President's Message

Happy 50th Anniversary to the ISSS

by Gary Braman

This year marks the 50th anniversary of the forming of our Society. In 1962, the System Safety Society was organized and chartered in California through the dedicated efforts of Roger Lockwood, C.O. Miller (University of Southern California), and Jerry Lederer (Flight Safety Foundation). These pioneers had a vision of how to use the system safety process to prevent accidents. They met to share their common interests, and it soon became apparent that existing professional organizations and societies did not provide the environment necessary for the long-range objectives envisioned for the system safety concept to flourish. In 1962, the Aerospace System Safety Society was founded.

The Society was founded as a non-profit organization and was chartered in the State of California. The first chapter was formed in Seattle, Washington in 1964 as the Northwest Chapter. In 1967, the name of the Society was shortened from the Aerospace System Safety Society to just the System Safety Society by a ballot vote of all the members. Company memberships (corporate sponsorship) were instituted in 1972 under the guidance of Ed Fosler and, on October 24, 1973, the System Safety Society was incorporated as a non-profit professional organization in the District of Columbia. The initial registered agent was Gordon F. MacDougal, who still serves as the Society's lawyer. Signers of the Society's articles of incorporation were Emerson Harris, E.T. Driver, and C.O. Miller, and the original Board of Directors included E.T. Driver, Donald “Red” Layton, C.O. Miller, Loran W. Sapp and D.A. Smith.

The people whom I just mentioned gave us our start as a professional organization, but many more dedicated professionals were required to sustain and grow the Society. Listed below are just some of these individuals, who have been members of the Society for 25 years (as of December, 2011). The year each person joined the Society is in parentheses:

- Brian Moriarty (1963)
- John Rankin (1963)
- Donald M. Layton (1965)
- Joyce McDevitt (1965)
- Ira Rimson (1966)
- Cliff Ericson (1966)
- Erskine E. Harton, Jr. (1967)
- Waymon Johnston (1970)
- Walter Yeager (1971)
- Ludwig Benner, Jr. (1971)
- Joseph Zboril (1973)
- Ronald Owen (1975)
- Richard Gmyra (1975)
- Ken Morrison (1975)
- Robert Cunitz, Jr. (1975)
- Lawrence Inokuchi (1975)
- Arthur L. Major (1975)
- Richard Weber (1976)
- Saverio DiLauro (1976)
- John C. Frost (1976)
- Naohiro Yuhara (1976)
- Deborah Blakeney (1977)
If you happen to know any of the dedicated system safety professionals mentioned in this article or see them at our Conference in Atlanta this summer, please thank them. And remember that a small group of managers, scientists and engineers dedicated to the science and engineering of system safety started our Society. We would not exist without them.

Thank you for supporting your Society!

See you in Atlanta!

Thank you!

— Gary Braman
Publishing in the 21st Century

by Clif Ericson

Publishing in the 21st century involves considerable competition, which seems to be driving a disturbing trend that affects industry — including the safety arena. A recent news article stated that Chinese scholars are being paid by their government for articles that they have printed in conference proceedings and in journals. All conferences and journals are rated by their "prestige" level, and the scholars receive more money for the higher-rated outlets. This means that paper outlets must strive for higher ratings in order to receive more submittals to their conference or journal. This seems like a "catch-22" situation. Some pragmatic conferences and journals will not receive the technical papers they need because they are not seen as "respectable," since they are more pragmatic than academic in nature. Yet, it is the practical and experiential information that the working-class folks who build large-scale systems desire most.

The first technical paper in this issue, "Practical Software Airworthiness/Safety and Computer Resources Criteria for Airworthiness Qualification of Military Unmanned Aircraft Systems" by Josh McNeil, Dr. Willie Fitzpatrick, Howard Kuettner and Richard Marten, won Best Paper Award at the 2011 International System Safety Conference. Unmanned Aircraft Systems (UASs) require unique criteria for software airworthiness qualification because the pilot-in-command is not aboard the aircraft; instead, he/she is located remotely. Furthermore, circumstances may require autonomous aircraft operation. The Software Engineering Directorate (SED) recognized the need for generic Army UAS software airworthiness/safety and computer resource qualification criteria, tailorable for specific systems, to aid system developers and evaluators in carrying out airworthiness qualification. With this in mind, SED researched existing airworthiness qualification criteria, then modified and supplemented those criteria to establish a set of criteria unique to UAS. The result is a generic set of software airworthiness/safety and computer resource criteria available for use by the UAS development and airworthiness qualification communities. These criteria provide the development community with consistent software airworthiness/safety and computer resource airworthiness qualification requirements, eliminating much previous ambiguity.

The second technical paper in this issue, "Medical Safety: Death by Medicine," by Clifton Ericson, discusses a lack of safety in the medical industry. More people die each year from medical errors than from highway deaths. This trend was recognized in a 2000 study, which generated many recommended safety improvements. Unfortunately, few of these recommendations have been addressed or implemented by the medical industry. The question remains, why does the medical industry not adopt and utilize the system safety process?

In his "System Safety in Healthcare" column, Dev Raheja discusses hazards in patient monitoring alarm systems. As might be expected, patient monitoring and alarm systems are safety-critical devices and, as such, there are many hazards associated with these devices. One of the most insidious hazards is that the alarm systems are often turned down or ignored because of the noise they produce.

In his "Unintended Consequences" column, Terry Hardy discusses a Cessna crash that occurred on
July 10, 2007, while performing an emergency diversion to Orlando Sanford International Airport in Orlando, Florida.

The "Design-Based Safety" column by Dave MacCollum discusses safety in the auto industry, and includes a discussion of behavioral-based safety versus design-based safety.

In his "TBD" column, Charlie Hoes discusses a presentation given to the Virtual Chapter of the ISSS on the topic of safety competency. This is an interesting discussion on qualifications for a safety practitioner and the need to establish competency requirements.

Remember, if you wish to opine, send me an email at journal@system-safety.org.

Until next time,
Clif
Steven Mattern gave a presentation during the March 2012 “Virtual Chapter” meeting on the topic of required competency for system safety professionals. My first reaction was intrigue at the use of the term “competency” rather than “qualifications.” I am not sure what the difference might be, but it “feels” like the first has to do with being able to do the tasks, while the second has more to do with having the correct items on a resume. I think the latter term is probably the correct one, but I will use the first because it sort of made me stop and think a bit.

For the past several years, the answer to the question of the required competency was partially answered by the Board of Certified Safety Professionals’ (BCSP) Certified Safety Professional specialty examination in system safety aspects. However, that certification is no longer offered, so that means of determining whether a person has the requisite minimal competency no longer applies.

That leaves us with a problem. What are the necessary competencies and qualifications, and how do we determine if a person has them? It seems like it matters, and it seems like the International System Safety Society (ISSS) should provide some assistance to those who need to be able to judge the level of competency of a particular individual. It is also important for people in the profession to know what is expected of them to assist in selecting the appropriate training, course work and experience to advance their careers.

Mattern presented two examples of attempts at addressing this issue. One was a detailed circular chart representing NASA’s view of system safety competencies. The chart breaks the competencies into five broad categories, which are further subdivided into specific areas. The categories (in no particular order) are: system safety analytical methods, mathematical skills, system safety in operational management, system safety in acquisition, and system safety rationale. These broad categories are a mixed bag of skills, goals, project phases and desired approaches. However, these give a flavor of the breadth of the field. While interesting, I think the list is too inconsistent and incomplete to be particularly useful. For example, it is not obvious why mathematical skills would be included, but general knowledge about how things work (engineering, physics, chemistry, etc.) is not.

The second set of materials that was presented came from the work of an ISSS “Competency Committee,” composed of five of our knowledgeable elders. They divided the system safety competency pie a little differently, focusing on safety engineering, safety management, education and training, and certification. They also went a step further and developed a philosophical precept indicating four levels of competency in each of these four areas — ranging from “supervised practitioner” to “expert and/or mentor.” The group put all of these criteria into a four-by-four table, creating further specific criteria for each cell in the table. As you can probably guess, this turned into an extensive effort because each block was broken down into subcategories, each of which has its own set of criteria. The group seems to have stalled out at 17 subcategories (many of which have...
their own subcategories), with 203 separate criteria.

A third effort at determining the necessary competencies for the profession was undertaken in developing the BCSP’s examination for the System Safety Aspects Certification. The development of this examination brought together yet another group of “experts” in the field. We worked together as a team to identify not only what we believed to be the desired competencies, but also developed questions to test for these various identified competencies. This resulted in an extensive and detailed description of what we believed to be critical — and testable — at that point in time.

All of these attempts have proven one thing: The field of system safety is broad, complex and requires extensive training and experience in an amazing number of general areas of knowledge. It also requires an in-depth knowledge of details specific to a particular industry, such as aircraft, semi-conductor manufacturing tools, medical devices, trains, etc.
While a solid understanding of physical science, mathematics and the other fields of study are necessary, they certainly aren't sufficient. In addition to the broad educational background so necessary for understanding "how things work," there is also a need for sufficient "hands on" experience to allow the safety professional to visualize the operation of the system in human terms. Normally, the bulk of the system safety effort occurs prior to the creation of any hardware. Therefore, it is important to have a good imagination to be able to visualize what the items will look like, how they will work, and how people will interact with them. Having experience "doing things" goes a long way toward being able to excel at the art of visualizing the system, using incomplete descriptions and drawings.

Assuming all these qualifications are in place, the question turns to the issue of implementing the system safety process (whatever that is). Back in the old days, this meant understanding MIL-STD-882 and implementing the various tasks described therein. Unfortunately, that standard is not at all clear about its intent. It is written in such a way that the reader already has to know the intended process and approach to be able to interpret the intent of the standard. This is not a fatal flaw in the standard — it just means that it can't be used as a tutorial, and that a solid background and understanding of the system safety process is required to use the standard.

