Integrating Safety into Cybersecurity Test and Evaluation

Michael G. Lilienthal, PhD, CTEP
EWA Government Systems Inc.
Herndon, Virginia

Abstract

Several studies and subject matter experts have concluded that most cyber breaches are caused by human error. Program managers developing new weapon systems find the human error causal factor very seductive. Unfortunately, fixing only human error symptoms can easily become a continuous fight without identifying and mitigating contributory root causes. Safety engineers repeatedly find complex systems almost always fail in complex ways. The safety lifecycle goals dovetail with those of cybersecurity to achieve high levels of functional safety and cybersecurity during conception, design, operation, testing and maintenance of cyber-physical systems. The value that the safety science approach adds to cybersecurity is determining why people behaved in the way they did and what weaknesses in the system allowed the breach (loss/accident) to occur. Cybersecurity testers can benefit from the progress safety science has made in methods of accident investigations and hazard analysis to supplement analysis of emerging systems for cyber vulnerabilities and cyber survivability.

Keywords: cybersecurity, safety science, human error, and hazard analysis

Introduction

Several studies and subject matter experts have concluded that most cyber breaches and incidents are caused by human error (Evans, Maglaras, He, and Janicke (2016), Nobels (2018), and Hughes-Lartey, Li, Botchey, and Qin (2021)). A Government Accountability Office (GAO) report finds cybersecurity vulnerabilities combined with human error facilitate cyberattacks. It also states that according to Kenneth Rapuano, the DoD Principal Cyber Advisor, cybersecurity experts estimate that approximately 90% of cyberattacks could be defeated by implementing basic “cyber hygiene” and sharing best practices to reduce human error (GAO 2020).

Program managers (PMs) developing new weapon systems find human error causal factors very seductive because of low cost workaround remediations. The PM can implement workarounds such as: (1) posting motivational posters and warning signs in the workplace, (2) increasing penalties for violations, slips, and errors, and (3) requiring annual mandatory online training as well as cyber hygiene education. The PM does not have to find additional funds to develop, test, and implement a software/hardware fix. New Department of Defense (DoD) acquisition pathways are geared to field new systems as rapidly as possible. Remedial fixes other than “more training” could delay weapon system deployment. The bias and the “hope” for one or two easily fixed root causes is very attractive. Perrow’s insight that this bias gives the illusion of control over complex systems that we can no longer understand is as true today as it was almost 40 years ago (Perrow, 1984).

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

Gutzwiller, Ferguson-Walter, & Fugate (2019) cyber red team research found biases that will also be present with cybersecurity testers and analysts. Four biases contribute to the focus on human error as the single causal factor:

(1) Anchoring bias – the tendency to rely too heavily (to “anchor”) on one trait or piece of information (usually the first) to make a decision;

(2) Confirmation bias – the tendency to search for, interpret, focus on, and remember information in a way that confirms one’s preconceptions,

(3) Framing Effect bias – the tendency to draw different conclusions from the same information, depending on how that information is presented, and

(4) Hindsight bias – the common cognitive bias to see events, even random ones, as more predictable than they are.

These biases encourage testers and analysts to stop their investigation once they find human error, slips, or violations. They are less likely to consider how the system and the mission environment induce human error, slips, or violations. Unfortunately, fixing only human error symptoms can easily become a continuous fight. The “whack a mole” approach to snuff out human error, slips, and violations will continue without identifying and mitigating contributory root cause(s).

Consider an example where human error was the accident indicator but not the causal factor that needed to be remedied from the past. During World War II B-17 Pilots executed wheels up landings damaging their aircraft (see Figure 1). The apparent causal factor was human error since the pilot lowered the wing flaps rather than the landing gear during the landing sequence. The traditional remedy was applied: more pilot training.

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

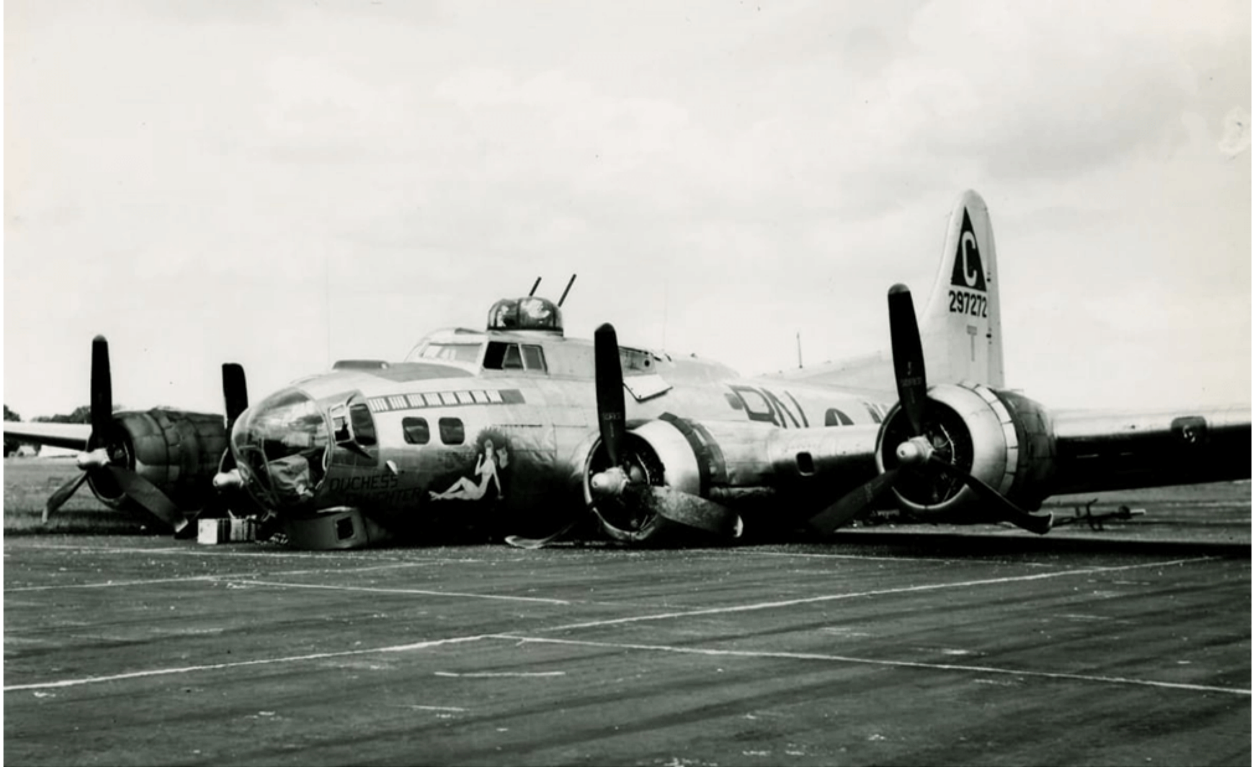


Figure 1: Result of a wheels up landing of a B-17 during World War II operations

However, engineers finally looked beyond that initial bias of human error and discovered the actual cause was design induced human error. The switch lowering the landing gear was located near the switch that controlled the wing flaps. (See Figure 2) During the landing sequence the pilot focuses on the landing approach and easily mistakes the feel of the control switches. The solution was to change the switch shapes so the pilots could easily differentiate the two controls by touch. Accidents dropped to zero overnight.

