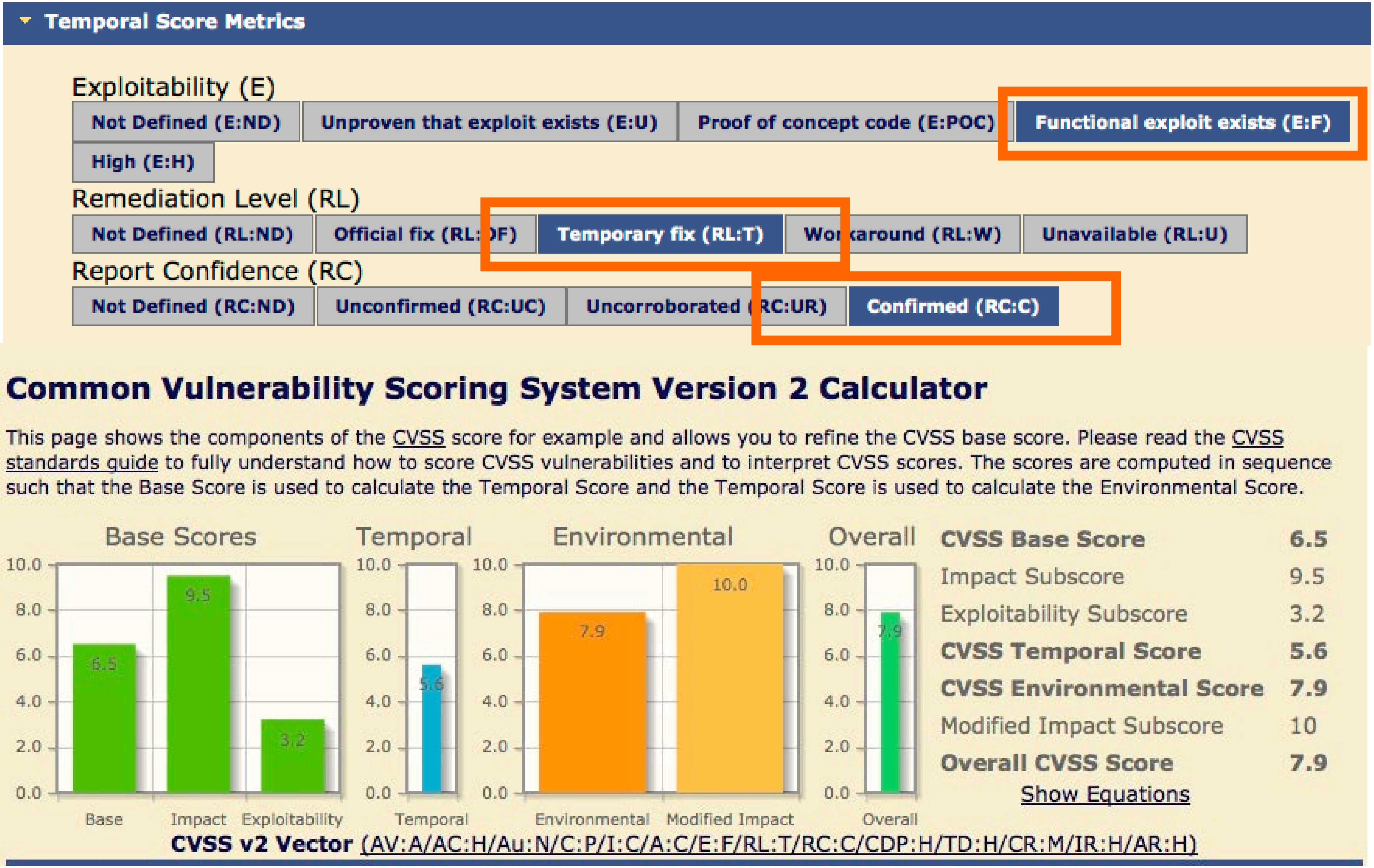
https://www.youtube.com/watch?v=bo1ZtpKqlYw