This implies that there is something more to the field — something specific about the field of system safety that one must understand in order to be a qualified system safety professional. That brings us to the real meat of the question. What is it that we do that is different from those things done by other members of a project team?

I ran into this question a while back when I went on a tour with an engineering society to a medical device design and manufacturing facility. At the end of the tour, there was a question and answer period, during which I was compelled to ask how big a safety staff the company maintains within its staff of 150-or-so design engineers. The answer surprised me: They have no engineers or other people assigned to safety. Since safety is such an important aspect of medical devices, the answer took me by surprise. None? Really? The presenter went on to explain that all of the company's designers are safety...
conscious and familiar with the standards and regulations, therefore dedicated safety professionals are not necessary.

Is that true? Are we not needed? Do we not bring anything special or important to the team? If we do something special, what is it that makes us special or necessary? Is it our backgrounds, or the position itself? Do we have something special or an unusual skill set to offer? Do we know of a process that is unique and difficult to learn? Or is it just that we are tasked with focusing and paying attention to safety issues, as opposed to other things, such as cost or reliability?

I actually don’t know how to answer these questions. I have learned from experience that there is something about the human mind that seems to make it almost impossible to focus on success and failure at the same time. Maybe that is all we really have to offer. Maybe it is just being a person who can understand how things work, understand how they are used, how they can cause harm, and most important, how to keep our focus on safety rather than all of the other things that others are doing.
In the Spotlight

Won Best Paper Award at 2011 International System Safety Conference

**Practical Software Airworthiness/Safety and Computer Resources Criteria for Airworthiness Qualification of Military Unmanned Aircraft Systems**

by Josh McNeil, BSEE, Redstone Arsenal, Alabama, Willie Fitzpatrick, Ph.D., Redstone Arsenal, Alabama, Howard Kueitner, BA, Huntsville, Alabama & Richard Marten, BSCS, MCS, Huntsville, Alabama

Abstract

Unmanned Aircraft Systems (UASs) require unique criteria for software airworthiness qualification because the pilot-in-command is not aboard the aircraft, but is located remotely. Furthermore, circumstances may require autonomous aircraft operation. The Software Engineering Directorate (SED) recognized the need for generic Army UAS software airworthiness/safety and computer resource qualification criteria, tailorable for specific systems, to aid system developers and evaluators in carrying out airworthiness qualification. With this in mind, SED researched existing airworthiness qualification criteria, then modified and supplemented those criteria to establish a set of criteria unique to UAS. The result is a generic set of software airworthiness/safety and computer resource criteria available for use by the UAS development and airworthiness qualification communities. These criteria now provide the development community with consistent software airworthiness/safety and computer resource airworthiness qualification requirements, eliminating much previous ambiguity.
Practical Software Airworthiness/Safety and Computer Resources Criteria for Airworthiness Qualification of Military Unmanned Aircraft Systems

by Josh McNeil, BSEE, Redstone Arsenal, Alabama, Willie Fitzpatrick, Ph.D., Redstone Arsenal, Alabama, Howard Kuettner, BA, Huntsville, Alabama & Richard Marten, BSCS, MCS, Huntsville, Alabama

Introduction

While supporting the airworthiness qualification activities of the Aviation Engineering Directorate (AED) at Redstone Arsenal, Subject Matter Experts (SMEs) of SED and A-P-T Research, Inc. (APT) have encountered Airworthiness Qualification Plans (AQP)s with varying degrees of technical requirements. We see substantial differences in the content, level of detail and structure in the AQP}s. As a result, the SED and APT recognized the need for standard Army UAS software airworthiness/safety and computer resource qualification criteria, tailorable for specific systems, to aid system developers and evaluators in carrying out UAS airworthiness qualification.

Airworthiness certification criteria for all manned and unmanned, fixed and rotary wing air vehicle systems are detailed in MIL-HDBK-516B [Ref. 1]. These criteria are tailorable and may be applied at any point throughout the life of an air vehicle system when an airworthiness determination is necessary, especially whenever there is a change to the functional or product baseline. The AED SMEs prepare an AQP for each new or updated air vehicle system development, which identifies the requirements and associated substantiation evidence needed to achieve the tailored airworthiness certification criteria for Army air vehicles. In response to this AQP, the air vehicle system developer prepares an Airworthiness Qualification Specification to provide specifics on how the airworthiness certification criteria will be satisfied.

In the past, ambiguity has existed as to the meaning and application of the MIL-HDBK-516B criteria, especially the computer resources and software airworthiness/safety criteria. As written, MIL-HDBK-516B is insufficient as a guide for achieving computer resources and software airworthiness/safety criteria, a situation that is compounded by the recent increase in demand for UASs (Figure 1 and Figure 2). This has resulted in additional and unnecessary efforts on the part of the air vehicle system evaluators and the system developers as they attempt to agree on the airworthiness qualification criteria for computer resources and software airworthiness/safety.

Because MIL-HDBK-516B does not have a definitive set of computer resources and software airworthiness/safety qualification criteria for unmanned aircraft, the AQP}s were inconsistent and typically did not contain the complete list of qualification criteria needed. We decided that a specific set of UAS airworthiness qualification criteria that can be inserted into each AQP for unmanned aircraft systems would aid both the system developer and the airworthiness qualification evaluator. We also concluded that such a set of criteria would provide the development community with consistent software airworthiness/safety and computer resources airworthiness qualification criteria, and eliminate much of the ambiguity which now exists.

During the past several years, the SED provided recommended corrections/updates to AQP}s in the areas of computer resources and software airworthiness/safety. Our attempt to ensure the inclusion of all necessary computer resources and software airworthiness/safety criteria required that we first perform an extensive evaluation of the criteria for each AQP. Secondly, the criteria that traced to a list of computer resources and software airworthiness/safety criteria that we thought appropriate was not always the same for each system. As we provided recommendations for AQP}s, it became obvious to us that an easier and more efficient way to obtain an AQP would be for the SED to
provide the computer resource and software airworthiness/safety criteria to AED before creation of
the AQP. Such a process will eliminate the need for intensive evaluation of the criteria included in the
AQP. We collected information from prior AQP reviews and created a complete set of computer
resources and software airworthiness/safety criteria for unmanned aircraft systems.

Figure 1 — UAS with Remote Terminal [Ref. 2].

Figure 2 — UAS Predator [Ref. 3], Reaper [Ref. 4] and Eagle Eye [Ref. 5].
Practical Software Airworthiness/Safety and Computer Resources Criteria for Airworthiness Qualification of Military Unmanned Aircraft Systems

by Josh McNeil, BSEE, Redstone Arsenal, Alabama, Willie Fitzpatrick, Ph.D., Redstone Arsenal, Alabama, Howard Kuettner, BA, Huntsville, Alabama & Richard Marten, BSCS, MCS, Huntsville, Alabama

Software Safety Considerations: Section 14 of MIL-HDBK-516B provides 15 system safety criteria and three software safety criteria for airworthiness qualification. The current software safety criteria are severely limited in scope and detail, and are definitely not to the level of detail necessary for UAS software qualification. Software qualification for UASs requires an extra level of detail because the pilot-in-command is not located on the aircraft, and command of the aircraft depends on aircraft-control center communications. If communication between the control center and the unmanned aircraft is broken, the aircraft is required to operate autonomously and either be guided to some predetermined location or self-destruct. Based on our software safety experience and because of the unique demands provided by UASs, we have developed a complete set of software safety criteria to be applied to UAS Airworthiness Qualification.

Results: Our research provided a total of 22 additional software safety criteria for UAS airworthiness. The additional requirements include everything from verification of Commercial Off-the-Shelf (COTS) software to software partitioning. Table 1 includes the three original (items 1-3) and the 22 additional software safety criteria. These criteria are to be applied to every Army UAS development and should be included in every AQP.

