

# **Software Quality Engineering Tackles Security Issues**

**Taz Daughtrey**  
Senior Scientist  
Quanterion Solutions, Inc.

*Software Quality Group of New England  
12 June 2013*

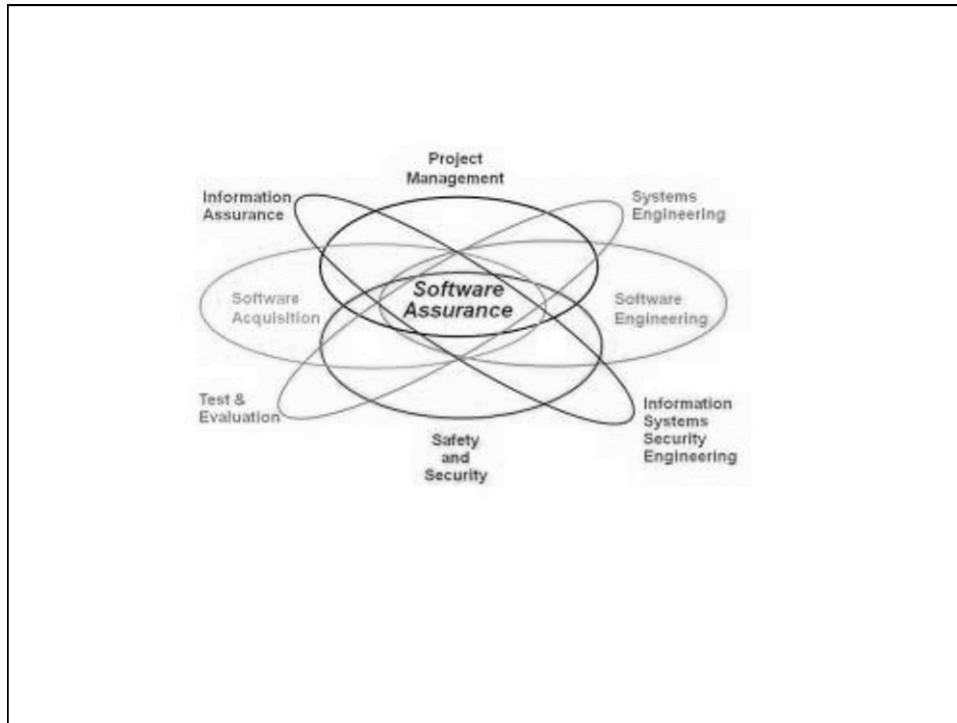
# **Software Quality Engineering Tackles Security Issues**

**Taz Daughtrey**  
Cyber Security Information Analysis Center



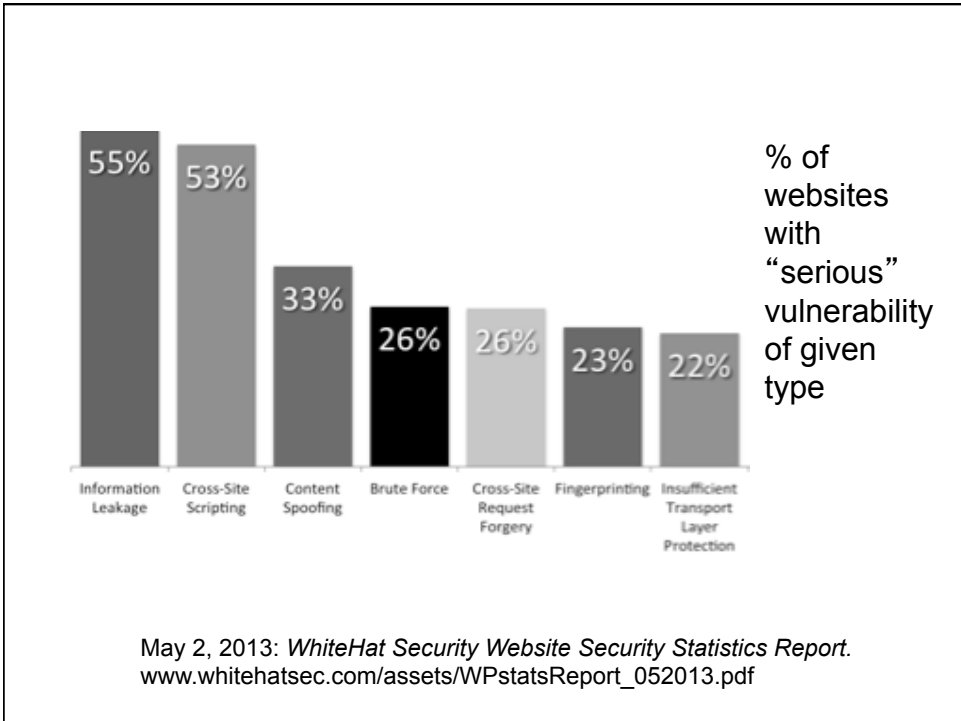
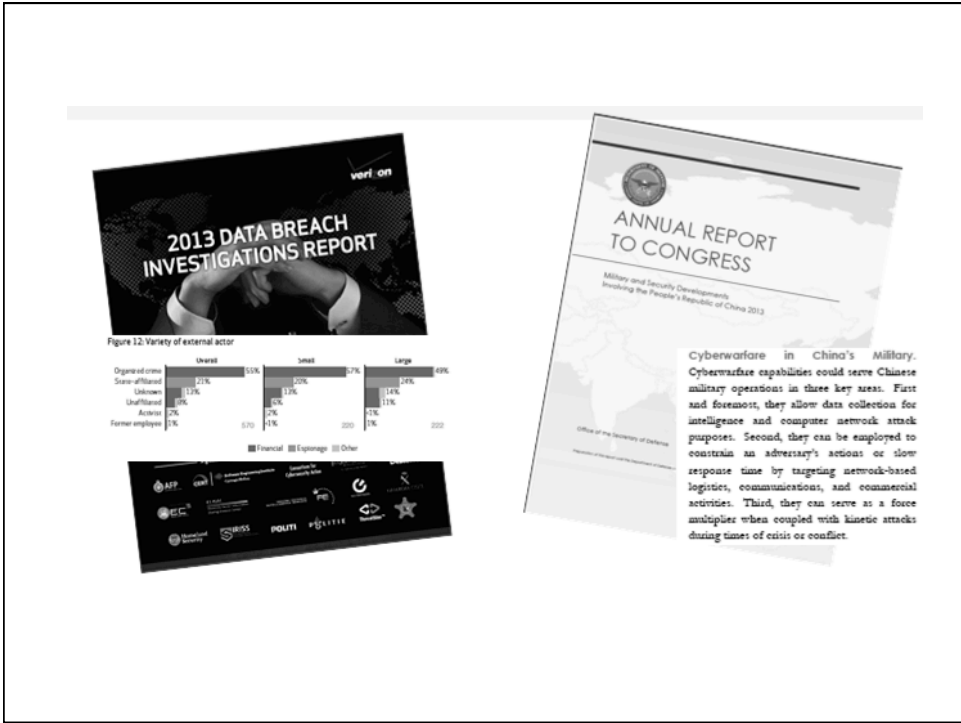
**American Software Testing Qualifications Board**