2001



https://www.youtube.com/watch?v=bo1ZtpKqlYw

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**

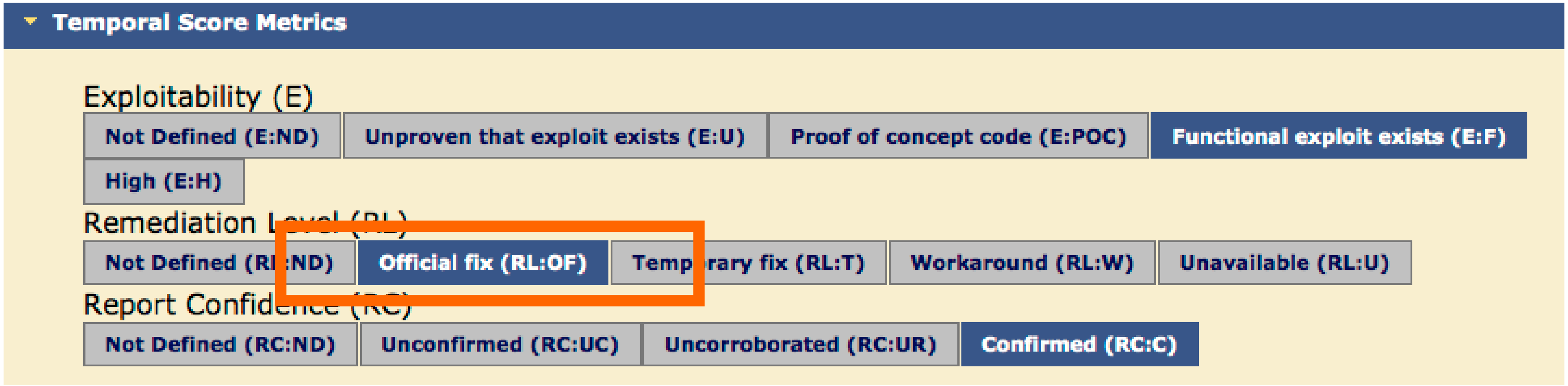
Show Equations

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

CVSS v2 2002



Temporal Score Metrics

Exploitability (E)

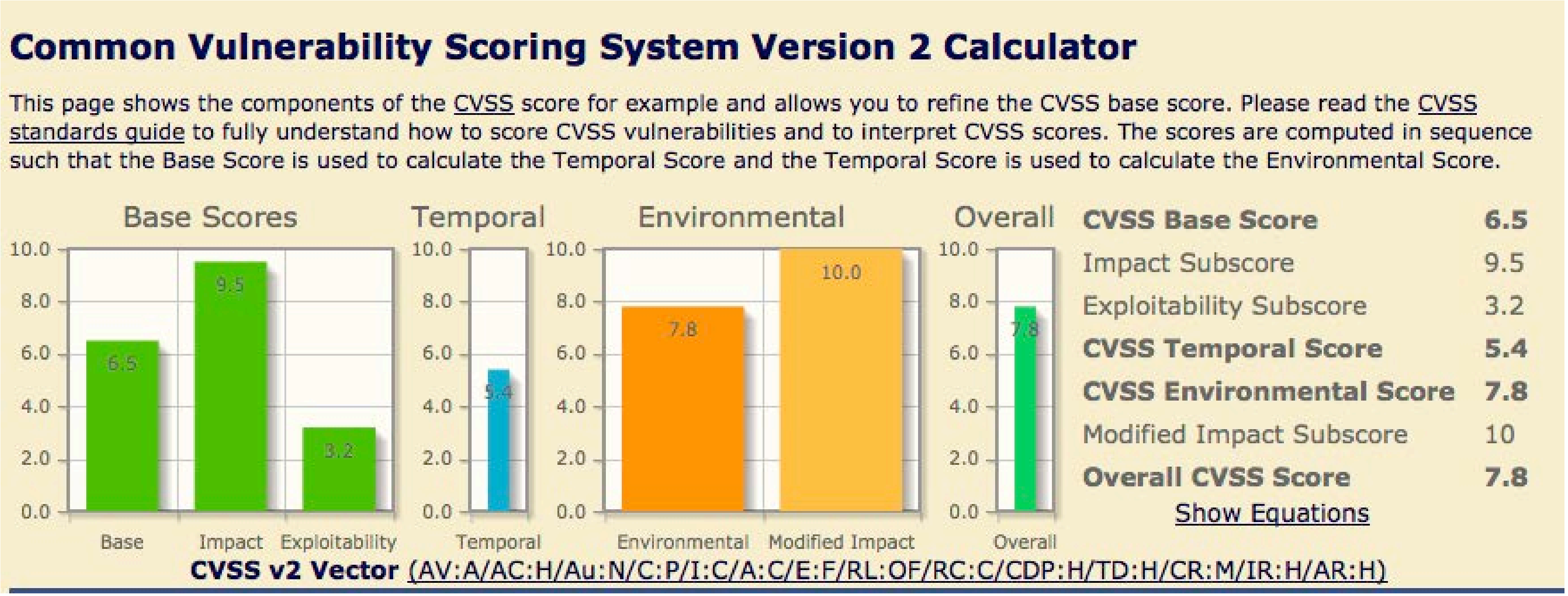
Not Defined (E:ND) | Unproven that exploit exists (E:U) | Proof of concept code (E:POC) | [✓ Functional exploit exists (E:F)] | High (E:H)

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)