<table>
<thead>
<tr>
<th>Item</th>
<th>Software Airworthiness/Safety Proposed Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verify that a comprehensive software safety program is integrated into the overall system safety program.</td>
</tr>
<tr>
<td>2</td>
<td>Verify that the software safety program requires appropriate software safety-related analyses to be performed as part of the software development process.</td>
</tr>
<tr>
<td></td>
<td>a. Software safety analyses preparation</td>
</tr>
<tr>
<td></td>
<td>b. Software safety requirements analysis</td>
</tr>
<tr>
<td>3</td>
<td>Verify that the design/modification software is evaluated to ensure that controlled or monitored functions do not initiate hazardous events or mishaps in either the on or off (powered) state.</td>
</tr>
<tr>
<td>4</td>
<td>Verify that COTS and reuse software (which includes application software and operating systems) are developed to the necessary software integrity level.</td>
</tr>
<tr>
<td>5</td>
<td>Verify adequate planning for software safety.</td>
</tr>
<tr>
<td>6</td>
<td>Verify that software safety is integrated into system engineering.</td>
</tr>
<tr>
<td>Item</td>
<td>Software Airworthiness/Safety Proposed Criteria</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>7</td>
<td>Verify that software safety is integrated into software development.</td>
</tr>
<tr>
<td>8</td>
<td>Verify that test plans and procedures include testing of software safety functional requirements and design requirements.</td>
</tr>
<tr>
<td>9</td>
<td>Verify that software causes and software controls of system hazards are identified.</td>
</tr>
<tr>
<td>10</td>
<td>Verify that software safety code analysis has been performed.</td>
</tr>
<tr>
<td>11</td>
<td>Verify that software safety test analysis has been performed.</td>
</tr>
<tr>
<td>12</td>
<td>Verify that all software changes have had safety change analyses performed on them.</td>
</tr>
<tr>
<td>13</td>
<td>Verify that appropriate software safety analyses and assessment tasks have been performed.</td>
</tr>
<tr>
<td>14</td>
<td>Verify software elements that perform functions related to system hazards have been identified and handled as safety-related software.</td>
</tr>
<tr>
<td>15</td>
<td>Verify that each safety-related software function is assigned a Software Hazard Criticality Index (SHCI).</td>
</tr>
<tr>
<td>16</td>
<td>Verify the traceability from the hazard analyses and assessments to system- and subsystem-level safety-related requirements and then from system- and subsystem-level safety requirements to safety-related software and interface requirements.</td>
</tr>
<tr>
<td>17</td>
<td>Verify that the processing of safety-related requirements is separated from the processing of non-safety-related requirements so that safety-related processing will not be corrupted by other processing, i.e., partitioning.</td>
</tr>
<tr>
<td></td>
<td><strong>Software Quality</strong></td>
</tr>
<tr>
<td>18</td>
<td>Verify that software safety planning includes adequate formal qualification testing and that the planned testing is accomplished.</td>
</tr>
<tr>
<td>19</td>
<td>Verify that software safety planning includes adequate requirements-based software structural coverage analysis and that the planned analysis is accomplished.</td>
</tr>
<tr>
<td>20</td>
<td>Verify that software safety planning includes adequate failure modes and effects testing and hazard testing, and that the planned testing is accomplished.</td>
</tr>
<tr>
<td>21</td>
<td>Verify that software safety planning includes adequate safety-related software testing, and that the planned testing is accomplished.</td>
</tr>
<tr>
<td>22</td>
<td>Verify that software safety planning includes adequate nominal and functional requirements-based software testing, and that the planned testing is accomplished.</td>
</tr>
<tr>
<td>23</td>
<td>Verify that software safety planning includes adequate robustness testing, and that the planned testing is accomplished.</td>
</tr>
<tr>
<td>24</td>
<td>Verify that software safety planning includes adequate systems integration laboratory testing of the safety-related software, and that the planned testing is accomplished.</td>
</tr>
<tr>
<td>25</td>
<td>Verify that software safety planning includes adequate aircraft system ground testing of safety-related software, and that the planned testing is accomplished.</td>
</tr>
</tbody>
</table>
Practical Software Airworthiness/Safety and Computer Resources Criteria for Airworthiness Qualification of Military Unmanned Aircraft Systems

by Josh McNeil, BSEE, Redstone Arsenal, Alabama, Willie Fitzpatrick, Ph.D., Redstone Arsenal, Alabama, Howard Kuettner, BA, Huntsville, Alabama & Richard Marten, BSCS, MCS, Huntsville, Alabama

Computer Resources

Considerations: The DO-178B guidelines shall be applied to UAV software. For UAS software, the DO-178B guidelines shall be applied to all UAS software that replaces functionality typically performed by a pilot of manned aircraft. In addition, the DO-178B guidelines shall be applied to safety-of-flight functionality in the Ground Control Station (GCS) and communications subsystems. DO-278 guidelines shall be applied only to software outside the takeoff-to-landing time frame.

These DO-178B and DO-278 guidelines shall be applied to all of the proposed checklist items.

Results: As for Computer Resources, we have provided a total of 65 additional computer resources criteria for UAS Airworthiness. The additional computer resources criteria are grouped into the following categories:

- Air Vehicle Processing Architecture
- Functional Design Integration of Processing Elements
- Electronics
- Architecture Mechanization
- Processing Architecture Verification for Safety of Flight (SOF) Items
- Software Development Planning
- Audits
- Software Requirements
- Software Architecture
- Software Design
- Software Code
- Software Integration
- Software Verification and Test
- Software Configuration Management (SCM)
- Software Quality Assurance (SQA)

Table 2 provides the identification of the 65 additional criteria. These criteria should be applied to every Army UAS development and should be included in every AQP.

<table>
<thead>
<tr>
<th>Item</th>
<th>Computer Resources Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verify that the flight-essential configurations are identified and that proper levels of redundancy (hardware and software) exist at the system level to preclude loss of critical processing capabilities.</td>
</tr>
<tr>
<td>2</td>
<td>Verify that the pilot/operator is notified upon the activation of a flight-essential redundant system to preclude loss of critical processing capabilities.</td>
</tr>
</tbody>
</table>

Table 2 – Computer Resources Criteria for UASs.
<table>
<thead>
<tr>
<th>Item</th>
<th>Computer Resources Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Verify that all processing elements of the architecture that interface (physically and functionally) with SOF functions are designed to meet SOF requirements.</td>
</tr>
<tr>
<td>4</td>
<td>Verify that all hardware and software safety/flight-critical items are identified and that their safety-critical functions are allocated to components within the architecture.</td>
</tr>
<tr>
<td>5</td>
<td>Verify that SOF hardware and software interfaces are clearly defined and documented, and that control flow and information flow are established.</td>
</tr>
<tr>
<td>6</td>
<td>Verify that redundancy (hardware and software) is incorporated to satisfy fault-tolerant SOF requirements, including probability of loss of control (PLOC) and reliability numbers.</td>
</tr>
<tr>
<td>7</td>
<td>Verify that separate and independent power sources are provided for redundant operations.</td>
</tr>
<tr>
<td>8</td>
<td>Verify that single component failure does not impede redundant operations.</td>
</tr>
<tr>
<td>9</td>
<td>Verify that physical and functional separation between safety/flight-critical and mission-critical is accounted for in the computer system architecture.</td>
</tr>
<tr>
<td>10</td>
<td>Verify that no patches (object code changes not resulting from compilation of source code changes) exist for flight-critical software.</td>
</tr>
<tr>
<td></td>
<td><strong>Functional Design Integration of Processing Elements</strong></td>
</tr>
<tr>
<td>11</td>
<td>Verify that all parameters passed among SOF processing elements are defined and that unnecessary coupling is avoided.</td>
</tr>
<tr>
<td>12</td>
<td>Verify that the level of autonomy achieved by the flight-essential elements is sufficient to preclude loss of flight-critical functions due to failure in mission or maintenance-related elements.</td>
</tr>
<tr>
<td>13</td>
<td>Verify that a controlled methodology is established and applied to integrate all safety-critical elements of the processing architecture, including verification coverage.</td>
</tr>
<tr>
<td></td>
<td><strong>Electronics</strong></td>
</tr>
<tr>
<td>14</td>
<td>Verify that all computer resources hardware components are safe, and that SOF elements have redundant buses that are physically separated.</td>
</tr>
<tr>
<td>15</td>
<td>Verify that all safety/flight-critical electronic components are physically and functionally separated from non-safety-critical items. (This includes items such as processors, memory, internal/external buses, input/output (I/O) management, internal/external power supplies, circuit cards, motherboards, etc.) If not separated, verify that non-safety-critical elements are treated as safety-critical items.</td>
</tr>
<tr>
<td></td>
<td><strong>Architecture Mechanization</strong></td>
</tr>
<tr>
<td>16</td>
<td>Verify that the executive/control structure execution rates are sufficient and consistently obtainable for SOF requirements, given the control structure, priority assignments and interrupts.</td>
</tr>
<tr>
<td>17</td>
<td>Verify that the software design, timing, control flow, interrupt structure and data structures meet the required processing capabilities of the SOF subsystem/system real-time architecture.</td>
</tr>
<tr>
<td>18</td>
<td>Verify that all mode inputs, failure detection techniques, failure management, redundancy management, self-checks and interfaces operate safely under all dynamic conditions.</td>
</tr>
<tr>
<td>19</td>
<td>Verify that embedded SOF software provides acceptable performance and safety.</td>
</tr>
<tr>
<td>20</td>
<td>Verify that the SOF software design has the necessary interrupt, re-initialization, resynchronization, re-check, and reconfiguration provisions to re-start or re-set safely and quickly in flight.</td>
</tr>
<tr>
<td>21</td>
<td>Verify that the method of SOF software loading and verification is safe and carefully managed. (This includes the software operational flight program (OFP) loaded on individual black boxes or the air vehicle-loadable OFP.)</td>
</tr>
<tr>
<td>22</td>
<td>Verify that the SOF software design has adequate self-check, failure monitoring, redundancy management, reconfiguration, voting, transient suppression, overflow protection, anti-aliasing, saturation interlock, memory protection and techniques for preventing failure propagation to preclude SOF issues.</td>
</tr>
<tr>
<td>23</td>
<td>Verify that there is sufficient through-put margin for both input/output and processor capabilities (including memory) under worst-case mode performance scenarios for both average and peak worst-case loading conditions.</td>
</tr>
<tr>
<td>24</td>
<td>Verify that a controlled methodology is established and applied to integrate all functional elements of a highly coupled, integrated OFP.</td>
</tr>
<tr>
<td>Item</td>
<td>Computer Resources Criteria</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>25</td>
<td>Verify the operation of BIT and redundancy/failure management algorithms.</td>
</tr>
<tr>
<td>26</td>
<td>Verify that critical hardware/software discrepancies are identified, and corrected or mitigated.</td>
</tr>
<tr>
<td>27</td>
<td>Verify that adequate configuration management controls are in place to ensure proper/functionally compatible software loading for the intended use on the air vehicle.</td>
</tr>
<tr>
<td>28</td>
<td>Verify that all data or communications are secure against unwanted intrusions and that security techniques used are implemented safely.</td>
</tr>
<tr>
<td>29</td>
<td>Verify that the total usable, addressable, physical on-board program instruction memory and data storage memory for each processor is adequate for safety, processing requirements and airworthiness.</td>
</tr>
<tr>
<td>30</td>
<td>Verify that each processor has a reserve vector interrupt capacity that exceeds required vectored interrupts.</td>
</tr>
<tr>
<td>31</td>
<td>Verify that the memory is expandable, usable and addressable to provide for growth over the total main memory for each processor. Techniques used should not degrade the computer system performance of the operational mission and should not require hardware re-design, and the software design should be structured to limit any necessary software changes.</td>
</tr>
<tr>
<td>32</td>
<td>Verify that the software development planning is adequate throughout the system lifecycle, considering system and software safety, magnitude of effort and software complexity.</td>
</tr>
<tr>
<td>33</td>
<td>Verify that there is adherence to the software lifecycle and transition criteria.</td>
</tr>
<tr>
<td>34</td>
<td>Verify that all software requirements and interfaces are identified and defined.</td>
</tr>
<tr>
<td>35</td>
<td>Verify that software requirements and interfaces are accurate, consistent (do not conflict with other software requirements), unambiguous, stated in quantifiable terms with tolerances (when appropriate), are sufficiently detailed and are verifiable.</td>
</tr>
<tr>
<td>36</td>
<td>Verify that the software safety requirements analysis identifies safety-critical requirements and associated criticality or level of rigor rating.</td>
</tr>
<tr>
<td>37</td>
<td>Verify that the software architecture is identified and defined.</td>
</tr>
<tr>
<td>38</td>
<td>Verify that the software architecture does not conflict with the software requirements, especially functions that ensure system integrity, such as partitioning schemes.</td>
</tr>
<tr>
<td>39</td>
<td>Verify that a correct relationship exists between components of the software architecture via data flow and control flow.</td>
</tr>
<tr>
<td>40</td>
<td>Verify that no conflicts exist, especially initialization, asynchronous operation, synchronization and interrupts, between software architecture and hardware/software features of the target computer.</td>
</tr>
<tr>
<td>41</td>
<td>Verify that the software architecture can be verified, such as ensuring that there are no unbounded recursive algorithms.</td>
</tr>
<tr>
<td>42</td>
<td>Verify that the software architecture or partitioning scheme ensures that partitioning breaches are prevented or isolated, and that additional low-level derived requirements are defined as necessary to ensure that partitioning integrity is maintained.</td>
</tr>
<tr>
<td>43</td>
<td>Verify that the software design is identified and defined to adequately fulfill its intended purpose.</td>
</tr>
<tr>
<td>44</td>
<td>Verify that the software design follows defined design standards.</td>
</tr>
<tr>
<td>45</td>
<td>Verify that there is traceability of software design to software requirements.</td>
</tr>
<tr>
<td>46</td>
<td>Verify that there is traceability of safety-critical requirements from hazard analyses to software design.</td>
</tr>
<tr>
<td>47</td>
<td>Verify that the software code is identified and defined to implement the defined design.</td>
</tr>
<tr>
<td>Item</td>
<td>Computer Resources Criteria</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>48</td>
<td>Verify that the code follows defined coding standards.</td>
</tr>
<tr>
<td>49</td>
<td>Verify that source code matches data flow and control flow defined in software architecture.</td>
</tr>
<tr>
<td>50</td>
<td>Verify that source code is accurate and complete with respect to software requirements and that no source code implements an undocumented function.</td>
</tr>
<tr>
<td>51</td>
<td>Verify that source code does not contain statements and structures that cannot be verified and that the code does not have to be altered to test it.</td>
</tr>
<tr>
<td></td>
<td><strong>Software Integration</strong></td>
</tr>
<tr>
<td>52</td>
<td>Verify that requirements-based hardware/software integration testing is performed.</td>
</tr>
<tr>
<td>53</td>
<td>Verify that for each new build, regression testing is performed to verify that subsequent builds do not impact the previously tested functionality.</td>
</tr>
<tr>
<td>54</td>
<td>Verify that regression testing is performed for software modifications or revisions within a build.</td>
</tr>
<tr>
<td>55</td>
<td>Verify that executable object code can be loaded into the target hardware for hardware/software integration.</td>
</tr>
<tr>
<td></td>
<td><strong>Software Verification &amp; Test</strong></td>
</tr>
<tr>
<td>56</td>
<td>Verify that the software development and test environment has been qualified for its intended use.</td>
</tr>
<tr>
<td>57</td>
<td>Verify that the software testing is adequate for the functionality and safety requirements of the software.</td>
</tr>
<tr>
<td>58</td>
<td>Verify that all requirements are verified by performing nominal and functional tests to demonstrate the ability of the software to respond to normal input conditions.</td>
</tr>
<tr>
<td>59</td>
<td>Verify that all requirements’ robustness, off-nominal, and failure condition testing is performed to demonstrate the ability of the software to respond to abnormal inputs and all failure conditions.</td>
</tr>
<tr>
<td>60</td>
<td>Verify that test coverage analysis performed is suitable for the criticality of the software.</td>
</tr>
<tr>
<td></td>
<td><strong>Software Configuration Management (SCM)</strong></td>
</tr>
<tr>
<td>61</td>
<td>Verify that the contractor has identified and defined adequate software configuration management.</td>
</tr>
<tr>
<td>62</td>
<td>Verify configuration management with respect to the identification of baselines, problem reports and change control.</td>
</tr>
<tr>
<td>63</td>
<td>Verify the recording, evaluation, resolution and approval of changes throughout the software lifecycle.</td>
</tr>
<tr>
<td></td>
<td><strong>Software Quality Assurance (SQA)</strong></td>
</tr>
<tr>
<td>64</td>
<td>Verify that the contractor has identified and defined adequate software quality assurance.</td>
</tr>
<tr>
<td>65</td>
<td>Verify that software quality assurance is obtained for the software product submitted as part of the certification application.</td>
</tr>
</tbody>
</table>
Practical Software Airworthiness/Safety and Computer Resources Criteria for Airworthiness Qualification of Military Unmanned Aircraft Systems