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

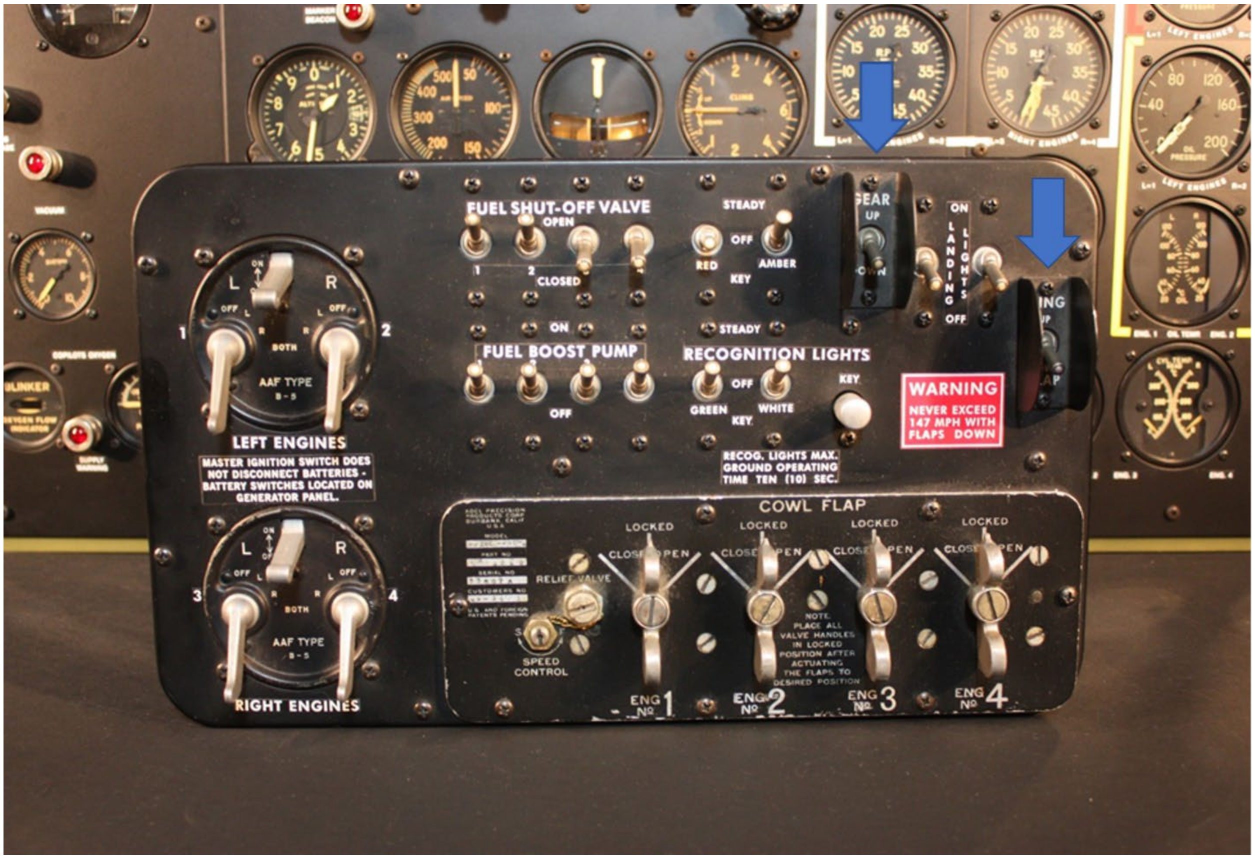

FUEL SHUT-OFF VALVE
OPEN
CLOSED
ON
FUEL BOOST PUMP
OFF
STEADY
RED
AMBER
KEY
RECOGNITION LIGHTS
GREEN
WHITE
GEAR
UP
LANDING LIGHTS
WARNING
NEVER EXCEED 147 MPH WITH FLAPS DOWN
RECOG. LIGHTS MAX. GROUND OPERATING TIME TEN (10) SEC.
LEFT ENGINES
MASTER IGNITION SWITCH DOES NOT DISCONNECT BATTERIES - BATTERY SWITCHES LOCATED ON GENERATOR PANEL.
AAF TYPE
RIGHT ENGINES
COWL FLAP
LOCKED
CLOSE
OPEN
RELIEF VALVE
SPEED CONTROL
NOTE PLACE ALL VALVE HANDLES IN LOCKED POSITION AFTER ACTUATING THE FLAPS TO DESIRED POSITION
ENG No 1
ENG No 2
ENG No 3
ENG No 4

Figure 2: B-17 cockpit control switches for Landing Gear and Wing Flaps (note the arrows point to the identical switches for the landing gear (top row)and the wing flaps (second row) (https://medium.com/swlh/the-flying-fortress-fatal-flaw-694523359eb)

Seven decades later, design solutions to fix "operator error" still must be relearned. In August 2015 the National Highway Traffic Safety Administration (NHTSA) investigated the 2014-15 Grand Cherokee; and expanded the investigation in February 2016 to include 2012- 2014 Dodge Charger & 300 w/3.6L engine after receiving complaints of unattended vehicle rollaway with the engine still on. Auto manufacturers considered it was just human error not putting the shift into park as the causal factor. In May 2016, NHTSA had letters sent to vehicle owners with an Electronic Shifter Quick Reference Information card warning of the hazard and safety precautions for the drivers to take. Drivers were instructed to: "ALWAYS DO A VISUAL CHECK that your vehicle is in "PARK" by looking for the "P" in the Electronic Vehicle Information Center (EVIC) or on the shift lever knob. Always fully apply the parking brake before exiting the vehicle." As with the B-17, the simplest solution was driver education.