2002

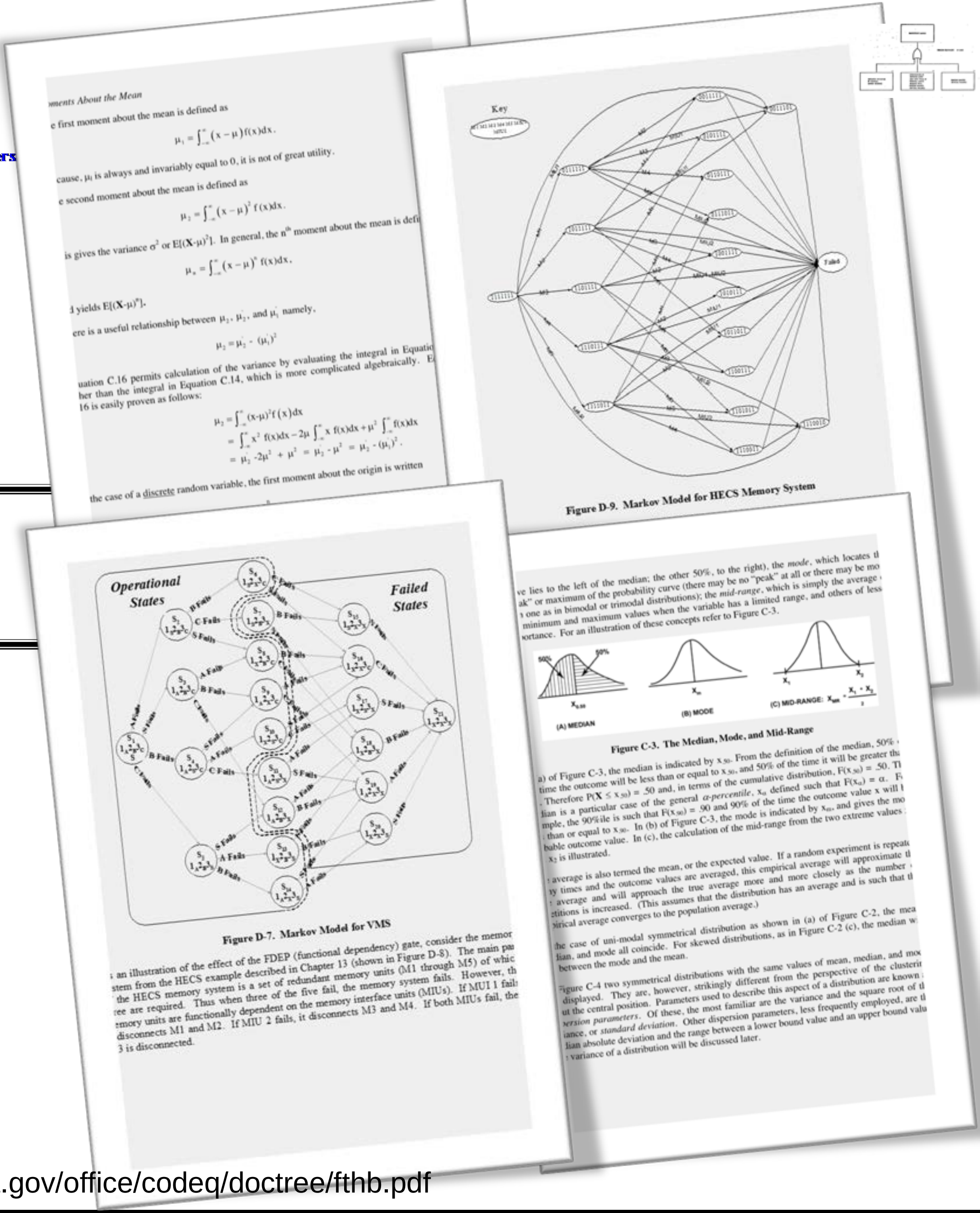
Fault Tree Handbook with Aerospace Applications

Vers

Fault Tree Handbook with Aerospace Applications

Prepared for
NASA Office of Safety and Mission Assurance
NASA Headquarters
Washington, DC 20546

August, 2002



ments About the Mean

e first moment about the mean is defined as

$$\mu_1 = \int_{-\infty}^{\infty} (x-\mu) f(x) dx .$$

cause, μ_1 is always and invariably equal to 0, it is not of great utility.

e second moment about the mean is defined as

$$\mu_2 = \int_{-\infty}^{\infty} (x-\mu)^2 f(x) dx .$$

is gives the variance σ^2 or $E[(\mathbf{X}-\mu)^2]$. In general, the n^{th} moment about the mean is defi

$$\mu_n = \int_{-\infty}^{\infty} (x-\mu)^n f(x) dx ,$$

d yields $E[(\mathbf{X}-\mu)^n]$.

ere is a useful relationship between μ_2, μ_2', and μ_1' namely,

$$\mu_2 = \mu_2' - (\mu_1')^2$$

uation C.16 permits calculation of the variance by evaluating the integral in Equatio
her than the integral in Equation C.14, which is more complicated algebraically. E
16 is easily proven as follows:

$$\begin{aligned} \mu_2 &= \int_{-\infty}^{\infty} (x-\mu)^2 f(x) dx \\ &= \int_{-\infty}^{\infty} x^2 f(x) dx - 2\mu \int_{-\infty}^{\infty} x f(x) dx + \mu^2 \int_{-\infty}^{\infty} f(x) dx \\ &= \mu_2' - 2\mu^2 + \mu^2 = \mu_2' - \mu^2 = \mu_2' - (\mu_1')^2 . \end{aligned}$$

the case of a discrete random variable, the first moment about the origin is written

Figure D-9. Markov Model for HECS Memory System

Figure D-7. Markov Model for VMS

an illustration of the effect of the FDEP (functional dependency) gate, consider the memor
stem from the HECS example described in Chapter 13 (shown in Figure D-8). The main pa
the HECS memory system is a set of redundant memory units (M1 through M5) of whic
ree are required. Thus when three of the five fail, the memory system fails. However, th
emory units are functionally dependent on the memory interface units (MIUs). If MUI 1 fail
disconnects M1 and M2. If MIU 2 fails, it disconnects M3 and M4. If both MIUs fail, the
3 is disconnected.

ve lies to the left of the median; the other 50%, to the right), the *mode*, which locates th
ak" or maximum of the probability curve (there may be no "peak" at all or there may be mo
one as in bimodal or trimodal distributions); the *mid-range*, which is simply the average
minimum and maximum values when the variable has a limited range, and others of less
ortance. For an illustration of these concepts refer to Figure C-3.