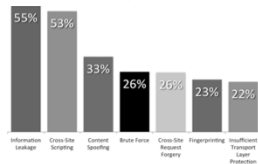
**Cybercrime Ring is Busted for \$45 Million Theft**  
-- Wall Street Journal May 9, 2013

"This was a 21st century bank heist that reached through the Internet to span the globe. But, instead of guns and masks, this cybercrime organization used laptops and malware."



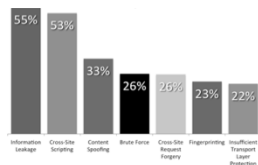
## “Serious” vulnerabilities: attacker could

- > take control over all or part of website
- > compromise user accounts on system
- > access sensitive data
- > violate compliance requirements
- > possibly make headline news.



***In short, serious vulnerabilities are those that should really be fixed.***

**86 percent** of all websites tested were found to have at least one “serious” vulnerability ...



and were exposed every day of 2012.

The **average** number of vulnerabilities per website, from 2011 to 2012: **79 → 56.**

Make it.

9

acceptable

Make it.

Make it work.

11

functional

acceptable

Make it.

Make it work.

Make it work right.

13

correct

functional

acceptable

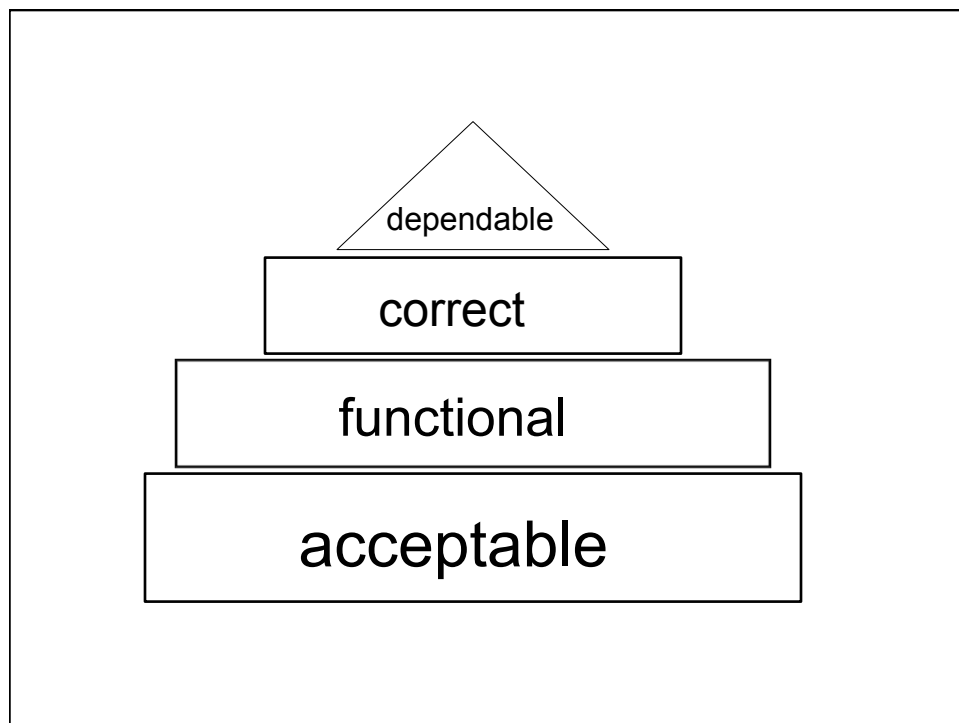
Make it.

Make it work.