However, NHTSA did not stop with that simplest solution. In June 2016, the NHTSA issued #16V-240, Safety Recall #S27 to replace four software modules for over 1.1 million vehicles to compensate for the Monostable gear shift poor control design (See Figure 3). The shift looked like a conventional console mechanical gearshift assembly but did not operate intuitively and had unfamiliar movement that did not give drivers tactile or visual feedback like from conventional shifters. The shifter has one neutral position that it snaps back to when the driver releases the shift knob. The manufacturer violated several basic human factors design guidelines (Green, Levison, Paelke, & Serafin, 1995). The operation of the unintuitive gear shift is demonstrated in this hyperlinked

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

video https://www.youtube.com/watch?v=YGc0I89-yd0 . The NHTSA went beyond human error to find the design induced human error after 1 fatality, 68 injuries, and 266 crashes/fires.

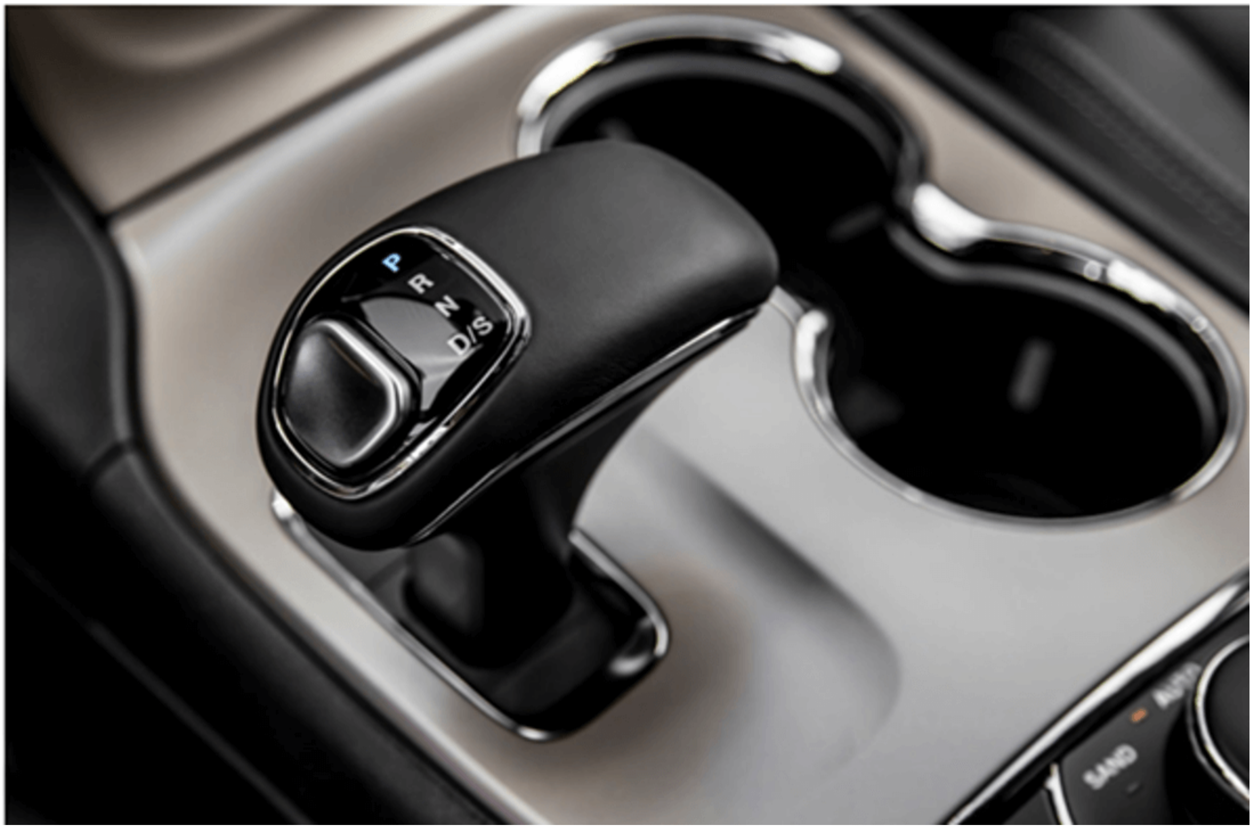


Figure 3: Monostable electronic (shift by wire) gearshift 2014-15 Grand Cherokee; 2012-14 Charger & 300 w/3.6L engine

The two examples above went beyond finding human errors to uncover the design induced errors through the methods safety engineers use in accident investigations. These safety methods can be applied to cybersecurity testing to complement the current cybersecurity methods and tools while also assessing human engineering MIL-STD requirements. Note that MIL-STD-46885A Human Engineering Requirements for Military Systems, Equipment, and Facilities calls for failure and human error analysis – "Human errors in critical tasks shall be analyzed to determine the reason for their occurrence."… "The contractor shall identify those design characteristics or procedures which may contribute substantially to human error and shall propose corrective action" (Paragraph 5.3)). Cyber breaches can be viewed like an unsafe event or hazard. A cyber event (e.g., accident) can be defined as an undesired or unplanned event (e.g., cyber breach) that results in a mission failure, loss of equipment, loss of human life, human injury, or loss of critical data, and information. A cyber hazard can be defined as a system state or set of conditions that together with a worst-case set of operational conditions, will lead to a cyber accident (breach). Safety Science theories can approach the same cyber breach (accident) and cyber vulnerability (hazard) from a different perspective adding insight and value to the analysis.

Safety Science, is a discipline that serves as an international medium for research in the science and technology of human and industrial safety. The field of safety science aims to identify potential weaknesses, initiating events, internal hazards, and potentially hazardous system states to prevent an

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

accident from happening. Accident investigations discover the causes, weakness, and states that led up to the accident. Unfortunately, improved system safety is usually written in the blood from accident findings. Similarly, security (including cybersecurity) aims to protect systems from internal and external threats as well as vulnerabilities that compromise the mission, the system, and operational personnel. Safety lifecycle goals dovetail with those of security to achieve high level functional safety and security during conception, design, operation, testing and maintenance of cyber-physical systems (ISA/IEC 61508, 2010, ISA/IEC 61511, 2023). This approach changes the focus from finding who to blame to why the event happened and how to prevent it happening in the future by developing actionable recommendations. The value that the safety science approach adds to cybersecurity is determining 1) why people behaved as they did 2) what weaknesses in the system allowed the breach (loss/accident) to occur, and 3) possible options to avoid recurrences.