Figure C-3. The Median, Mode, and Mid-Range

a) of Figure C-3, the median is indicated by $x_{.50}$. From the definition of the median, 50%
time the outcome will be less than or equal to $x_{.50}$, and 50% of the time it will be greater tha
. Therefore $P(\mathbf{X} \le x_{.50}) = .50$ and, in terms of the cumulative distribution, $F(x_{.50}) = .50$. Th
lian is a particular case of the general *α-percentile*, x_α defined such that $F(x_\alpha) = \alpha$. F
mple, the 90%ile is such that $F(x_{.90}) = .90$ and 90% of the time the outcome value x will b
than or equal to $x_{.90}$. In (b) of Figure C-3, the mode is indicated by x_m, and gives the mo
bable outcome value. In (c), the calculation of the mid-range from the two extreme values
x_2 is illustrated.

average is also termed the mean, or the expected value. If a random experiment is repeat
ny times and the outcome values are averaged, this empirical average will approximate th
average and will approach the true average more and more closely as the number
etitions is increased. (This assumes that the distribution has an average and is such that th
pirical average converges to the population average.)

he case of uni-modal symmetrical distribution as shown in (a) of Figure C-2, the mea
lian, and mode all coincide. For skewed distributions, as in Figure C-2 (c), the median w
between the mode and the mean.

Figure C-4 two symmetrical distributions with the same values of mean, median, and mo
displayed. They are, however, strikingly different from the perspective of the clusterin
ut the central position. Parameters used to describe this aspect of a distribution are known
persion parameters. Of these, the most familiar are the variance and the square root of th
iance, or *standard deviation*. Other dispersion parameters, less frequently employed, are th
lian absolute deviation and the range between a lower bound value and an upper bound valu
variance of a distribution will be discussed later.

http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf

2003

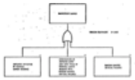
Veterans of the Challenger experience say that it sounds cautious and logical to argue that all potential causes of the disaster should be examined and eliminated, one by one.

…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

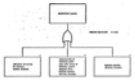
http://static.ddmcdn.com/gif/shuttle-columbia-launch-660x433-130201-1.jpg

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 Community 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

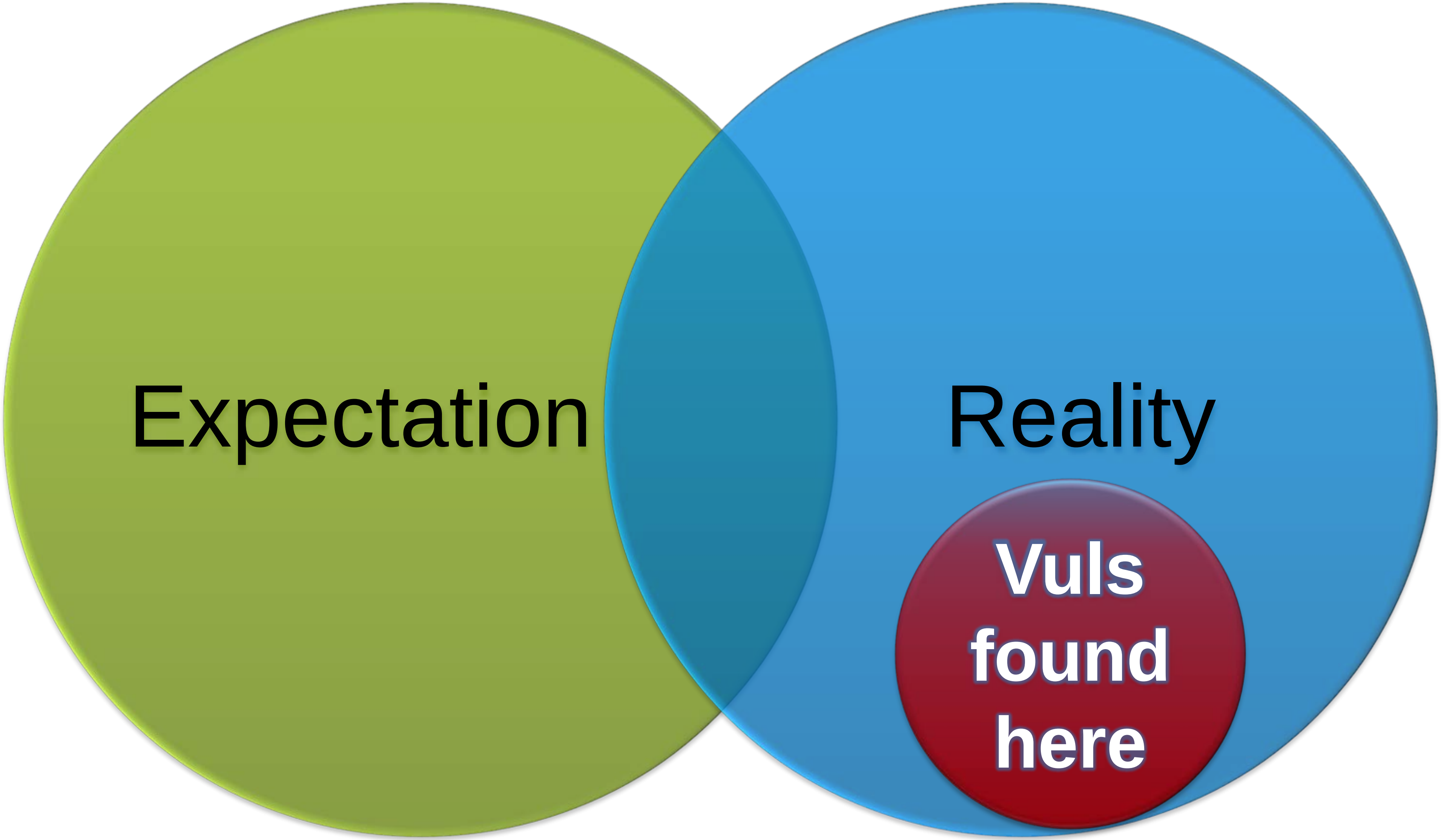
Dana Epp, Microsoft MVP - Enterprise and Developer Security