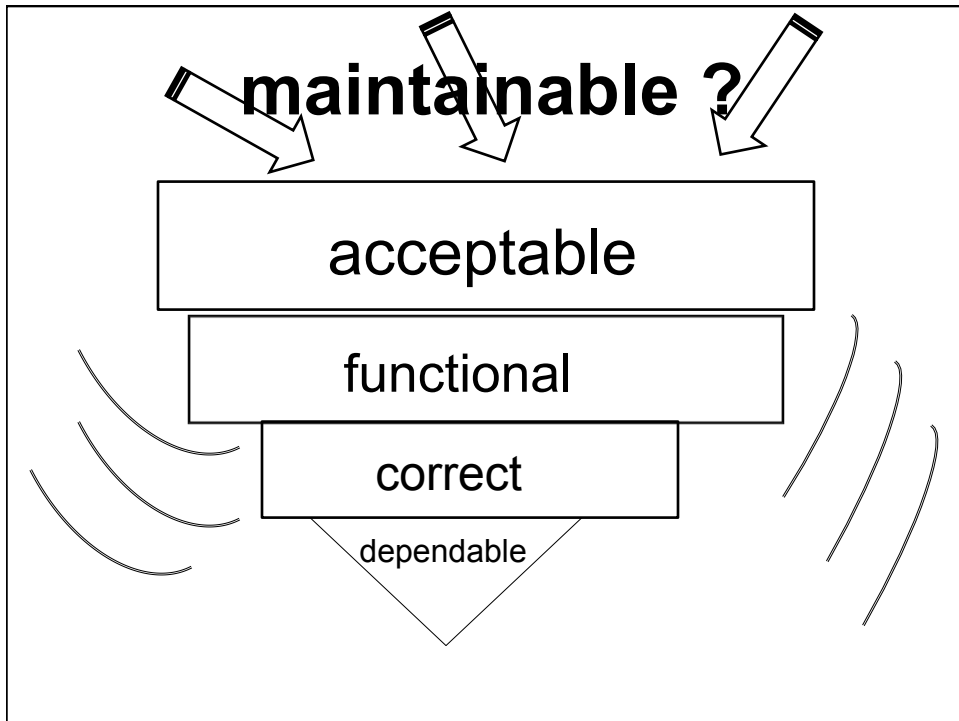
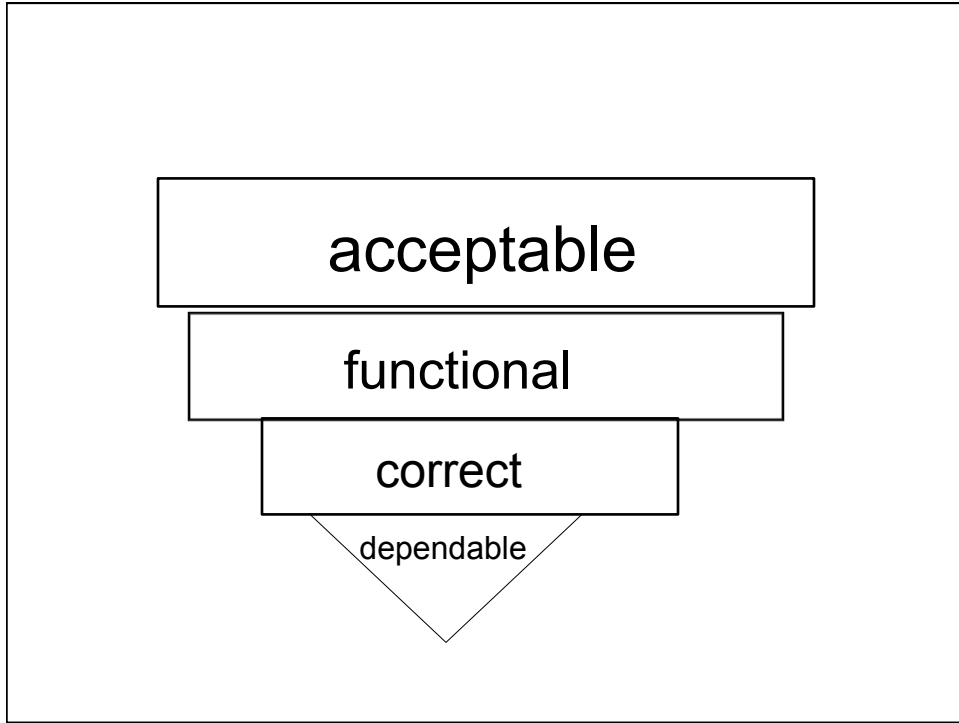
Make it work right.

Make it work right, regardless ...

15





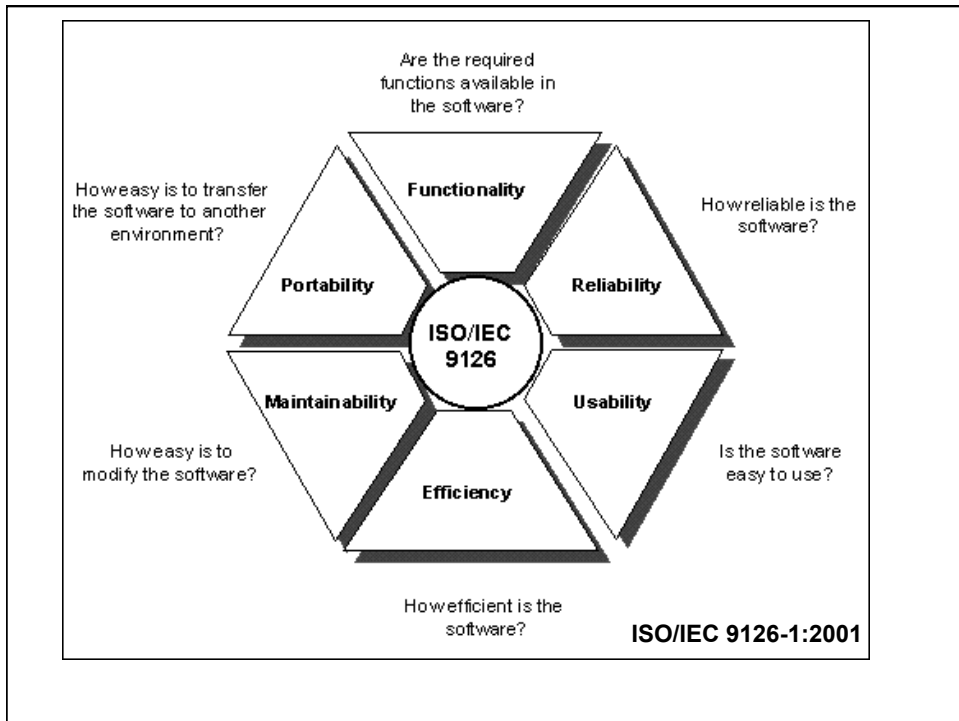
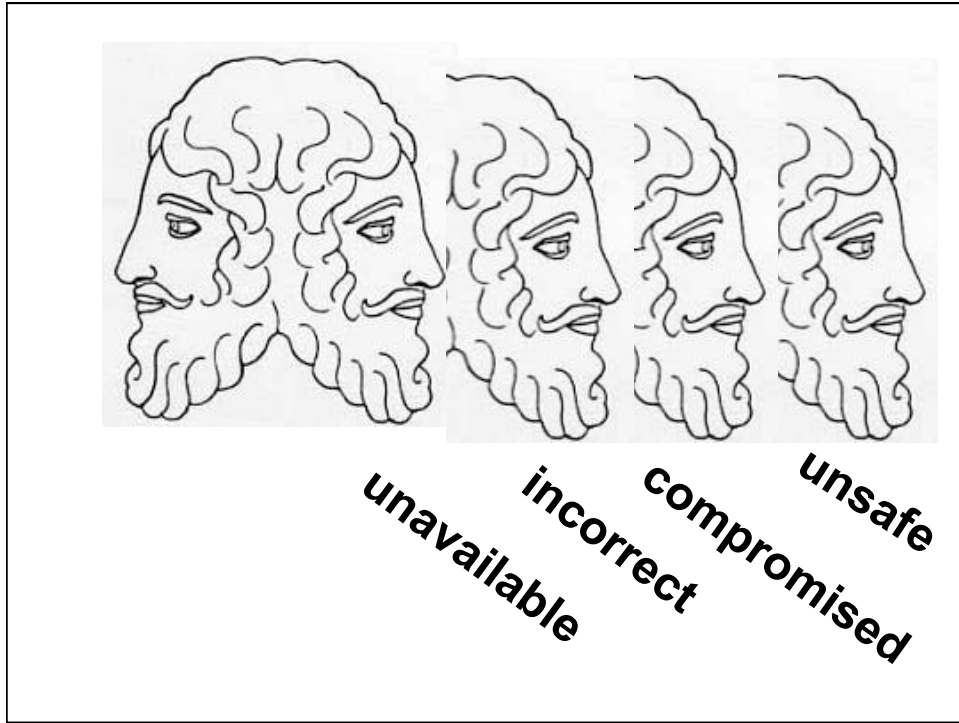