by Josh McNeil, BSEE, Redstone Arsenal, Alabama, Willie Fitzpatrick, Ph.D., Redstone Arsenal, Alabama, Howard Kuettner, BA, Huntsville, Alabama & Richard Marten, BSCS, MCS, Huntsville, Alabama

Summary

SED and APT researched existing software airworthiness/safety and computer resources qualification criteria, then modified and supplemented those criteria to establish a set of criteria unique to UAS. The result is a standard set of software airworthiness/safety and computer resource criteria available for use by the UAS development and airworthiness qualification communities. These criteria now provide the development community consistent software airworthiness/safety and computer resource airworthiness qualification requirements, eliminating much previous ambiguity.

Biography

Jonathan McNeil Sr. received his BS in electrical and computer engineering from the University of Alabama in Huntsville. McNeil has worked in the aerospace industry for 20 years as a software safety and system safety engineer. In his current position, he is responsible for performing software safety analyses on various U.S. Army military programs and software airworthiness assessments on various U.S. Army Manned and Unmanned Aviation Systems (UAS). McNeil has given several tutorials on software safety and written numerous papers on software safety. He has also been an active member of the International System Safety Society for more than 17 years, serving as the director of publicity and media (2001-2005); executive chair for the 19th International System Safety Conference (ISSC) (2001); and past president of the Tennessee Valley Chapter (1997).

Willie J. Fitzpatrick, Jr., Ph.D. has more than 35 years of experience in the software/systems engineering area. His experience includes the development and assessment of automatic control systems, systems engineering and software engineering on various aviation and missile systems. He is currently chief of the aviation division in the Software Engineering Directorate (SED) of the U.S. Army Research, Development, and Engineering Command's Aviation and Missile Research Development and Engineering Center (AMRDEC). Dr. Fitzpatrick is responsible for the management of lifecycle software engineering support and airworthiness assessments for several aviation systems, including the Apache, Armed Reconnaissance, Blackhawk, Chinook and Kiowa aircrafts. He is also the directorate's manager for software safety analysis and assessments for aviation and missile systems. He has co-authored several technical reports and publications. Dr. Fitzpatrick is a member of the International System Safety Society and an active Senior Member of the IEEE. He served as chair of the IEEE Huntsville Section during 2007-2008.

Howard D. Kuettner, Jr. holds a bachelor's degree in physics. He has more than 35 years of experience in the software/systems engineering area. His experience includes the development and assessment of automatic control systems, systems engineering and software engineering on various aviation and missile systems. He is currently chief of the aviation division in the Software Engineering Directorate (SED) of the U.S. Army Research, Development, and Engineering Command's Aviation and Missile Research Development and Engineering Center (AMRDEC). Kuettner has been the software safety lead for several major system development programs in DoD and is currently a senior software system safety analyst for airworthiness supporting the Software Engineering Directorate (SED) of the Aviation and Missile Research, Development, and Engineering Center (AMRDEC). Kuettner has been a member of the Tennessee Valley Chapter of the International System Safety Society since 2000, has co-authored papers presented at four International System Safety Conferences (ISSCs), was co-presenter for a software system safety tutorial at ISSC 27, and has co-authored an article published in CrossTalk, The Journal of Defense Software Engineering. He was the SSS TVC Engineer of the Year for 2003.
Richard J. Marten holds a bachelor's degree in computer science from Loyola University of Los Angeles and a master's in systems engineering from the California Institute of Technology. He has more than 35 years of experience in systems and software development, software quality assurance, software configuration management, software test and integration, and acceptance testing. Marten has been the software development lead for several major system development programs in DoD, NASA deep-space probes, and commercial engineering avionics. In addition, Marten has initiated software quality assurance programs for several DoD major firms, including Rockwell's Space Shuttle Operations and several of Raytheon's satellite and defense divisions. Currently, he is a senior software system safety analyst for airworthiness supporting the Software Engineering Directorate (SED) of the Aviation and Missile Research, Development, and Engineering Center (AMRDEC). Marten is a recent member of the International System Safety Society Tennessee Valley Chapter.