Safety scientists consider safety a system emergent property. That is, safety can only be determined in the context of the entire system and its “mission.” The safety of a component in isolation is meaningless without information about the mission context since a component deemed safe in one system or in one environment may not be in another. Security including cybersecurity is also an emergent property. It, like safety, must look beyond the component behavior to the potential interactions as the system executes its mission(s). The system, people, and environment provide the context for the “accident” and the “hazard” whether it is safety or cybersecurity related.

Accident Analysis – Cybersecurity Analysis

Consider an example of the accident analysis approach. Data analysis conducted during an accident investigation does not stop when the apparent root cause is human error because accidents rarely had a single cause. There are multiple contributing factors. The same is true for cybersecurity breaches. Accidents and cyberattacks in themselves are complex processes and usually involve flaws in: (1) Engineered equipment and software, (2) Operator behavior, (3) Management decision making, (4) Safety culture, and (5) Regulatory oversight (Decker, 2019). This is a systems approach that includes all the components, subsystems, and systems that are interrelated within the mission(s) and the environmental context.

One historic example of the system’s approach’s utility for accident analysis is the evolution of the naval aviation accident investigation process. Accident investigators consider both mechanical and human error to recommend actions to reduce aircraft accidents. Multiple programs and safety protocols have reduced the accident rate over time (See Figure 4). However, the human error causal factors (black dots on upper line) did not respond as well as the mechanical root causes (yellow dots in lower line) to the remedies. Automation, additional training, and changes to the Naval Air Training and Operations Procedures Standardization (NATOPS) went only so far to reduce accidents.

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

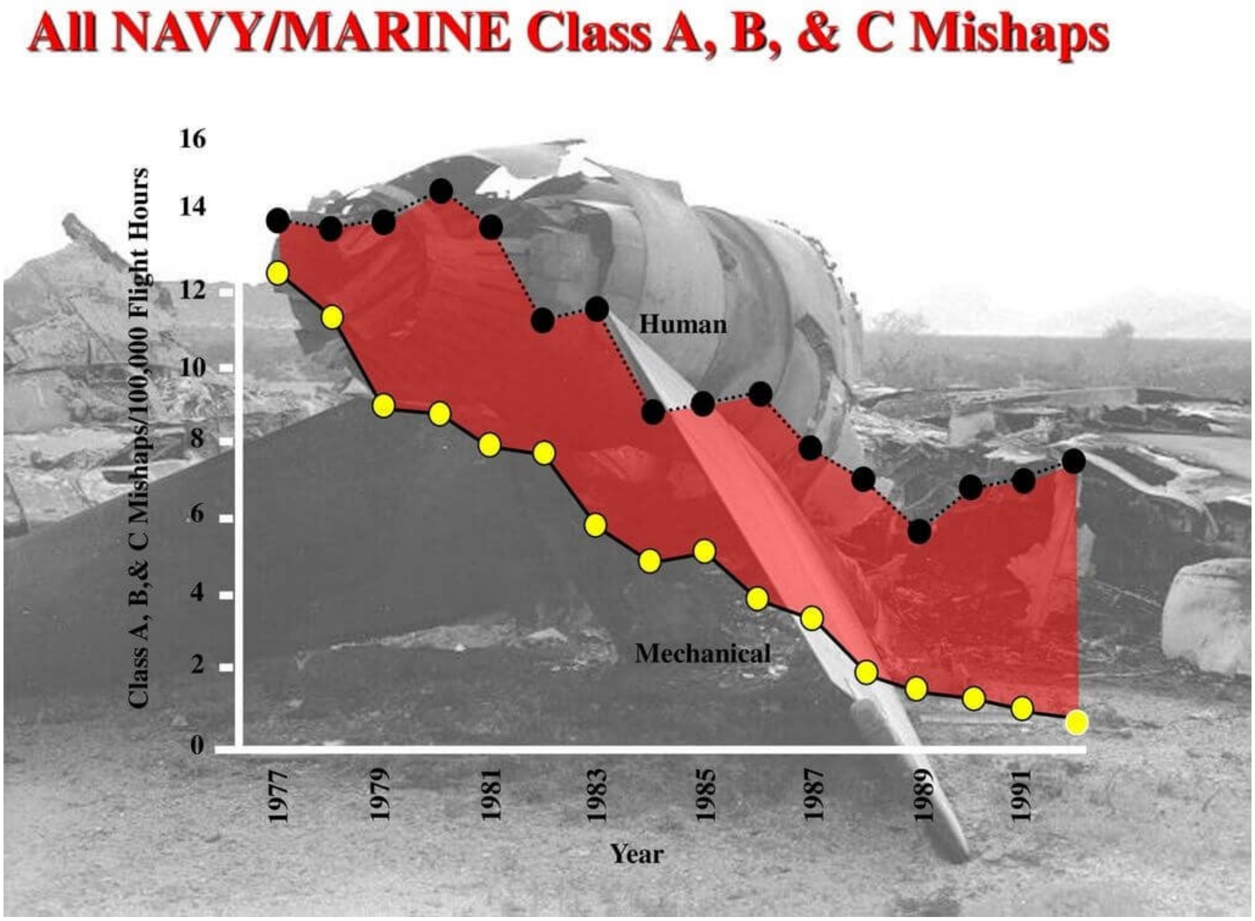


Figure 4: Naval Aviation Mishaps: 1977 to 1992 Class A (fatality or permanent disability), Class B (permanent partial disability or 3 or more personnel are hospitalized) and Class C (nonfatal injury resulting in 1 or more days away from work) (Wiegmann & Shappel, 2017)

Therefore, the Navy Safety Center conducted an in-depth accident analysis. The Center's flight surgeons, and aerospace experimental psychologists leveraged knowledge gained from research (Reason, 1990) into human error to apply a system of systems approach to accident investigation processes. Naval aviation developed the Human Factors Analysis Classification System (HFACS). This approach (Figure 5) examined the unsafe act (that resulted in the accident) and three condition categories that precede (contribute) to that unsafe act, namely: (1) preconditions for the unsafe act, (2) supervisory conditions, and (3) organizational conditions (see Appendix A below for operational descriptions). Systems have complex interactions and interdependencies which we do not understand but which influence both the safety and security of the mission(s). Luckily, developmental, and operational T&E are starting to move from single component and system focused T&E to mission focused T&E. As part of this shift Cybersecurity T&E will have to adopt methods to consider the entire sociotechnical system which includes organizational factors (e.g., operations, command and control, maintenance, training) and supervisory factors (e.g., communications, priorities, mental models, and oversight) just as the Navy has had to include these factors to understand what influences aircraft accidents. This approach is necessary if DoD wants to understand the causal factors that contribute to or reduce mission safety and mission security so it can ensure safe, reliable, (cyber)secure missions.