**Reliability:** *does what is expected*

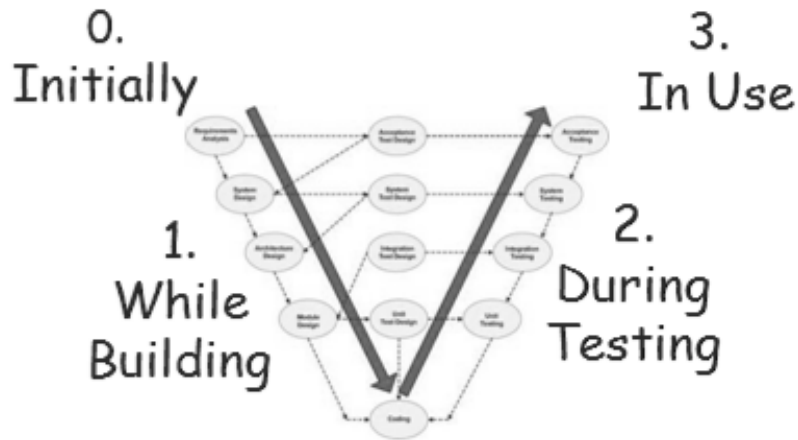


**Unreliability:** *doesn't do what is expected*

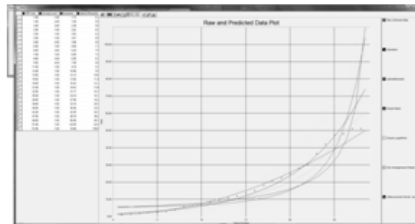




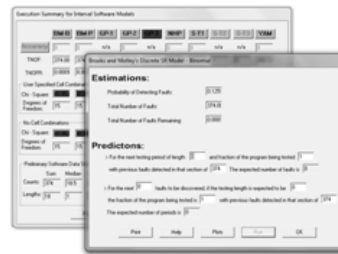
# Software Reliability Modeling



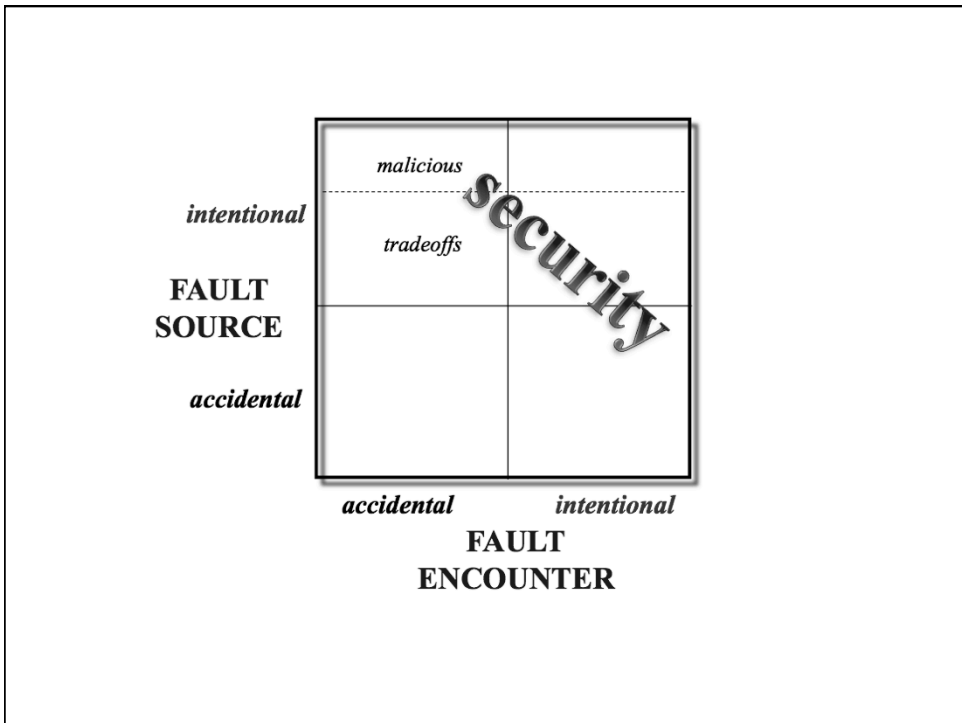
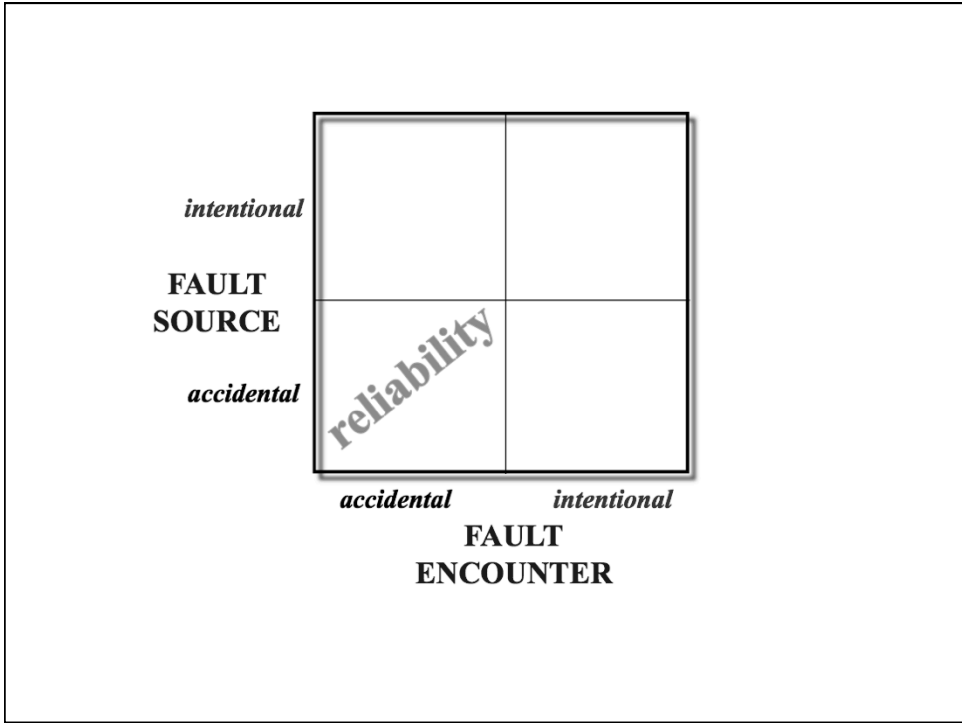
## Statistical Modeling and Estimation of Reliability Functions for Software