http://technet.microsoft.com/en-us/security/hh778966.aspx

ACT IV

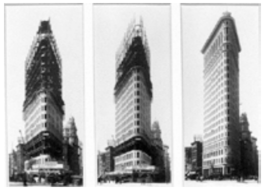
Whither From Here?

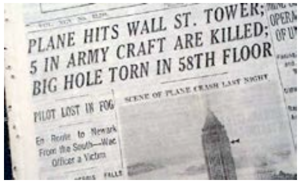
Vulnerability Discovery in One Diagram



Build Security In?

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





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

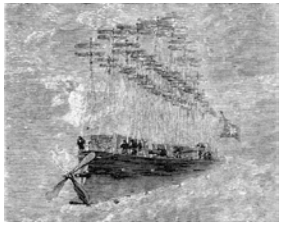
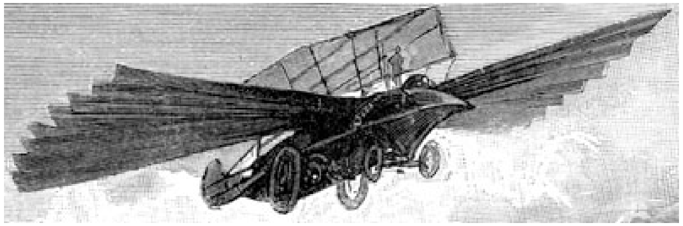
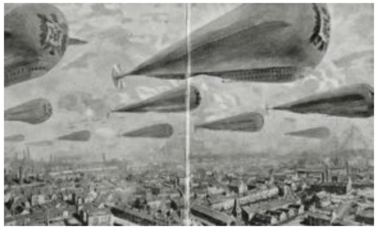
PILOT LOST IN FOG

En Route to Newark From the South—War Officer a Victim

SCENE OF PLANE CRASH LAST NIGHT

OPERA
OF U

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**.

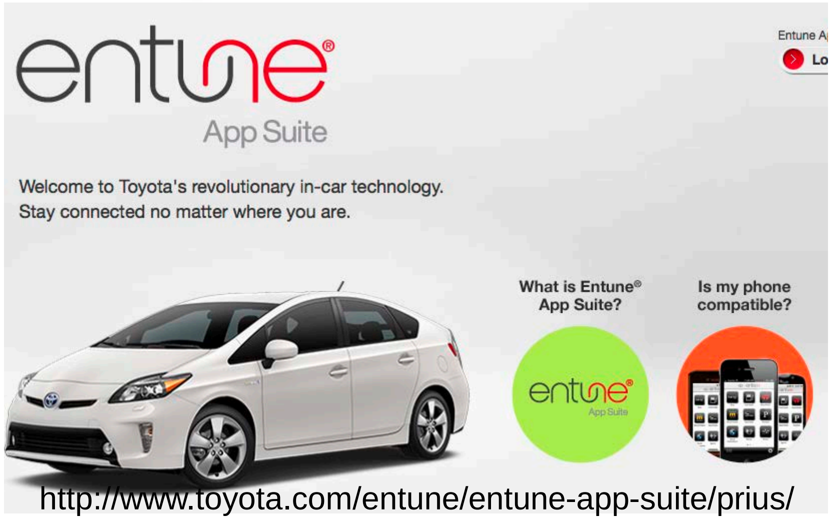
That combination -- **long lived and not reachable** -- is the trend that **must be dealt with**, possibly even reversed.

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

Points to ponder

How long will your next refrigerator last?

How about your next car?



entune® App Suite

Welcome to Toyota's revolutionary in-car technology.
Stay connected no matter where you are.

What is Entune® App Suite?