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

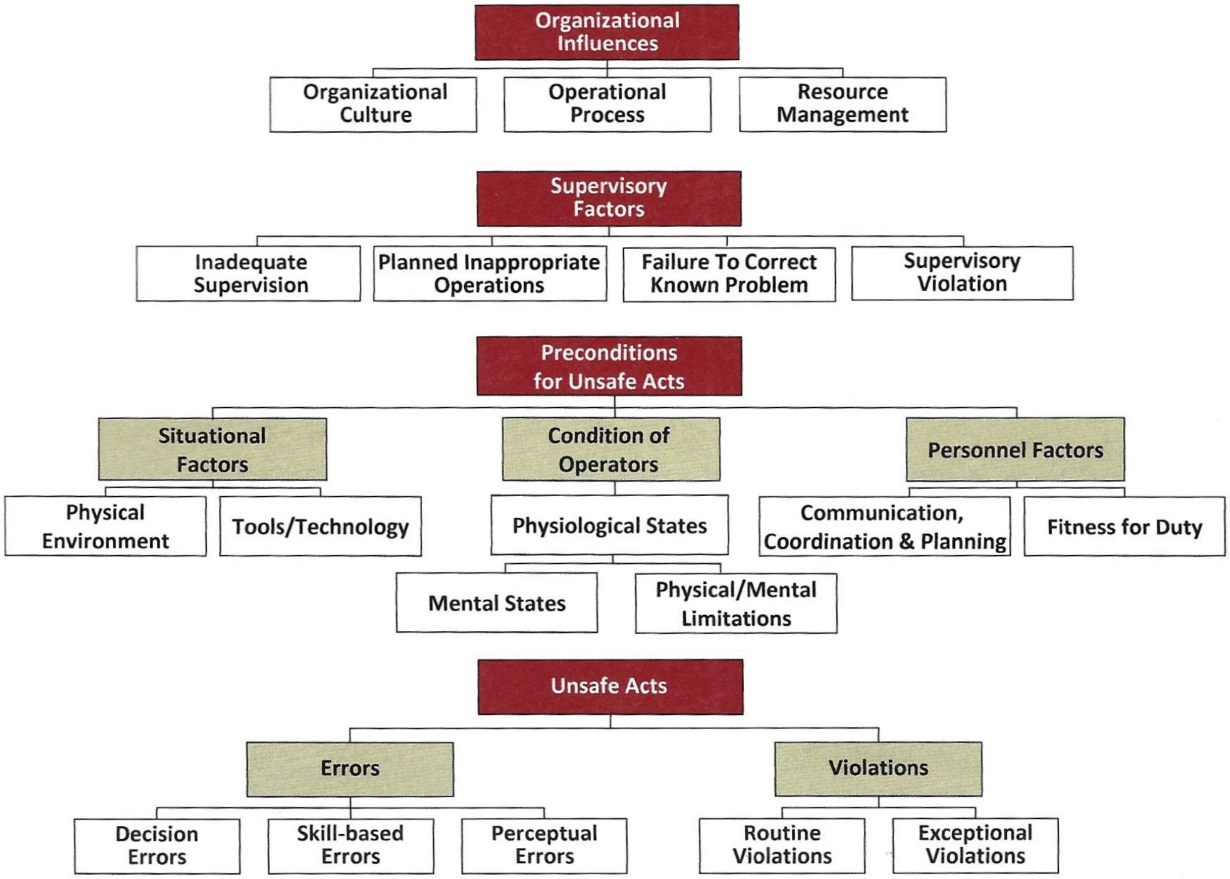


Figure 5: Human Factors Analysis and Classification System (HFACS) (Wiegmann & Shappel, 2017)

The Navy's approach to unsafe acts includes analyzing data on both errors and violations (both consequences of decision making). Errors and violations also occur in cyberspace. Operational testing is good at identifying distinct categories of human error like the three used in HFACS accident investigations, namely: (1) Decision errors, (2) Skill-based errors, and (3) Perceptual errors. These categories were derived from previous human factors research (Reason, 1990). Violations, on the other hand, are not as readily observed as are skill-based and perceptual based errors. Insider violations can be intentional (malicious), unintentional (non-malicious), and intentional (non-malicious). Guo, Yuan & Connelly (2011) provides the following criteria to define nonmalicious security violations, namely: (1) Intentional (not accidental actions), (2) Self-benefiting without malicious intent (no unethical actions such as stealing, e.g., save time), (3) Voluntary rule breaking (violation of policy), and (4) Possibly causing damage or security risk. A lot of emphasis has been placed on malicious and unintentional nonmalicious insider threats but less so on nonmalicious intentional threat behavior. The assessment of how well a system (either human or automated) can detect, prevent, and mitigate nonmalicious insider threats is difficult especially during an operational test event. The test community must differentiate among violation categories (routine, situational, exceptional, and optimizing (see Table 1)) in order to make actionable recommendations. This requires more unobtrusive data collection over a longer period while the system under test is executing its mission(s). That is, the information collection to assess the risk to the mission needs to focus not only on detecting the slips, errors, and violations that lead to a cyber

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

breach but the conditions that precede the actions which include the operating conditions, the time pressures the operators and maintainers are under, reactions to unexpected events and conditions, Information Technology (IT) rules, and the usability of the human-machine interfaces under those conditions as well as organizational, and supervisory factors that are all part of the mission. The unsafe act is meaningful only in the system context within which it occurs which includes the mission, the software, the hardware, the firmware, the environment, the user, the maintainer, and the organization.