Typical SMERFS Output Curves



Typical SMERFS Output Calculations



## Software Security Engineering

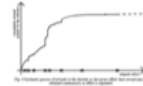


Establish multiple quantitative targets

Use threat modeling to identify abuse cases



Rethink software reliability growth modeling



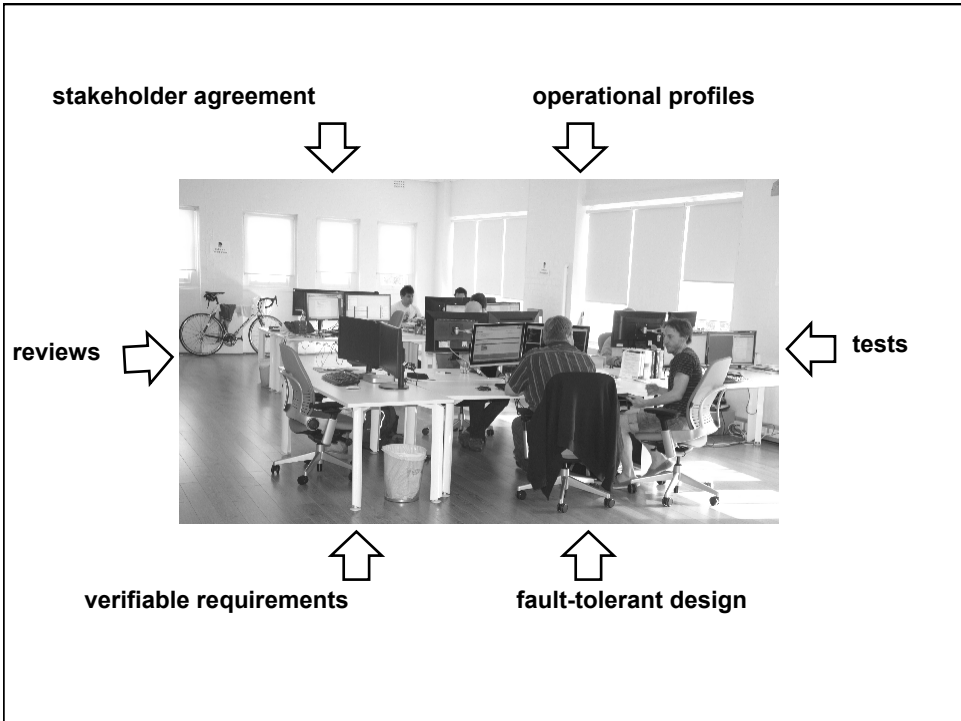
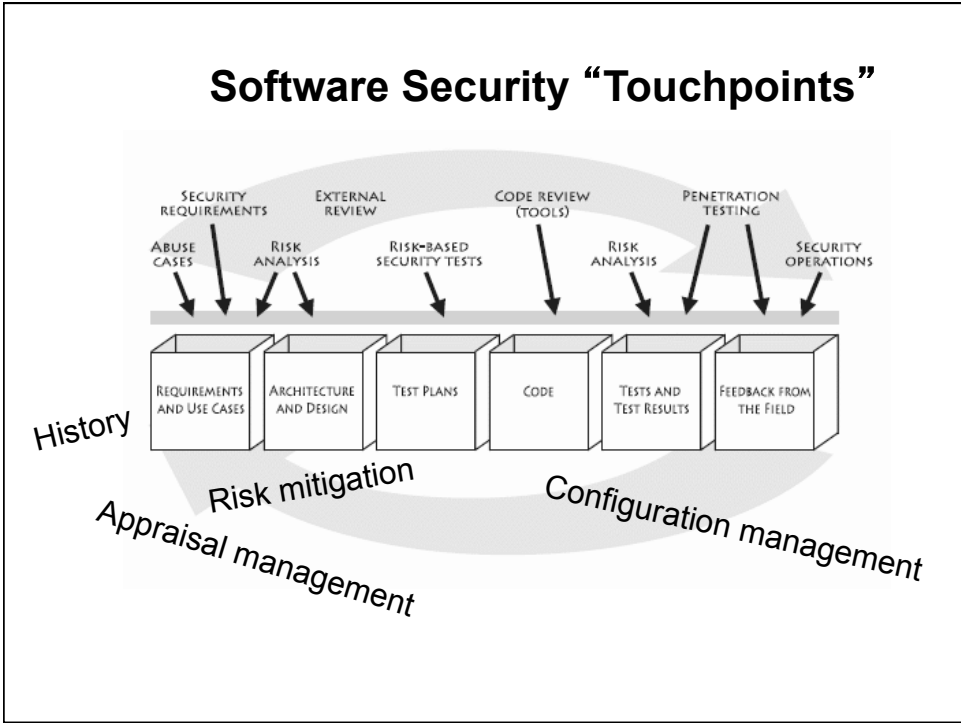
## Software Security Engineering

confidentiality

integrity



accessibility





Ozmet (2005) analyzed OpenBSD 2.2 data

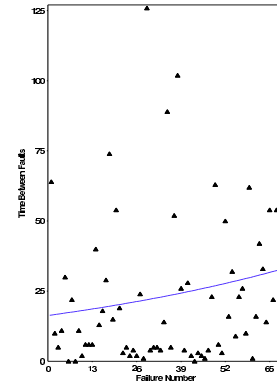
Berkeley Software Distribution = Unix-derived OS