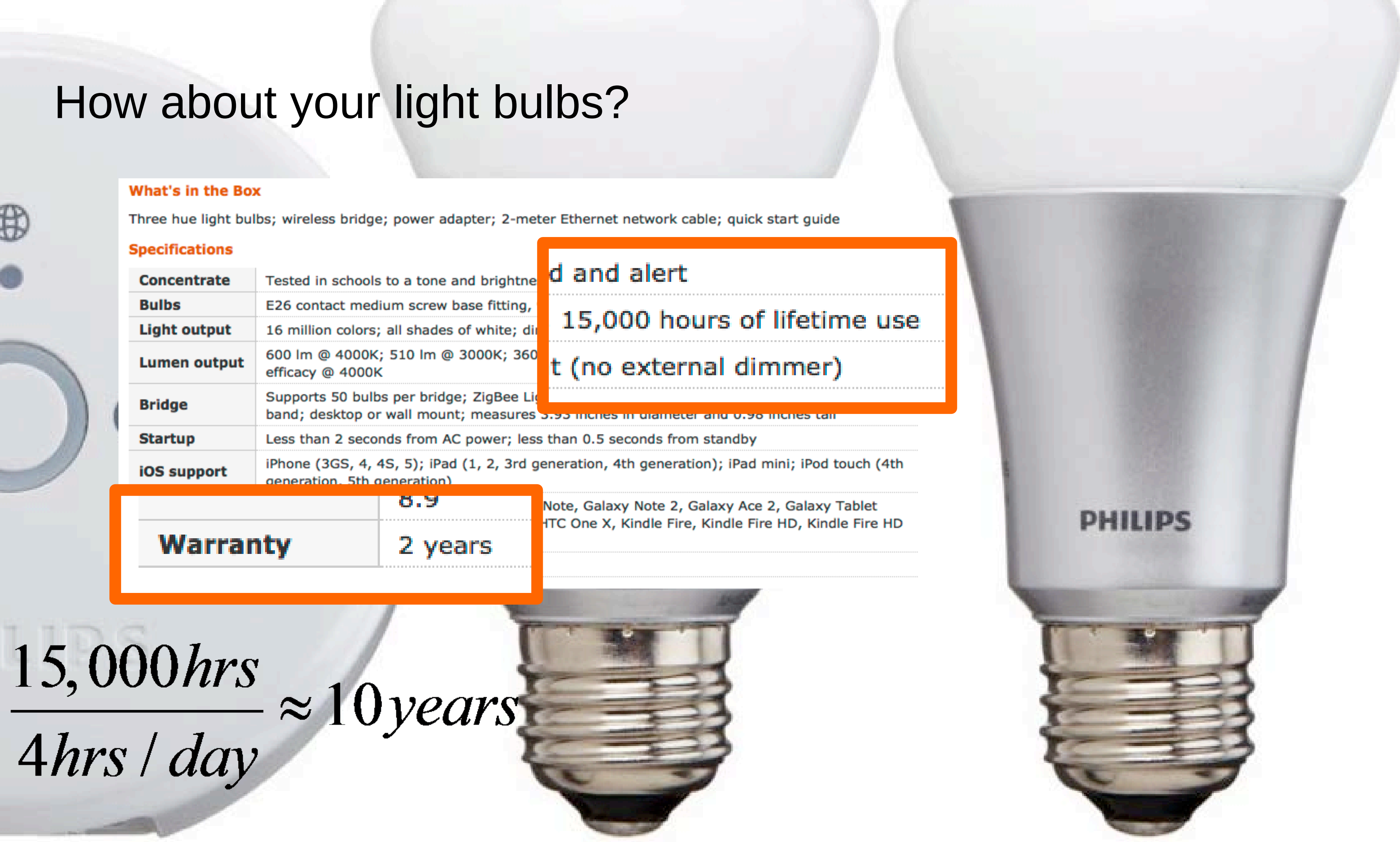
Is my phone compatible?

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 network cable; quick start guide

Specifications

Concentrate	Tested in schools to a tone and brightne
Bulbs	E26 contact medium screw base fitting,
Light output	16 million colors; all shades of white; di
Lumen output	600 lm @ 4000K; 510 lm @ 3000K; 360 efficacy @ 4000K
Bridge	Supports 50 bulbs per bridge; ZigBee Li 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 generation, 5th generation)
	Note, Galaxy Note 2, Galaxy Ace 2, Galaxy Tablet HTC One X, Kindle Fire, Kindle Fire HD, Kindle Fire HD