References
Most people will readily place their lives in the hands of a doctor or hospital, yet they live with fear and trepidation in regard to commercial airplane flights or driving on major freeways. Based on statistical evidence, it appears that our trust is misplaced. Do you wake up at night in a cold sweat because you are dreaming about dying in a car wreck while on your way to work? Are you afraid to fly to Barbados for a vacation because you fear dying in a catastrophic commercial aircraft crash? Well, fear no more! Research shows that you are more likely to die from a medical error than an automobile accident or a commercial aircraft mishap. Although the problem is well known in the medical industry, it seems little is being done to seriously address and fix the root causes. Perhaps it is time that medicine makes a major paradigm shift, moving from an age-old arts-and-crafts mentality to a more modern engineering mentality and approach to resolve the many complex issues associated with modern medicine. Current statistical data show that more people die each year in the U.S. from medical errors than die in traffic accidents. Studies have been performed on the root causes of this problem, with recommendations as to how to alleviate it. After 10 years, few of the recommendations have actually been implemented. Although sincerely concerned, it appears that the medical industry is not yet prepared to take the necessary steps to resolve its medical error problem. It is disconcerting that the public does not seem aware of the extensiveness of this problem. Some important issues need to be addressed, such as: are doctors part of the problem or the solution? Does the medical industry need to make a major paradigm shift? Most people will readily place their lives in the hands of a doctor or a hospital, yet they live with fear and trepidation in regard to commercial airplane flights or driving on major freeways. Based on statistical evidence, it appears that our trust is misplaced. Even though medicine and the medical industry has been around longer than aircraft and automobiles, the medical industry has not kept pace with the safety record of these other industries. Is it because these industries receive considerable notoriety and government oversight when an airplane crashes, killing 400 people in one incident? When people die individually due to medical errors, however, the notoriety and attention is just not there — apparently because no one is tracking the totals. With less notoriety, there is less oversight and forceful attention or regulation applied to the process. One would expect some undesirable outcomes in high-risk industries, such as medicine, nuclear power, bullet trains, weapon systems, commercial aircraft, etc. But it does not seem reasonable to go into a hospital and have the wrong leg amputated, to die from a chemo overdose or to die from the erroneous application of the wrong drug. A physician's prime directive is "first, do no harm," yet this is not what's happening. Can, and should, the medical industry be forced to maintain safety statistics, with a government mandate to reduce and control these statistics as is done in other high-risk industries?
To err is human, but to allow errors to kill is preventable and unacceptable. In Death by Medicine, author Gary Null concludes that the leading cause of death in the United States is medical errors [Ref. 1]. The yearly death rate even exceeds that of automobile accidents. Medical error is not just a matter of lost wages, lost days of work or lost productivity — it is a matter of life and death. Null cites the following rather startling U.S. medical statistics:

- The number of people with in-hospital adverse reactions to prescribed drugs is approximately 2.2 million per year.
- The number of unnecessary or inappropriate antibiotics prescribed is approximately 45 million per year.
- The number of unnecessary medical and surgical procedures performed each year is approximately 7.5 million.
- The number of people unnecessarily hospitalized each year is 8.9 million.
- The number of deaths caused by medical errors is currently about 800,000 people per year.

In contrast to these stark figures, in 2010 in the United States, 32,788 people died in auto accidents, 652,091 people died from heart disease and 559,312 people died from cancer in 2005. It is, and should be disconcerting that the number of medical error deaths is so much higher than these figures.

In 1986, Alphonse Chapanis, the respected human factors engineer gave a presentation "To Err Is Human, To Forgive, Design" at the 25th annual American Society of Safety Engineers (ASSE) professional development conference and exposition in New Orleans [Ref. 2]. Dr. Chapanis issued a challenge to the engineering community by introducing his concept that the only true human errors are really design errors. He stated that engineers should design products that look into the future and guard against all the types of use and misuse that people might make of them. This concept includes all of the human conditions that can occur when using the product — fatigue, boredom, inattentiveness, misunderstandings and other factors. Equipment, systems and machines have to be made to accommodate how people are, not the other way around. His work dealt with human error in many different industries, including the medical industry.

Error is defined as the failure of a planned action to be completed as intended, or the use of a wrong plan to achieve an aim [Ref. 3]. According to noted expert James Reason [Ref. 4], errors depend upon two kinds of failures: Either the correct action does not proceed as intended (an error of execution) or the original intended action is not correct (an error of planning).

Human error is the incorrect or wrong execution of a required human action; i.e., it is a human failure. Human error and mistakes typically result from the frailties of human nature. Human errors can easily cause hazards and place people, equipment and systems at risk. Human error is an act that through ignorance, deficiency or accident departs from, or fails to achieve, what should be done. Errors can be predictable, or they can be unpredictable and random. Errors can also be categorized as "primary" or "contributory." Primary errors are those committed by personnel immediately and directly involved with an accident. Contributory errors result from actions on the part of personnel whose duties preceded and affected the situation during which the results of the error became apparent.
In order to eliminate or reduce human error, the concept itself must be understood. There are several ways to categorize human error, such as:

- **By fault type**
  - Omission
  - Commission
  - Sequence error
  - Timing error

- **By situation assessment versus response planning**
  - Errors in problem detection
  - Errors in problem diagnosis
  - Errors in action planning and execution (for example: slips or errors of execution versus mistakes or errors of intention)

- **By level of analysis**
  - Perceptual (e.g., optical illusions)
  - Cognitive
  - Communication
  - Organizational

- **By exogenous versus endogenous source (i.e., originating outside versus inside the individual)**
- **By physiology (burn-out, depression, addiction)**

Medical errors committed in hospitals and other types of healthcare settings have been classified into the following categories:

- **Human factors**
  - Fatigue
  - Depression
  - Burn-out
  - Diverse patients
  - Time pressures
  - Variations in training and experience
  - Failure to accept the prevalence of errors

- **Medical complexity**
  - Complicated technologies
  - Powerful new drugs
  - Intensive care
  - Prolonged hospital stays

- **System failures**
  - Poor communication
  - Unclear lines of authority between physicians, nurses and other care providers
  - Complications as patient-to-nurse-staffing ratio increases
  - Disconnected reporting systems within a hospital
  - Fragmented systems in which numerous hand-offs of patients result in lack of coordination and errors
  - Drug names that look alike or sound alike
  - The impression that action is being taken by other groups within the institution
  - Reliance on automated systems to prevent error
  - Inadequate systems for sharing information about errors that hamper analysis of contributory causes and improvement strategies
Cost-cutting measures by hospitals in response to reimbursement cutbacks
- Irrelevant or frequent warnings that interrupt work flow
- Environment and design factors — for example, in emergencies, patient care may be rendered in areas poorly suited for safe application or monitoring
During the past 50 years, various authoritative sources have questioned the safety of healthcare methods and procedures. Perhaps the most stunning revelation occurred in 2000, when the Institute of Medicine published a report that carried this message on its cover: First, Do No Harm: To Err is Human. This report, however, revealed the failure of hospitals to comply with medicine's prime directive ("first, do no harm"). It disclosed that up to 98,000 people each year were dying in hospitals from preventable medical errors. The report called for a 50 percent reduction of errors within five years. This did not happen. Instead, 10 years later, the updated statistical evidence projects that 794,000 patients are dying from foreseeable and avoidable medical mistakes [Ref. 3].

Infrastructure failure is a concern, especially in Third World countries. According to the World Health Organization (WHO), 50 percent of medical equipment in developing countries is only partly usable, due to lack of parts or skilled operators. As a result, diagnostic procedures or treatments cannot be performed, leading to substandard treatment and potential medical errors.

One potential cause of medical errors stems from medical schools. The knowledge, skills and attitudes needed for safe practices are not normally taught in medical school. The methods and processes for system safety need to be taught in medical schools in order to start the paradigm shift in medical thinking.

Technology-induced errors are significant and increasingly more evident in healthcare systems. As a result, a new term has been coined: technologicaliatrogenesis. This term describes a new category of adverse events that are emerging from technological innovations that create disturbances and contribute to medical errors. Healthcare systems are complex and adaptive, meaning there are many networks and connections working simultaneously to produce certain outcomes. When these systems are under the increased stresses caused by the diffusion of new technology, unfamiliar and new errors often result. If not recognized, over time, these new errors can collectively lead to catastrophic system failures. For example, in a survey of more than 500 healthcare facilities, 84 percent of respondents identified automated drug dispensing as a cause of error. Technology may lead to a false sense of security in regard to healthcare safety.

Pay for performance (P4P) is being touted as a possible solution to medical system problems. P4P systems link compensation to measures of work quality or goals. The idea is to connect at least part of an employee's pay to measures of performance. However, current methods of healthcare payment may actually reward less-safe care, since some insurance companies will not pay for new practices to reduce errors, while physicians and hospitals can bill for additional services that are needed when patients are injured by mistakes.

Evidence-based medicine is being suggested as a possible cure for medical errors. Evidence-based medicine is an approach that integrates an individual doctor's exam and diagnostic skills for a specific patient, with the best available evidence from medical research and best practices available. The doctor's expertise includes both diagnostic skills and consideration of an individual patient's rights and preferences in making decisions about his or her care. The clinician uses pertinent clinical
research on the accuracy of diagnostic tests, and the efficacy and safety of therapy, rehabilitation and prevention to develop an individual plan of care.

An advantage of evidence-based medicine is that it may reduce adverse events, especially those involving incorrect diagnosis, outdated or risky tests or procedures, or medication overuse. Errors related to changing shifts or multiple specialists are reduced by a consistent plan of care. As medical advances become available, doctors and nurses can keep up with new tests and treatments as guidelines are improved. There are some negative aspects, however; for example, managed care plans may attempt to limit unnecessary services to cut the costs of health care, despite evidence that guidelines are not designed for general screening, but as decision-making tools for an individual practitioner to use to evaluate a specific patient. Implementing guidelines and educating the entire healthcare team within a facility costs time and resources. Clinicians may resist evidence-based medicine as a threat to traditional relationships between patients, doctors and other health professionals, since any participant can influence decisions.
Safety in healthcare seems to be where the aviation industry was about 40 years ago, when engineers and managers did not question the establishment. Engineers went to reviews — similar to the Mortality and Morbidity boards in hospitals — where active discussions are held, but there is practically no discussion of how to change the system to prevent more accidents. Very few participants challenge each other or hospital superiors to bring out what is best for patient safety.