79 vulnerabilities discovered 1998-2002

Applied reliability growth models in SMERFS

Found best fit from  
Musa logarithmic model

Acceptable results also from  
other models

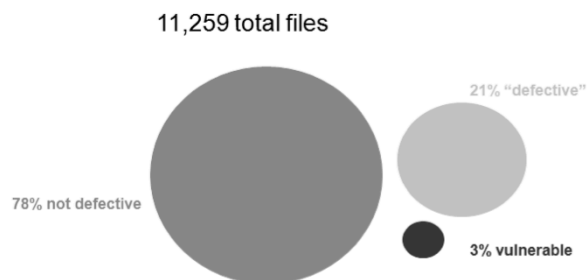


“Software Security Growth Modeling: Examining Vulnerabilities with Reliability Growth Models.” Andy Ozment, University of Cambridge. First Workshop on Quality of Protection, Milan, Italy, September 15, 2005.

Shin and Williams (2013) analyzed Firefox web browser

Used fault prediction models based on traditional metrics

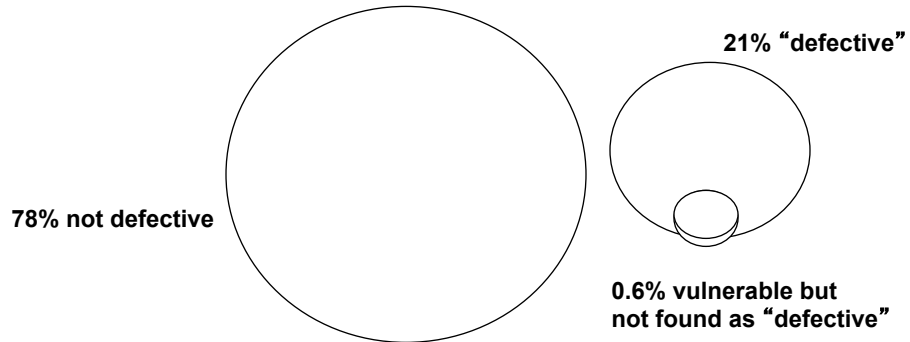
Found valid to predict vulnerabilities, although with high rate of false positives



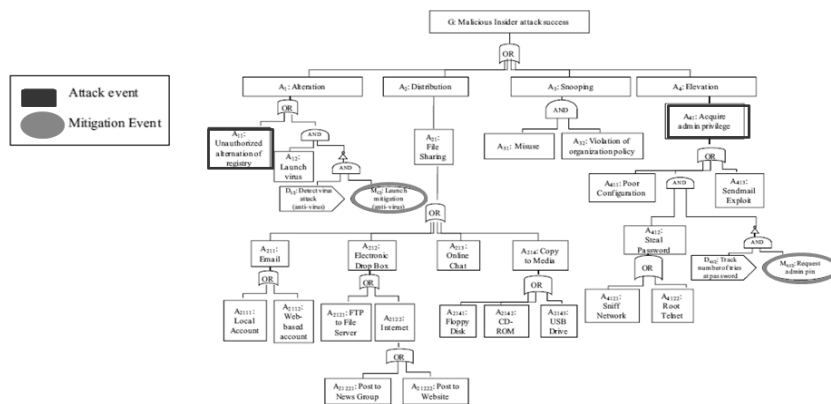
“Can traditional fault prediction models be used for vulnerability prediction?” Yonghee Shin (DePaul University) and Laurie Williams (North Carolina State University). Empirical Software Engineering (2013) 18:25-59.

## Shin and Williams (2013) ... Firefox web browser

11,259 total files



## Software Security Modeling



Attack + Countermeasure Tree

## Security Risk Exposure =



**Probability** of occurrence

**X**

**Consequence** of occurrence



## Security Risk Exposure =



**Probability** of occurrence

(knowledge \* skill \* resources \* motivation)

**X**

**Consequence** of occurrence



# Security Risk Exposure =



**Probability** of occurrence

(knowledge \* skill \* resources \* motivation)

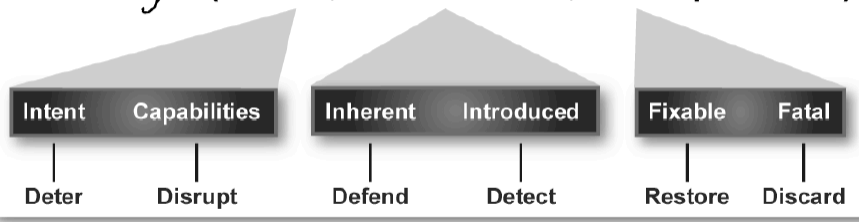
**X**



**Consequence** of occurrence



$$\text{Risk} = f(\text{threat, vulnerabilities, consequences})$$



Risk Management Parameters

*Resilient Military Systems and the Advanced Cyber Threat*  
Defense Science Board Task Force Report: January 2013


**ROI = return  
investment**

**ROSI = risk exposure reduction  
security investment**




## Cyber Security and Information Systems Information Analysis Center

---



[Ask CSIAAC](#)
[Websites](#)
[Community](#)
[My stuff](#)

---



**Software Security Growth Modeling**  
Security growth modeling, analogous to reliability growth modeling, is an attempt to quantify how the projected security of a system increases with additional detection and removal of... read more

**Presenter:**  
Taz Daughtrey  
Senior Software Quality Scientist

**Related:**

- Webinar Videos
- Journal: Software Reliability Engineering
- Security and Software Assurance Programs

**Automated Test and Re-Test (ATR)**

**Quantifying Uncertainty in Early Lifecycle Cost Estimation**

**Software Security Growth Modeling**

**Social Media Analytics and Privacy**

**Managing Technical Debt**

**CSIAAC Software Engineering**  
Intensive Systems Engineering includes the entire field of software and systems engineering.