d and alert

15,000 hours of lifetime use

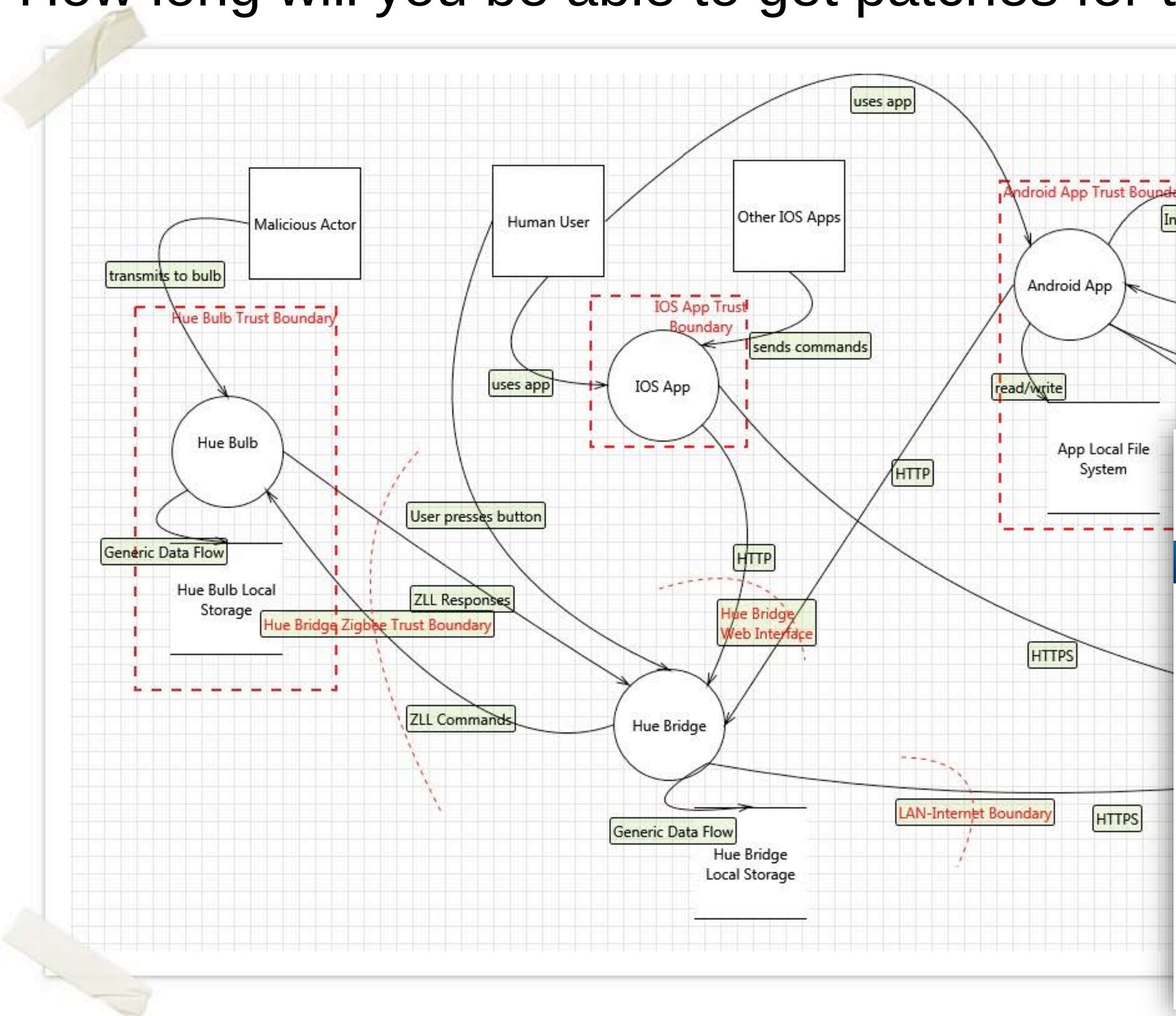
t (no external dimmer)

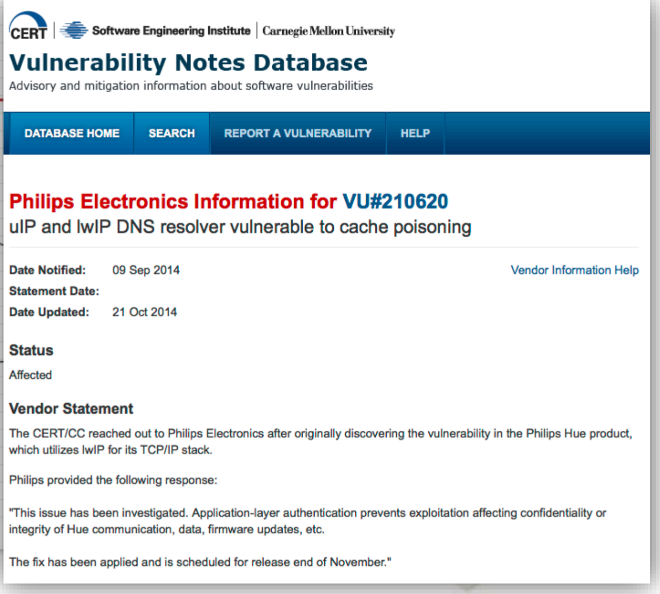
	8.9
Warranty	2 years

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

Points to ponder

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




CERT | Software Engineering Institute | Carnegie Mellon University
DATABASE HOME
SEARCH
REPORT A VULNERABILITY
HELP

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

Philips Electronics Information for VU#210620

uIP and lwIP DNS resolver vulnerable to cache poisoning

Date Notified: 09 Sep 2014

Statement Date:

Date Updated: 21 Oct 2014

Vendor Information Help

Status

Affected

Vendor Statement

The CERT/CC reached out to Philips Electronics after originally discovering the vulnerability in the Philips Hue product, which utilizes lwIP for its TCP/IP stack.

Philips provided the following response:

"This issue has been investigated. Application-layer authentication prevents exploitation affecting confidentiality or integrity of Hue communication, data, firmware updates, etc.

The fix has been applied and is scheduled for release end of November."

So now what?