A number of things can be done to address and correct many of the root causes of the medical-error death problem. For example, the system safety engineering discipline has been successfully applied to industries such as commercial aircraft, nuclear power, high-speed rail and weapon systems. The system safety process has helped to keep accident and mishap rates extremely low in these industries. Special engineering tools are applied, including hazard analysis and fault tree analysis to identify hazards and mitigate their root causes. These processes and tools could easily be applied to medical processes.

Tools from the reliability engineering process could also be applied to the medical industry. For example, Failure Mode and Effects Analysis (FMEA) is just now being introduced to the analysis of medical processes. The FMEA technique identifies potential failure modes in a design or a process, and then evaluates the overall effect of these failure modes should they occur. Once failure modes having high probability of occurrence are identified, they can be mitigated through the application of alternative steps or the application of special safety measures in the process.

Systems engineering and systems engineering tools would also be applicable in establishing and maintaining disciplined medical processes. For example, functional flow diagrams, events sequence diagrams, and configuration control processes would provide many benefits.

Another safety tool that is now beginning to gain ground in the medical industry is the checklist. It seems ludicrous that something as simple as a checklist has not been previously applied in medical procedures. The safety checklist is used in the airline industry to help pilots ensure that all of the necessary and critical steps in a process are performed. Prior to use of the checklist, many pilots were forgetting necessary steps, resulting in aircraft-related mishaps. The checklist became extremely important when pilots were under stress due to some emergency.

Atul Gawande, an associate professor at Harvard Medical School, has written a book titled *The Checklist Manifesto — How*
to Get Things Done Right [Ref. 5]. In this book, Gawande states the need and benefits of using the checklist in the medical industry. In addition, he cites many case studies from his medical work. The medical industry is just recognizing checklists, but the airline industry has been using checklists for how many years now?

The noted management expert W. Edwards Deming taught that improving the process is the only way to improve quality. This philosophy seems to directly apply to the medical industry's problem of unnecessary medical errors. By changing its overall process to one that is well defined, measurable and disciplined — similar to those in engineering and manufacturing — the medical industry may be able to reduce and control its accident rate. It may require a major shift in thinking for the medical industry to change its practices. Perhaps the time of the individual doctor reigning free and uncontrolled is over. Perhaps, too, some major changes are also needed in the medical insurance industry, which forces many medical decisions that may not be appropriate. Death by medicine is an unfortunate and unacceptable problem that can only be solved through major paradigm shifts and the commitment of the entire medical profession and industry.

About the Author

Clifton A. Ericson II has 45 years of experience in the field of system safety, software safety, hazard analysis and fault tree analysis. He worked for the Boeing Company for 35 years and is currently a system safety consultant performing system safety analysis and training. Ericson was president of the International System Safety Society in 2001-2003 and won the Society's President's Achievement Award in 1998, 1999 and 2004 for outstanding work in the field of system safety. He has many published technical papers, he is presently editor of Journal of System Safety and he is author of the following books:

- Hazard Analysis Techniques for System Safety, Wiley, 2005
- System Safety Primer, printed by CreateSpace, 2011.
- Fault Tree Analysis Primer, printed by CreateSpace, 2011.

References

Different strategies have been used to provide constant monitoring to sick patients in hospitals. Equipment and system designs have often incorporated the use of alarm systems, which alert the clinician when a certain value is outside its target range. For example, a heart rate monitor can be set up to send an alarm signal when the patient’s heart rate is above 100 or below 60. Alarm systems, in general, were designed to signal the presence of a potential hazard requiring urgent attention and to summon the assistance of medical personnel.

In the critical care setting, numerous monitoring systems are in place to manage each patient’s complex — and often changing — hemodynamics and physiology. These include alarms from ventilators, cardiac monitors, intravenous pumps, dialysis machines, compression devices and hospital beds, to name a few. One of the major hazards in monitoring the condition of critically ill patients is called alarm fatigue. It is a clinical scenario that may occur when an alarm sounds so often that the responders become desensitized to it and may not respond quickly enough — or at all.

Failure of alarm discriminability, the clinician’s ability to distinguish one medical device alarm from another to respond correctly to the actual alarm, is another major hazard. Problems with alarm volume may occur when the alarm sound is not loud enough, can’t be adjusted to be loud enough for the responder to hear, or when settings have been changed and not reassessed frequently enough. Issues with alarm activation thresholds also occur when the sensitivity levels for a given medical device alarm are adjusted based on a clinical situation or environment and are left at that setting and not readjusted for a new patient or new clinical situation [Ref. 1].

There are numerous alarm-related hazards within medical devices used by patients, as well. Such devices include medication-dispensing systems, cell phones, pagers and telephones alarm systems. A *Boston Globe* investigation identified at least 216 deaths nationwide between January 2005 and June 2010 that were linked to alarms on patient monitors that track heart function, breathing and other vital signs. In many cases, medical personnel did not react with urgency or did not notice the alarm, a type of desensitization that occurs from hearing alarms, including many that are false [Ref. 2]. The investigation revealed that some of the problems were related to incidents involving warning alarms on ventilators, where the caregivers failed to respond to warning beeps because the alarms were set improperly, volume settings were too low or because they were not calibrated correctly.

### Reducing Alarm Fatigue

MedSun, a medical product safety network, reports adverse medical events on the FDA Website, and has posted a summary of surveys [Ref. 1].

Alarm fatigue is so common that it makes the ability to distinguish one alarm from another more challenging. When a hospital staff member hears a single alarm, or multiple device alarms, he or she can differentiate one from the other using several methods. These methods include checking central monitors in the nursing station, searching from room to room, using split screens in patient rooms,
and recognizing sound variety. The majority of respondents report that their device alarms are loud enough to be heard from the central location on the unit. However, they report that there are several factors that may make it more difficult to differentiate these alarms, depending on the size and configuration of units and the noise level in the unit itself.

Nearly all say that they can distinguish an urgent or critical alarm from the others most of the time because of a distinct difference in tone, sound or rhythm. Many memorize the sounds to know the differences and say that over time, staff members can learn the different tones. However, some respondents say that after a prolonged period of time, the tones can begin to blend together. In addition, one respondent reports that some device alarms sound identical, for example, patient beds and infusion pumps, making it even more difficult to distinguish which device is alarming.

In addition to auditory alarms, all respondents report that most of their devices have visual alarms. Visual alarms include blinking and/or colored lights, and monitors with pictures or text. Nearly all respondents find visual alarms helpful. Some respondents describe a visual “red” (critical) alarm that flashes along with the room call light at the central monitor, which helps to quickly locate the alarm and the patient room. However, no one thought that voice alarms on devices would be helpful. Respondents believed that voice alarms would add to the noise and confusion on the nursing unit and thought it would be even easier to tune out voice alarms than standard alarms. Also, they believed voice alarms may upset patients and their families.

Alarm activation thresholds are another critical concern involving medical device alarms. Half of the respondents say volume and parameter threshold settings are adjusted based on a patient’s clinical status and clinical judgment. Others say that default parameter settings are adjusted depending on the type of nursing unit, such as the cardiac intensive care unit. Six of nine respondents say parameters are adjusted by unit nurses or other clinical staff. The remaining respondents have their biomedical engineering department make the parameter adjustments. When discussing silencing these alarms, seven respondents say they are able to temporarily silence alarms for purposes of troubleshooting for a period of 30 seconds to three minutes. After this time frame, the alarm usually resets and turns back on. The majority of respondents say that serious alarms, such as those for lethal heart rhythms, cannot be permanently disabled. And, according to nearly all respondents, once a patient is discharged from the device, the alarm settings revert back to their default settings.
Reducing alarm-related mishaps requires the utilization of risk management methods by hospitals, as well as by manufacturers. An ideal situation would be one in which hospitals and manufacturers would develop solutions together. The FDA is taking the first step by intensifying its pre-market review of medical devices.

Respondents have several ideas about alarm modifications that may improve the safety and effectiveness of medical device alarms. One suggestion is increasing the use of "smart alarms." An example of this is an IV pump occlusion alarm that self-corrects when the occlusion is the result of a patient who temporarily bends an arm with the IV or rolls on the tubing. Another suggestion is linking the apnea and oxygen saturation monitor alarms because apnea monitors are very sensitive and alarm even when oxygen saturations values are within set parameters. Also, many oxygen saturation alarms do not distinguish between values that are high or low. For example, the alarms for values of 89 percent and 30 percent are the same sound, so different sounds would be more helpful.

Another suggestion is providing an escalating alarm or two different tones on cardiac monitors specifically for detecting bradycardia (slow heart rate) in infants. Having two distinct tones for bradycardia and tachycardia (rapid heart rate), particularly for infants in neonatal intensive care units, would help clinicians identify problems faster.

Several respondents say that when multiple alarms are sounding at once, it would be beneficial if the device could indicate the nature of the problem so the clinician could determine the type of response required. Examples of this include having different tones for a "leads-off patient" alarm versus an alarm for a critical patient issue, or an alarm that specifically indicates a high heart rate versus a low heart rate for an individual patient.

Respondents' suggestions also included designing better technology to improve the safety and effectiveness of device alarms. These include providing clinicians with the ability to receive a text message about a device that is alarming on a smart phone, designing noise-canceling technology for unit hallways, providing portable monitoring through use of a pad or tablet, and improving algorithms in individual-patient monitor software that are more accurate and can help eliminate false alarms. In the event that an alarm is disabled, some suggest having a question appear on a monitor screen asking, "Do you want this alarm to remain off?"