**CSIAAC M&S Modeling & Simulation**  
Modeling and Simulation (M&S) is the use of models, including emulators, prototypes, simulators, and stimulators, either statically

**Upcoming events**


**May 18** 11th Annual Conference on Systems Engineering Research (CSER 2013) Location: Georgia Institute of Technology, Atlanta, Georgia  
Group:

**Apr 7** Defense Intelligence Worldwide Location: Baltimore Convention Center Group: Software Intensive Systems Engineering, Knowledge Management & Information Sharing, Information Assurance, Modeling & Simulation


**Apr 28** APOC's 2013 Knowledge Management Conference Location: Houston, Texas Group: Knowledge Management & Information Sharing

**Sept 4** 14th European Conference on Knowledge Management Location: Kaunas, Lithuania Group: Knowledge Management &

## Community of Practice → Practical Products



discussion



SMES

**CSIAAC Learning from Success Stories**  
A CSIAAC Topical Report  
September 2012

This study represents another investigation into the use of professional social media to produce useful products dealing with software-intensive systems engineering.

Tom McElbourn, reading to yet another story of a massively dysfunctional development project (FBI case management system) asked "Are there any successful large and complex modern day software system stories out there? What were the success factors?"

Several responses included citations, which could be the basis for including in a publishable case study. As with others also suggested, it's not immediately clear how many "lessons learned" would apply to development methodologies, to project management, or to other aspects.

Base Strike Right corner: Flanagan, C. "They Wrote the Right Stuff." *Real Company*, December 1994.

2000 Olympick, K. Gabbay, K. "Methods to evaluate non-represented software based on real time execution results." *IEEE Systems Journal*, January 2005.

CSIAAC Direct, a real time testing platform, is featured at [www.csiaac.gov/CSIAACDirect/News/NewsItem.aspx?NewsID=100](http://www.csiaac.gov/CSIAACDirect/News/NewsItem.aspx?NewsID=100)

Business concept: providing online environment, auditing and getting services. Berlin, C.O. "The Evolution of Super Apps: Building Software Creativity." <http://www.innovationtoday.com/2012/07/>

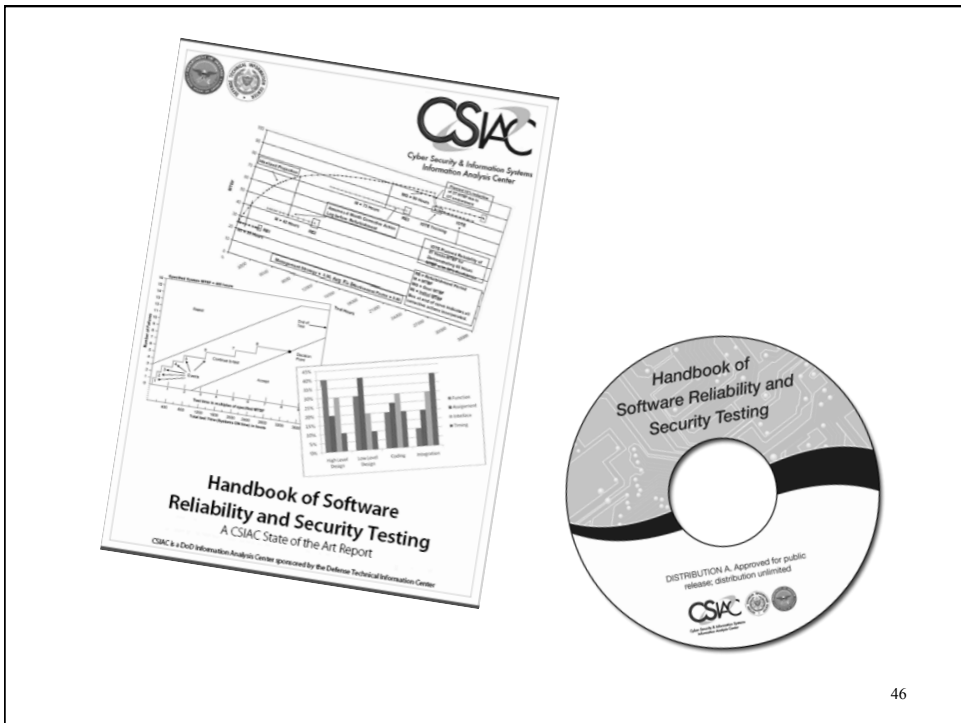
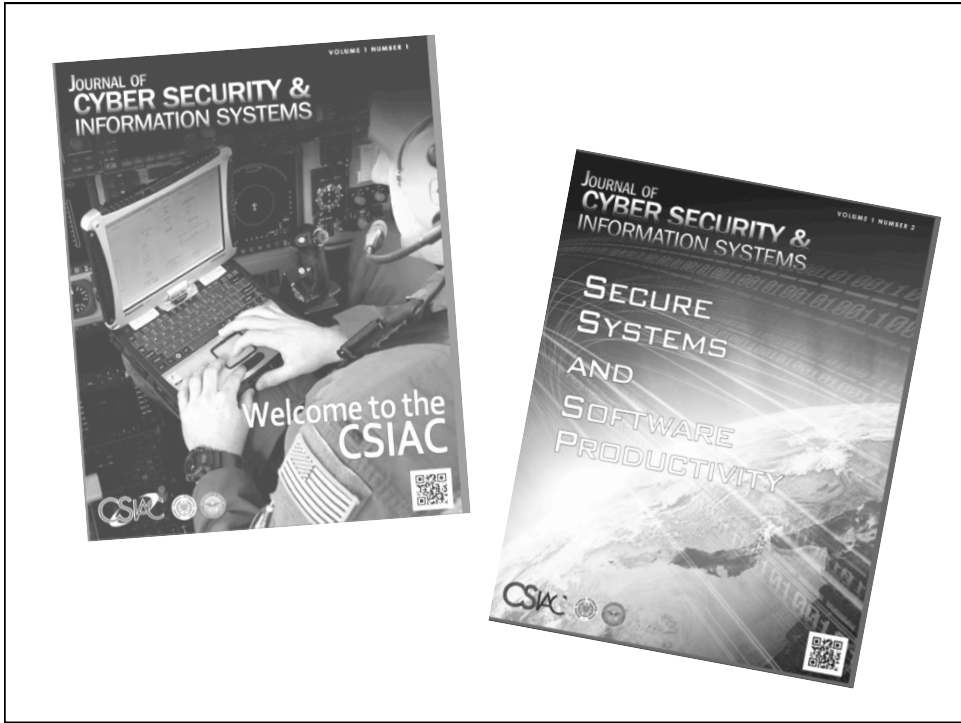
The McColligan suite-like system (TCSA) presenting multiple mobile conditions that would have a 100% hit rate. <http://www.csiaac.gov/CSIAACDirect/News/NewsItem.aspx?NewsID=100>