CATEGORY	DESCRIPTION	EXAMPLE
Routine violations	Normal and accepted ways of behaving by the peer group and often their supervisors, linked to rules perceived as overly restrictive or outdated, and where monitoring or discipline is lacking	Connect personal electronic equipment that has superior performance or comfort compared to government issue
Situational violations	Situations where the rule does not appear to work or be relevant, winked at by supervision in the name of production	Using military aircraft USB or computer access points to charge smart phone
Exceptional violations	Situations which have never before been encountered previously, where the consequences of the violation may not be thought through	Temporarily remove firewall rulesets while troubleshooting interconnectivity problems in preparation for a Live, Virtual, & Constructive Exercise
Optimizing violations	Solve trade-offs between security or safety and other objectives (e.g., sustained operations) or explore the boundaries of system operation	Execute shortcuts to restore computer functionality aboard ship for the Commanding Officer under short time constraints

Table 1: Taxonomy of violation descriptions (Reason, 2017)

The likelihood of unsafe acts increases when there is a mismatch between security measures and users' goals/tasks. Security is often not seen as an end user task; it is seen as IT's responsibility. Users are very pragmatic. They care more about job performance than IT security. The users' job performance ratings do not usually include how well they conduct IT security measures. For most users the security risk appears too vague, and they do not see how it applies to them. People under time pressure will learn ways to get around poorly designed security policies, interfaces, and slow to respond tech support. They will commit nonmalicious violations (see Table 1) that can open the way for a cyberattack.

Any increases in cyber security by IT administrators to prevent or reduce violations usually decreases the usability of the computer system (Proctor, Schultz & Vu, 2009; Schultz, 2012). How IT Administrators

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

implement their security tools needs to be assessed as part of the testing of the new system. The rules and security tools are part of the overall usability of the system that is being tested. For example, the administrators can set the password length from 0 to 128 characters, the number of password fails before being locked out, the duration of the lockout, audit tools for weak passwords, the complexity of characters required, the number of days before passwords have to be changed, the number of different passwords that have to be used before you can reuse a password and the like, all of which can make computer usage difficult for the user who will pragmatically find work-arounds regardless of security tools to get his primary job done. Usability assessments of the security measures and how operators and maintainers react to them will provide information on the risk and likelihood of system and mission induced user compliance violations. One such assessment approach is described in the next section.

Hazard Analysis

Another tool already in analysts' kits is Hazard Analysis. Hazard Analysis investigates the accident before it occurs. It assumes accidents (and cyber breaches) are more complex processes than just chains of component (humans are a component) failure events. That is, human decisions that can result in an action or inaction that "causes" a mission failure can be analyzed like system safety hazards. This approach places safety hazards into five categories: (1) hardware failures, (2) software inputs (or lack of software input), (3) human error, (4) software-influenced human error, and (5) software defects. Note defects can be activated by user input causing erroneous system behavior, or from inaccurate information displayed to the operator causing an incorrect input response, or due to weak safety/security features that fail to detect incorrect user input. System hazard analysis can be used to identify and categorize initial causes and contributing factors to cyber breaches. Hazards rarely result from one specific cause.

One hazard analysis tool is the Systems-Theoretic Process Analysis (STPA), a hazard analysis technique based on the STAMP (Systems-Theoretic Accident Model and Processes). STAMP is an accident causation model based on systems theory (Leveson, 2011). STPA identifies the unsafe control actions that could create hazardous state(s). It further identifies how each potentially hazardous control action identified could occur within a specific system context.

STPA goes beyond component failures (e.g., human error) examining interdependencies and component interaction—including accidents that occur even though all components behave as expected. STPA takes a systems approach with the understanding that modern systems involve complex interactions among many components (software, hardware, human operators, artificial intelligence systems, environment, management, leadership, and maintenance). The main goal is to understand why failures were not detected and mitigated or what are the human-computer interaction issues, among others, which increase the hazards. It is like Navy aircraft accident investigations that approach the aircrew and maintainer behavior as a product of the environment which leads to a wider analysis of the complex interactions and interdependencies of the environment, the personnel, and the mission. This leads to actionable recommendations to reduce errors and accidents.

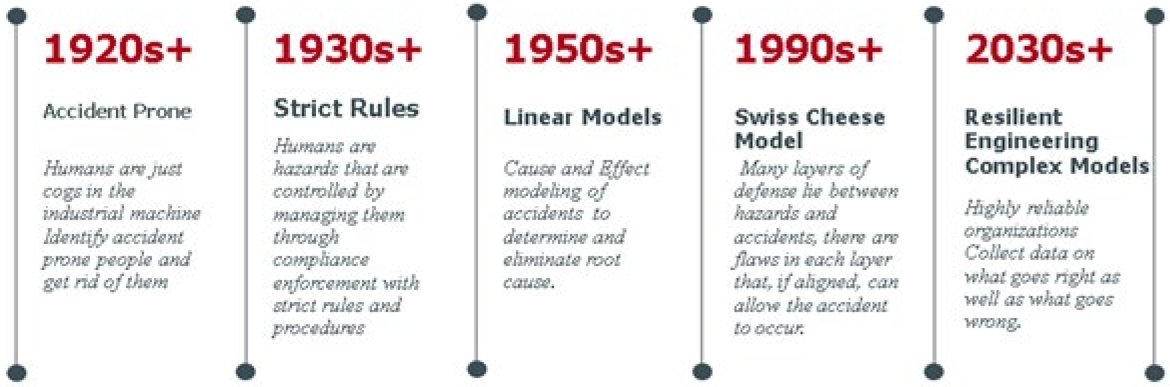
The Evolving Sciences of Systems Safety and Cybersecurity

Safety science draws on engineering, physical sciences, epidemiology, sociology, psychology, and other sciences to develop theories to understand accidents and their root causes. It has evolved over more

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

than a century as the complexity of systems has evolved. Unfortunately that evolution comes mostly as a response to major system failures (e.g., Three Mile Island, Columbia Space Shuttle, and Deepwater Horizon). The science has moved from identifying and removing accident prone people from the workplace, to seeing accidents as having preventable causes through enforcement of compliance with rules and best practices to developing linear models of cause and effect. The science took a systems perspective moving the analytical core from WHO is responsible to WHAT is responsible. It is still a work in progress (Figure 6). Along with all the tools of failure analysis there is the beginning of understanding what is responsible for success (i.e., safe operations). There is a shift from best ways for people to comply to understand people and their variable performance in a security critical operational environment. It is important to understand why systems do NOT fail in the presence of human error and how human factors contribute to facilitating highly reliable (resilient) operations. (Dekker, 2019)



1920s+

Accident Prone

Humans are just cogs in the industrial machine Identify accident prone people and get rid of them

1930s+

Strict Rules

Humans are hazards that are controlled by managing them through compliance enforcement with strict rules and procedures

1950s+

Linear Models

Cause and Effect modeling of accidents to determine and eliminate root cause.