Reducing Alarm-related Hazards in Patient Devices

"Fresh from surgery, the patient was wheeled into the intensive care unit and immediately hooked up to a cardiac monitor that would alert nurses to a crisis. Sometime during the following days, though, the cables running from her chest to the machine slipped loose. The monitor repeatedly sounded an alarm — a low-pitched beep. But on that January night two years ago, the nurses at St. Elizabeth’s Medical Center in Brighton didn’t hear the alarm, they later said. They didn’t discover the patient had stopped breathing until it was too late [Ref. 3]." Such incidents are unfortunate, but preventable. There have been numerous Class I (high risk of harm) recalls related to cables affecting the alarms. A cable, which transmits an alarm from the ventilator to the nurses’ station, was recalled because an electrical shortage unexpectedly shut down the alarm system [Ref. 4]. Among other alarm-related recalls were: ventilators/oxymeters giving false positives/negatives, medical devices disabled by patients and delayed alarm and inherent failures in the alarm software or hardware.
Reducing alarm-related mishaps requires the utilization of risk management methods by hospitals, as well as by manufacturers. An ideal situation would be one in which hospitals and manufacturers would develop solutions together. The FDA is taking the first step by intensifying its pre-market review of medical devices. The Joint Commission, the national organization that accredits hospitals, is planning to survey hospitals and nursing homes and evaluate these devices.

**FDA Preventive Actions**

The following summary illustrates how the FDA plans to mitigate alarm-related hazards [Ref. 2]. It wants to provide additional training on alarm standards and alarm safety to its reviewers, who are responsible for scrutinizing 4,000 applications a year from manufacturers seeking permission to sell their medical devices, including heart and oxygen monitors. Alarms on monitors and medication pumps, ventilators and beds already blare endlessly in hospitals, and one of the FDA's top device officials indicated that he wants to prevent new products that do not serve an important function from needlessly adding to the cacophony.

Dr. William Maisel, deputy director and chief scientist at the Center for Devices and Radiological Health, said, "Reviewers are poring over new applications with increased awareness" about whether alarms provide information that is important to patient care and measure what a company claims they measure. "We certainly recognize our important role in addressing the alarm issue," he said.

Maisel, a cardiologist who previously worked at Beth Israel Deaconess Medical Center in Boston, said that the FDA is particularly focused on "new alarms trying to measure new things," such as alarms that monitor various physiological functions at once.

Manufacturers of these devices claim that considering several parameters together allows them to better predict when a patient is in trouble. Many monitors measure just one function, such as heart rate and rhythm.

The FDA is also considering more comprehensive measures, such as issuing guidance documents that would communicate to the industry a “significant changing expectation” regarding the use of alarms. Maisel said the “FDA could do everything right, but if the health care community is not doing its job, that won’t be enough.” Many of the patient safety lapses with ventilators are “not a malfunction of the alarm, but the use of the alarm.”

Alarm systems are in place to assist health care providers. Numerous design innovations and implementation strategies should be used to improve patient safety, while recognizing the inherent challenges in the care of sick patients, especially in critical care units. Although these devices can be life saving, it is the diligent care of the healthcare professional that provides the best warning, something at which an alarm is often not good enough.

**References:**

As engineers, we need to overcome the faulty mindset that auto safety is all about improving driver behavior. Historically, the auto industry was not the initial leader in promoting seat belts. Early on, the U.S. military and other groups were at the forefront as they provided seat belt installation programs. The adoption of airbags was actively delayed by automakers who made vocal objections to President Richard Nixon. The battle cry was "safety doesn't sell."

It was Dr. William Haddon, an emergency room medical doctor, who brought before Congress the need for safety-glass windshields and for removal of hazardous projecting control knobs located on dashboards. Both broken glass and protruding knobs were unnecessary hazards for car occupants if a collision or sudden braking occurred, throwing occupants into the dashboard. In the early 1980s, electronic technology included closed-circuit television to overcome blind zones, ultra-high-frequency near-object radar detection to reduce collisions and automatic braking systems to prevent skidding. It wasn't until nearly 30 years later that these innovations became standard equipment on the more expensive luxury cars. Compare this to our nation's race to place people on the Moon and ensure their safe return, where the development of new safety technology was a major priority.

Early in the 1950s, when I began my engineering career in design-based safety, I learned that car manufacturers' top management accepted safety features only when these features reduced production costs. They felt the idea of personal injury to
The battle cry was ‘safety doesn’t sell.’

The user was speculative, and provided no basis for an added product cost. Little awareness existed of the fact that by ensuring for safe design, greater profits would ensue. Compare this to building design and engineering professions that required licensed engineers to stamp and sign their work to ensure the work met all standards and was safe. Because of this, their failure rate was phenomenally lower than that of the auto industry. Now, compare the millions of dollars expended for the cost of liability or recall for auto accidents due to unsafe design to that of accidents occurring in the building industry. The difference is glaringly lower.

Let us connect some dots to see why the auto industry is more vulnerable to costly lawsuits and recalls. The answer is almost too obvious! Car manufacturers have long claimed that they are competent to select qualified engineers, which they call the engineer licensing exemption. Is it that they do not want their engineers to have the last legal word in requiring safe design, or is it that licensed engineers may demand more compensation for their professional services? When it came to the earnings of the CEOs of these car manufacturers, it seems as though the sky was the limit. When the company loses money from an incompetent CEO’s choice of unsafe design that produces liability and recalls, these CEOs do not waive their obscene salaries. When canned, they simply float away on their “golden parachutes.” In the corporate boardroom of auto manufacturers, safe design was not a high-priority issue. Corporate legal counsel was always quick to claim that runaway tort liability was the cause of the loss, and that it was working with its lobbyists to enact tort reform.

As long as auto accidents are the fault of drivers’ misbehavior, no one is responsible for ensuring safer design. Change is on the way as driverless cars are arriving. Safe design now overcomes foreseeable driver error. Google is doing tests on self-driving cars. Ford Chairman of the Board Bill Ford is pressing ahead with the design of automated cars to overcome design hazards that cause both accidents and roadway congestion. Volvo has a car that can drive itself in busy traffic. Safety features that provide for the car’s intervention overcome the variables of human driver performance in maintaining safe clearance from other vehicles. Both Michigan and Nevada are allowing the testing of “driver assist” features on public roads. It is said that up to 30 percent of a car’s cost can be attributed to the design safety electronics, and by 2040, that may rise to 40 percent. This dramatic change presents a real need for the skills of system safety engineers in the auto industry.

Finally, behavior-based safety is being replaced by design-based safety that provides for driver-assist and passenger protection features. This change, at last, involves management’s acceptance of design-based safety and provides new opportunities for system safety specialists.
Cessna Crash
by Terry Hardy

On July 10, 2007, a Cessna 310R corporate jet crashed while performing an emergency diversion to Orlando Sanford International Airport in Orlando, Florida. The two pilots onboard the aircraft and three people on the ground were killed in the crash. Four others on the ground sustained serious injuries. The airplane was part of the National Association for Stock Car Auto Racing (NASCAR) corporate fleet. The National Transportation Safety Board (NTSB) determined that the probable causes of the crash were actions and decisions made by NASCAR management to allow the airplane to fly with a known, unsolved discrepancy and the pilots’ decision to fly with that discrepancy.

On the day before the accident, another company pilot had noticed a burning smell in the airplane while in flight. The pilot pulled a circuit breaker to the weather radar system and the burning smell went away. Upon landing, the pilot left the circuit breaker pulled and reported the discrepancy, providing both written and verbal descriptions of the problem to the director of maintenance and a maintenance technician. NASCAR’s aviation director, director of maintenance and chief pilot discussed the report, but did not inspect the airplane, according to the NTSB. The airline transport pilots were informed of the discrepancy and could have stopped the flight, but chose to fly anyway. It is believed that the problem was with the electrical wiring in the weather radar system, and, in flight, the pilots re-set the radar circuit breaker, thus restoring the electrical power to the weather radar system and causing the fire that led to the crash of the airplane. In this case, by pulling the circuit breaker, the symptom, or proximate cause, of the accident was eliminated, but the root cause remained (the electrical wiring problem). The NTSB also faulted the safety management system at NASCAR that would allow an airplane with a known problem to be released for flight.

Lesson Learned: Analyses after accidents often show that clues existed before the mishap occurred. Such clues frequently take the form of anomalies observed during the lifecycle of a project. An anomaly is an apparent problem or failure that occurs during verification or operation, and affects a system, subsystem, process, support equipment or facilities. Anomaly reporting and corrective action, therefore, can play an important role in system safety. However, it is not enough to just report a problem — the issue must be investigated, and actions must be taken to prevent an accident. An effective anomaly report and corrective action process not only allows for the reporting of problems, but also implements a closed-loop process for finding and fixing the root cause.

Readers are encouraged to review the full accident and mishap investigation reports referenced here to understand the often-complex conditions and chain of events that led to each accident discussed. Additional lessons learned are available at www.systemsafetyskeptic.com.

References:
This quarter, we have been working on two important projects. A program plan is under development to document and communicate the Director's mentoring, research and development (M, R&D) program, which includes processes, protocols and requirements to meet the Society's goals, objectives and priorities on system safety related to M, R&D efforts. We received positive feedback from a number of Fellows concerning the draft plan.

As part of our mentoring process, we continually encourage discussion of various R&D topics that are applicable to the system safety discipline. A number of white papers have been posted and published for consideration. The topics range from risk assessment through hazard analysis methods.