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

Defense mechanisms

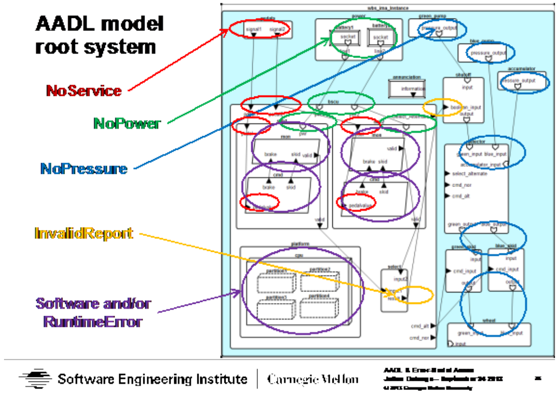
- Field upgradability
- Layered defenses
- Planned obsolescence
- Read more Science Fiction

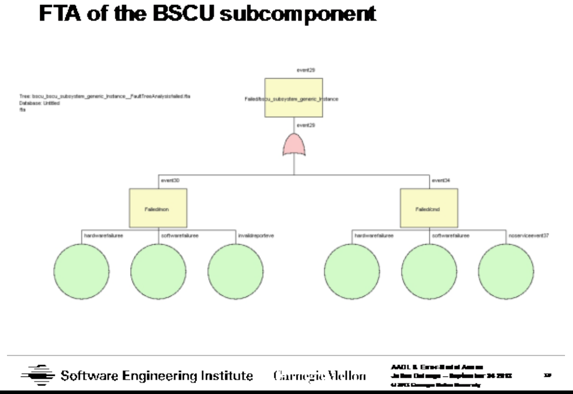
Ongoing work at CERT, SEI

Vulnerability Discovery & Systemic Vulnerability Programs

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

Model-driven architecture with automated fault & safety analysis


AADL model root system


FTA of the BSCU subcomponent

This talk inspired by…

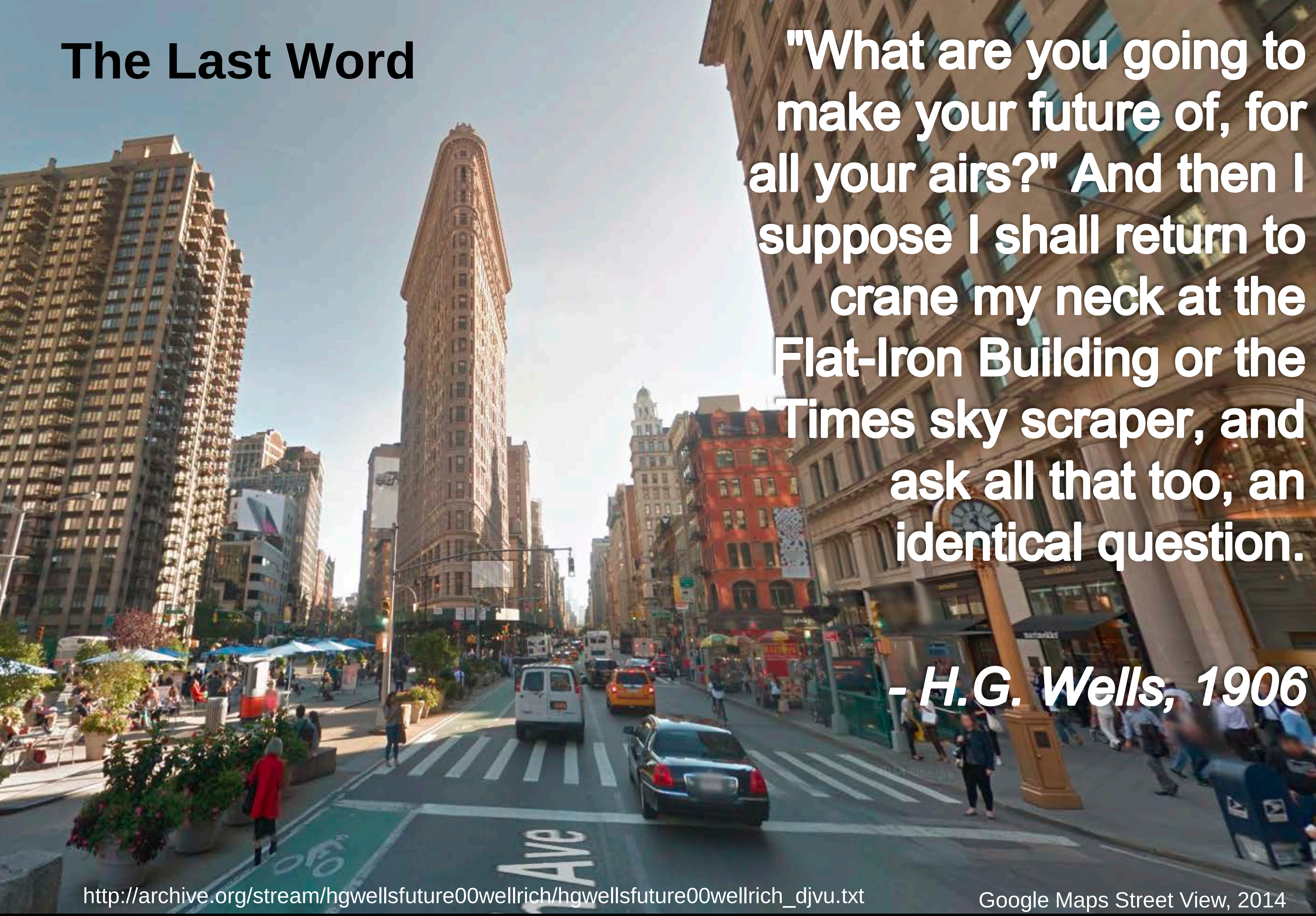
KC-135s from the 171st Air Refueling Wing often circle the Pittsburgh area. From the perspective of my office at CMU looking out at the view seen here, the planes usually fly right above or behind the Cathedral of Learning.

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

The Last Word



"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