1990s+

Swiss Cheese Model

Many layers of defense lie between hazards and accidents, there are flaws in each layer that, if aligned, can allow the accident to occur.

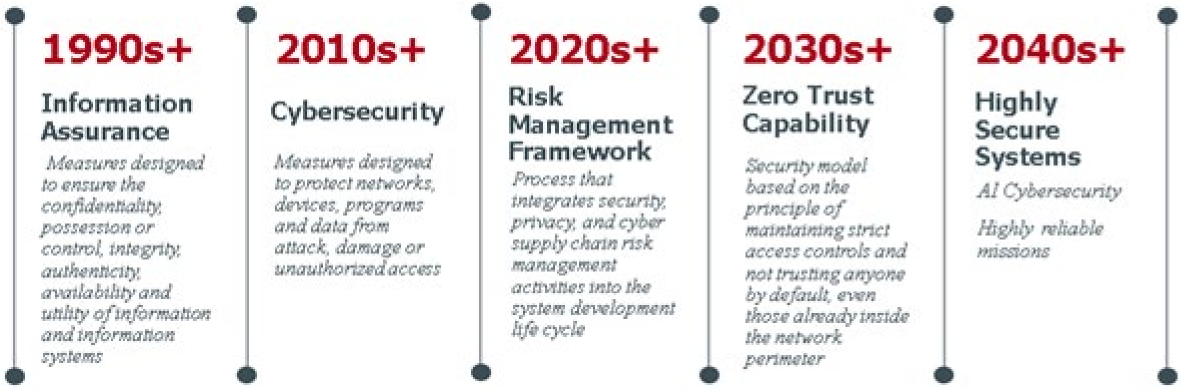
2030s+

Resilient Engineering Complex Models

Highly reliable organizations Collect data on what goes right as well as what goes wrong.

Figure 6: Evolution of Safety Science theories and models

Cybersecurity science, a much younger science, is also a work in progress and is interdisciplinary in nature, studying cybersecurity breaches, vulnerabilities, slips, errors, and violations to develop more secure systems. Linear cause and effect decomposition of systems has been useful for cybersecurity as it has been for accident and hazard analysis. The evolution of cybersecurity guidelines (See Figure 7) has informed and will continue to inform T&E data collection and analysis methodologies.



1990s+

Information Assurance

Measures designed to ensure the confidentiality, possession or control, integrity, authenticity, availability and utility of information and information systems

2010s+

Cybersecurity

Measures designed to protect networks, devices, programs and data from attack, damage or unauthorized access

2020s+

Risk Management Framework

Process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle

2030s+

Zero Trust Capability

Security model based on the principle of maintaining strict access controls and not trusting anyone by default, even those already inside the network perimeter

2040s+

Highly Secure Systems

AI Cybersecurity

Highly reliable missions

Figure 7: Evolution of cybersecurity guidelines

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

Cybersecurity will benefit from studying safety science's current evolutionary pathway that is being forged from the results of the analysis of major accidents. The 2010 Deepwater Horizon accident findings reiterated those from the 2002 Columbia Space Shuttle accident "complex systems almost always fail in complex ways" (Graham, Reilly, Beinecke, Boesch, Garcia, Murray, and Ulmer, 2011). As DoD develops increasingly complex systems, we have reached the limits of modeling and analyzing accidents as a series of linear failures or because of a series of latent and active conditions that are usually only discovered in hindsight. (Perrow, 1984). A single causal factor such as human error is insufficient to inform the design and fielding of more secure missions. Cybersecurity T&E methodology, if it is to evolve to a mission focused approach, will have to include the analysis of individual, organizational, and supervisory issues as safety science continues to do. Cybersecurity science is not there – yet. Hopefully, cybersecurity testers and analysts will:

(1) Observe that multiple and unexpected accidents are the result of complex and tightly coupled systems.
(2) Realize multiple and unexpected cybersecurity breaches are more likely with increasingly complex and tightly coupled systems.
(3) Adapt safety assessment approaches such as the examples briefly discussed here to analyze major cybersecurity breaches.
(4) Deliver actionable recommendations that will inform the design and operation of systems within cyber threat environments that are also evolving in capability and lethality at a rate many times quicker than kinetic threat environments.

Author Biography

Dr. Lilienthal has a PhD in Experimental Psychology from the University of Notre Dame. He is a graduate of the Navy War College Command and Staff College, has a Navy Postgraduate School Certificate in Systems Engineering, is a Certified Professional Ergonomist and an IEEE Certified Biometrics Professional. He is also an ITEA Certified T&E professional. He is a Fellow of the Aerospace Medical Association and the Aerospace Human Factors Association. He retired as a Navy O6 after over 30 years as an Aerospace Experimental Psychologist. He currently supports the OSD Field Office, Test Resource Management Center on matters related to cybersecurity T&E as an EWA GSI Senior Analyst.

Acknowledgements

The opinions and viewpoints expressed in this article are those of the author and do not represent those of the Department of Defense nor the author's company. The author would like to thank Dr. William Moroney, Professor Emeritus, University of Dayton, a fellow Navy CAPT and Aerospace Experimental Psychologist who reviewed drafts of this article and provided valuable critiques and encouragement. The author would also like to thank Pete Christensen, retired Director of the National Cyber Range who reviewed drafts as well and has always been a role model of how to excel while enjoying every moment no matter what the situation.

References

Dekker, S. (2019) Foundations of Safety Science: A Century of Understanding Accidents and Disasters. Routledge.

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

Evans, M., Maglaras, L. A., He, Y., and Janicke, H. (2016) Human behaviour as an aspect of cybersecurity assurance. Security Comm. Networks, 9: 4667– 4679.

Government Accountability Office. (2020). Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene. (GAO Publication No. 20-241). Washington, D.C.: U.S. Government Printing Office

Green, P., Levison, W., Paelke, G., & Serafin, C. (1995). Preliminary human factors design guidelines for driver information systems, pgs 9-11. Washington, DC: Federal Highway Administration (FHWA–RD–94–087). https://deepblue.lib.umich.edu/bitstream/handle/2027.42/1098/88512.0001.001.pdf

Graham, B., Reilly, W. K., Beinecke, F., Boesch, D. F., Garcia, T. D., Murray, C. A. and Ulmer, F. (2011) Deep water: The Gulf oil disaster and the future of offshore drilling. (Report to the President). Washington, D. C.: National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling.