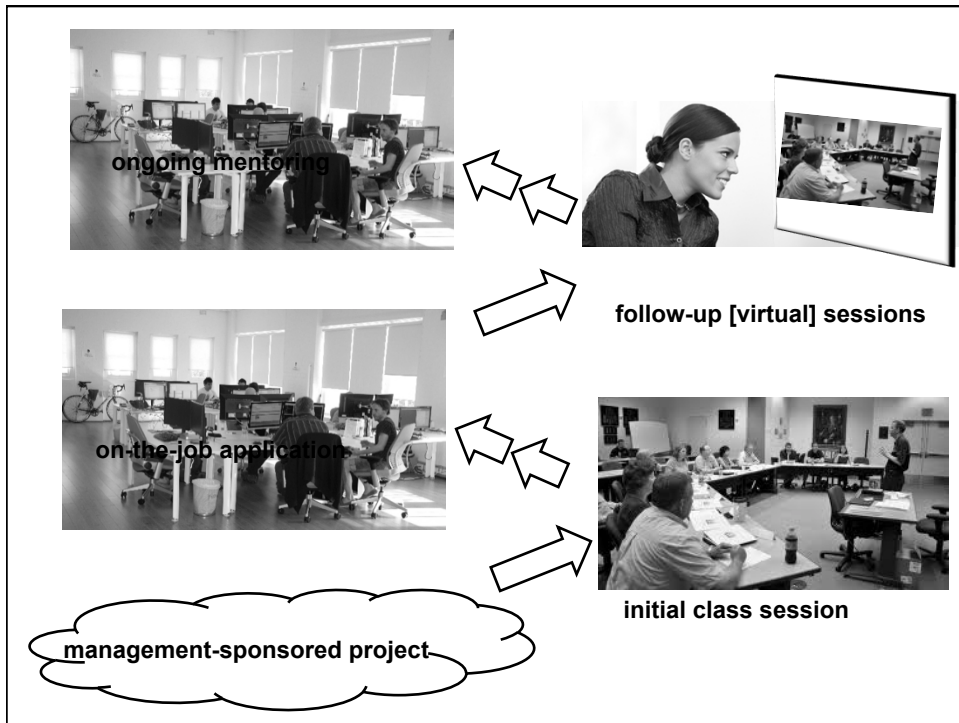
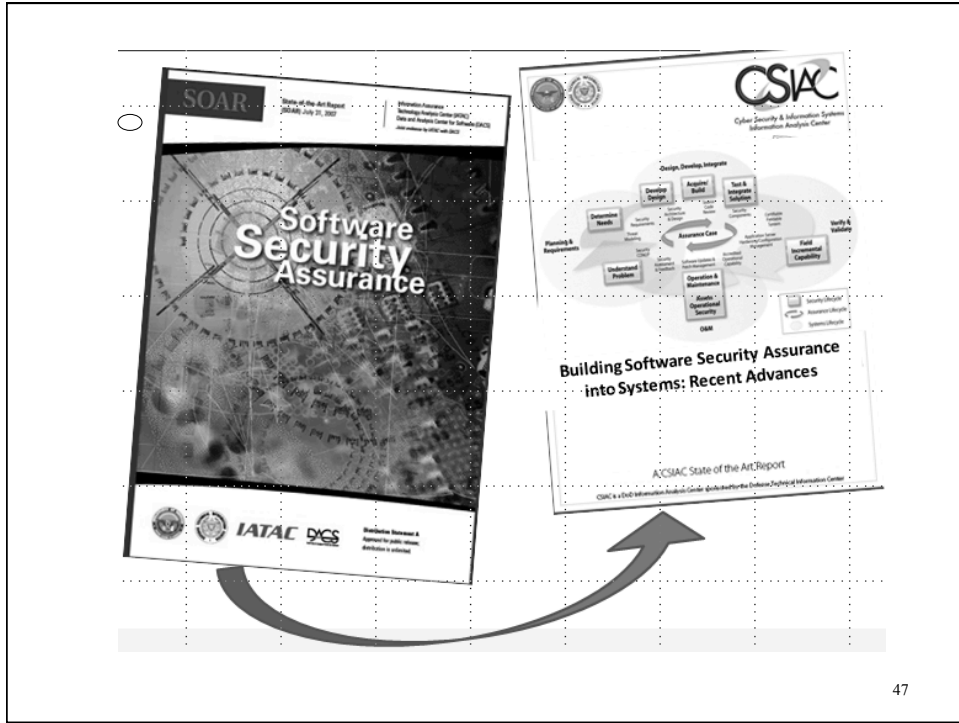
CSIAAC Direct, a real time testing platform, is featured at <http://www.csiaac.gov/CSIAACDirect/News/NewsItem.aspx?NewsID=100>

Other suggested cases (for which we still need published references) included:

- FBI's Federal Systems Division performance on the State Planning System (SPS) Ground Station
- Hudson project on June 28, 1990 a "go live" date of 1990 was announced. Successfully achieved on November 1990
- Software for sea view vehicles using the Ford B804 (Electronic Engine Control)

The Cyber Security and Information Systems Information Analysis Center is a Department of Defense Information Analysis Center sponsored by the Defense Technical Information Center and operated by [www.dtic.mil](http://www.dtic.mil) Solutions.







**Software Quality Engineering  
Tackles Security Issues**

**Taz Daughtrey**

[hdaughtrey@quanterion.com](mailto:hdaughtrey@quanterion.com)