Guo, Ken & Yuan, Yufei & Archer, Norm & Connelly, Catherine. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. J. of Management Information Systems. 28. 203-236.

Gutzwiller, Robert & Ferguson-Walter, Kimberly & Fugate, Sunny. (2019). Are Cyber Attackers Thinking Fast and Slow? Exploratory Analysis Reveals Evidence of Decision-Making Biases in Red Teamers. Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 63. 427-431.

Hughes-Lartey, Kwesi, Meng Li, Francis E. Botchey, and Zhen Qin. "Human factor, a critical weak point in the information security of an organization's Internet of things." Heliyon 7, no. 3 (2021): e06522.

International Society of Automation/International Electrotechnical Commission (ISA/IEC) 61508 (2010) Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems

International Society of Automation/International Electrotechnical Commission (ISA/IEC) 61511 (2023): Functional safety – Safety instrumented systems for the process industry sector

Leveson, N. (2011). Engineering a safer world: Systems thinking applied to safety.

MIT Press Nobles, Calvin. (2018). Botching Human Factors in Cybersecurity in Business Organizations. Holistica. 9. 71-88.
Perrow, Charles. 1984. Normal Accidents: Living with High-Risk Technologies New York: Basic Books.

Proctor, Robert W., E. Eugene Schultz, and Kim-Phuong L. Vu. "Human factors in information security and privacy." Handbook of research on information security and assurance (2009): 402-414.

Reason, J.T. 1990. Human Error. Cambridge: Cambridge University Press.

Reason, James. (2017) A life in Error. 1st Ed. CRC Press https://www.perlego.com/book/1572828/a-life-in-error-from-little-slips-to-big-disasters.pdf

Reeves, A., Delfabbro, P.H., & Calic, D. (2021). Encouraging Employee Engagement with Cybersecurity: How to Tackle Cyber Fatigue. SAGE Open, 11.

Schultz, E.E. (2012). Human factors and information security. In G. Salvendy (Ed.), Handbook of Human Factors and Ergonomics (Vol. 4; pp. 1250–1266). Hoboken, NJ: Wiley.

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

Stanton, B.C., Theofanos, M.F., Prettyman, S.S., & Furman, S.M. (2016). Security Fatigue. IT Professional, 18, 26-32.

Wiegmann, Douglas A., and Scott A. Shappel. A human error approach to aviation accident analysis: The human factors analysis and classification system. Routledge, 2017.

APPENDIX A: HFAC Category Descriptions

Errors

CATEGORY	DESCRIPTION
Decision Errors (DE)	These “thinking” errors represent conscious, goal-intended behavior that proceeds as designed, yet the plan proves inadequate or inappropriate for the situation. These errors typically manifest as poorly executed procedures, improper choices, or simply the misinterpretation and/or misuse of relevant information.
Skill-based Errors (SBE)	Highly practiced behavior that occurs with little or no conscious thought. These “doing” errors frequently appear as breakdown in visual scan patterns, inadvertent activation/deactivation of switches, forgotten intentions, and omitted items in checklists often appear. Even the manner or technique with which one performs a task assessed
Perceptual Errors (PE)	These errors arise when sensory input is degraded as is often the case when flying at night, in poor weather, or in otherwise visually impoverished environments. Faced with acting on imperfect or incomplete information, aircrew run the risk of misjudging distances, altitude, and decent rates, as well as responding incorrectly to a variety of visual/vestibular illusions.

Violation

Routine Violations (RV)	Often referred to as “bending the rules” this type of violation tends to be habitual by nature and is often enabled by a system of supervision and management that tolerates such departures from the rules.
Exceptional Violations (EV)	Isolated departures from authority, neither typical of the individual nor condoned by management.

TABLE A1: HFACS Unsafe Acts

Situational Factors

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

Tools/Technological Environment (TE)	Tools/Technological Environment (TE) This category encompasses a variety of issues including the design of equipment and controls, display/interface characteristics, checklist layouts, task factors and automation
Physical Environment (PhyE)	The category includes both the operational setting (e.g., weather, altitude, terrain) and the ambient environment, such as heat, vibration, lighting, toxins, etc.

Condition of Operator

Adverse Mental States (AMS)	Acute psychological and/or mental conditions that negatively affect performance such as mental fatigue, pernicious attitudes, and misplaced motivation
Adverse Physiological States (APS)	Acute medical and/or physiological conditions that preclude safe operations such as illness, intoxication, and the myriad of pharmacological and medical abnormalities known to affect performance
Physical/Mental Limitations (PML)	Permanent physical/mental disabilities that may adversely impact performance such as poor vision, lack of physical strength, mental aptitude, general knowledge, and a variety of other chronic mental illnesses

Personnel Factors

Communication, Coordination, & Planning (CC)	Includes a variety of communication, coordination, and teamwork issues that impact performance
Fitness for Duty (PR)	Off-duty activities required to perform optimally on the job such as adhering to crew rest requirements, alcohol restrictions, and other off-duty mandates.

Table 2: HFACS: Preconditions for UnSafe Acts

Communication, Coordination, & Inadequate Supervision (IS)	Oversight and management of personnel and resources including training, professional guidance, and operational leadership among other aspects.

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.

Planned Inappropriate Operations (PIO)	Management and assignment of work including aspects of risk management, crew pairing, operational tempo, etc.
Failed to Correct Known Problems (FCP)	Those instances when deficiencies among individuals, equipment, training, or other related safety areas are “known” to the supervisor yet are allowed to continue uncorrected.
Supervisory Violations (SV)	The willful disregard for existing rules, regulations, instructions, or standard operating procedures by management during their duties.

Table 3: HFACS Supervisory Factors

Organizational Climate (OC)	Prevailing atmosphere/vision within the organization including such things as policies, command structure, and culture.
Operational Process (OP)	Formal process by which the vision of an organization is carried out including operations, procedures, and oversight among others.
Resource Management (RM)	This category describes how human, monetary, and equipment resources necessary to carry out the vision are managed.

Table A4: HFACS: Organizational Influences

The ITEA Journal of Test and Evaluation, (ISSN 1054-0929), is published four times each year by the International Test and Evaluation Association, 11350 Random Hills Rd, Suite 800, Fairfax, VA 22030 (www.itea.org)

Copyright 2023, International Test and Evaluation Association, All Rights Reserved. Reproduction in whole or in part is prohibited except by permission of the publisher.