A new white paper is under development, discussing the analysis of complex systems of systems and families of systems by applying techniques of interaction, interface and integrated hazard analyses. Interactive, interface and integrated hazard analyses have been defined and applied for many years to evaluate the human, software, firmware, hardware and environmental elements of a complex system (SOS or FOS), with different levels of abstraction. From a system safety perspective, these elements and levels of abstraction may be analyzed with specific safety analytical techniques (which may include software, hardware, human and environmental hazard analyses methods) that are suited for each of the specific elements.

As always, if you would like to participate in one of our projects, give me a call at (571) 232-7960.
Colorado Chapter

The Colorado Chapter held a meeting on March 5, 2012 via teleconferencing using the AT&T Web Meeting Service, an interactive presentation and collaboration tool that combines audio conferencing and data sharing through the Internet. The presentation focused on "System Safety: Promoting a Healthy Skepticism," which reviewed lessons learned from accident reports to illustrate potential failures in the system safety process. The presentation provided insights to help promote a healthy skepticism that can improve system safety efforts.

The guest speaker for the event was Terry Hardy, director of safety and risk management at Great Circle Analytics, who has 25 years of experience in system safety and software assurance. A Colorado Chapter member, he is also a regular contributor to Journal of System Safety on unintended consequences. Hardy is the author of the recent book The System Safety Skeptic: Lessons Learned in Safety Management and Engineering, and has created a Website at www.systemsafetyskeptic.com to provide lessons learned in system safety. Other event topics included recruiting and maintaining membership, promoting the 30th ISSC in Atlanta and encouraging submission of abstracts, the annual call for nominations for awards and opportunities for Chapter input to JSS and submission of papers. Several communications to the Chapter were issued as reminders for the 30th ISSC and awards nominations. The Chapter has also been supporting the ISSS regarding hosting a booth at the American Society of Safety Engineers' Professional Development Conference in June in Denver, Colorado.

Georgia Chapter

The Georgia Chapter has added three new International System Safety Society members during the first quarter of 2012: Terri Hall, Clyde Watson and Coleen Thornton. Georgia Chapter members have been central to the planning for the 30th ISSC in Atlanta August 6-10, 2012. The core planning team from the Georgia Chapter includes President Terry Gooch, Past President Odell Ferrell, Treasurer Colleen Sadeski, 30th ISSC Chair Barry Hendrix, Terri Hall, Coleen Thornton, Steve Lee, Bhavin Patel, Clyde Watson, Tom Lewis, James Harris, Dennis J. Beard and David Alberico. Conference activities have been focused on ensuring that 30th ISSC plans and activities meet high standards per the schedule and are within budget allocations. Registration and technical programs are the priority, but dozens of other priority and essential tasks are being performed, from getting sponsors and exhibitors to mass communications mailings. The most recent accomplishment was a support contract issued to provide transportation to the offsite event to the Georgia Aquarium with Wolfgang Puck dinner on August 8. Additionally, spousal programs transportation has been contracted for Atlanta attractions (with a tour guide) on the morning of August 7, and another one-destination tour will be provided on August 9.

Three of four requests for banquet speakers have been fully arranged. The most recent focus has been on supporting the technical program being spearheaded by Dave West and several others. Abstract and tutorial goals established are being met, thanks to the tireless effort and support of many. The Georgia Chapter is working diligently with the Loews Hotel staff, and all volunteers are proud to support the 30th ISSC to provide the best possible activities and outcome on the 50th anniversary of the ISSS.
New Mexico Chapter

The New Mexico Chapter and the Los Alamos Chapter recently combined into one chapter. We welcome the Los Alamos Chapter members and have included them in our communications and activities.

The Chapter held an interesting meeting on February 12, 2012. We met at the National Museum of Nuclear Science and Technology for a presentation entitled "Colossal Failures in High-Tech Projects" by John H. Stichman, Ph.D., PE. John is a retired executive vice president of Sandia National Laboratories. Sandia Labs is, among other things, the nation’s R&D lab for nuclear weapons safety issues. John is exceptionally well versed in safety engineering and management, especially high-consequence events.

He started his presentation with some philosophy — for good or ill, the (safety) engineer’s results are in plain view and the full impact of a creative enterprise cannot be predicted. The professional approach of the engineer is:

- To serve the public good
- Based on special knowledge
- Of profound potential impact
- Leads to an ethical imperative

Thus, we must take positive steps to avoid avoidable errors. Norm Augustine, former chairman & CEO of Lockheed Martin, said, "Engineers who make bad decisions often don’t realize they are confronting ethical issues."

There are a number of ways for errors to occur:

- Errors of execution
  - Mistakes — Making a bad decision
  - Slips — Doing it wrong
  - Lapses — Forgetting
- “Passive” ignorance
  - Lack of a body of knowledge
- “Active” ignorance
  - Overlooking a body of knowledge

John then discussed several practical maxims of engineering that apply equally to safety engineering and management:

- **Demonstrate utter integrity with respect to the engineered object.** Never hope for a miraculous success. He cited the case of the Swedish warship, Vasa, built 1626-1628. The ship foundered and sank after sailing less than a nautical mile on its maiden voyage on August 10, 1628. Vasa was built top-heavy and had insufficient ballast. The Swedish king, Gustavus Adolphus, was impatient to see it join the Baltic fleet, and the king’s subordinates lacked the political courage to discuss the ship’s structural problems frankly or to have the maiden voyage postponed. Sound familiar? Could we make similar observations about contemporary programs?

- **Communication is essential to good engineering and management.** It is shared interpretation, not just shared information. It is essential in achieving informed consent. An example is the unfortunate accident of the Challenger space shuttle, in which the risks associated with the O-rings were not adequately presented to nor understood by management.

- **Consider the human factor.** We are in an age where, more and more, automation (self-acting systems) conflict with autonomy (self-governance of people). There are several aircraft accidents to demonstrate this principle, (“The concept of pilot as a monitor has been popularized in a joke that states that aircraft will eventually be crewed by a pilot and a dog: The pilot will monitor the automated systems, and the dog will bite the pilot if he or she touches anything.” – “The Tyranny of Automation” by John Sheehan)

- **Plan: It is the essence of engineering.** Done correctly, it assures success, elevates the consciousness of risks, illuminates task dependences and makes effective use of resources. John’s example was the Quebec Bridge that was constructed between 1887 and 1907. Despite 20 years of planning, there was inadequate engineering analysis, among other issues. When the bridge was collapsing, there was no one onsite who, by experience, knowledge or ability, was competent or authorized to make decisions.

- **Obtain thorough, objective, authoritative reviews of work.** It is essential to discover all classes of error. Review early and regularly. Redundancy is not independence. An example is American Airlines Flight 96 on June 12, 1972 — a cargo door blew out and caused the loss of hydraulic controls.
• **Know thy product.** Find ways to gain insights into the product’s characteristics. Insight is gained by examining three levels of characteristics: theoretical, computational and physical.

• **Work with discipline and prudence.** This should be self-explanatory. The rewards for doing otherwise are pervasive and immediate.

### Sierra High Desert Chapter (SHDC)

The Sierra High Desert Chapter provided a presentation with a phone number and invited 11 other chapters to participate in our meeting on February 27 in China Lake, California. Our Chapter invited the Bay Area, Central California, Houston, New Mexico, North Texas, Saguaro, Southern California, Twin Cities, Virtual, Washington DC and Winner's Circle Chapters to call in to our Chapter meeting. We thank our speaker, Eric Hawley of the Naval Ordnance Safety and Security Activity, for his brief on “Providing Ordnance Safety for the Naval Enterprise.” Our February lunch meeting was held at the Pizza Factory in Ridgecrest, California.

![Sierra High Desert Chapter Officers and Salvation Army Envoy from left to right are: Treasurer Ken Chirkis, Envoy Donna Griffin, and Vice President Staci Mathews](image)

In March, the Chapter donated to the Salvation Army Food Basket Program and the Toys for Tots drive through the local Marine Aviation Detachment stationed at Naval Air Warfare Center Weapons Division (NAWCWD).

![Chapter Officers and Toys for Tots Marine Corps First Sergeant, from left to right are: Treasurer Ken Chirkis, First Sergeant Dwight McDuffie and Vice President Staci Mathews](image)

The Chapter announced the start of our second annual scholarship program. This year, we changed the program to a single $500 scholarship, rather than the two co-educational scholarships of $250 each awarded last year.
Virtual Chapter

On the second Monday of every month between September and June of each Society Year, the Virtual Chapter holds a Web-based meeting using WebEx and a toll-free teleconference number. The toll free numbers for this teleconference are provided for a number of countries and we have had participants from Australia, Singapore, China, Canada and the U.S.

Chapter meetings are open to anyone who would like to participate. We take a few minutes at the start of each meeting to cover Chapter business, but always follow this with a technical presentation and discussion. Professional discussions allow for opposing views, and participants develop a stronger understanding from the exploration of these topics. A lot can be learned from the different perspectives brought together by a group of qualified professionals.

Last November, we had an excellent presentation from Steve Mattern on "Level of Rigor and Software Safety." Steve addressed the philosophical precepts behind the level of rigor approach and presented practical examples of where this has been implemented in industry. This was followed in December with a presentation by Bob Schmedake identifying some issues with the level of rigor approach and his concerns that the higher levels of rigor process steps should correlate with the condition that drove the developer to the need for a higher level of rigor; otherwise, a false sense of safety results.

In January, Charlie Hoes presented a thought-provoking presentation on wind turbine safety and the issues present in those systems. Many of us were surprised by data presented that challenged the positive impacts of wind turbines on our environment.

This past February, Terry Hardy presented "A Skeptical Look at Hazard Controls." He cited examples of cases where the hazard control introduced new hazards to the system that were inadequately assessed and resulted in catastrophic mishaps.

Our March meeting featured a presentation by Steve Mattern on "System Safety Competencies" as a means of improving our discipline. In this presentation, Steve discussed the merits of assessing a standard set of skills for system safety professionals. An approach that NASA is exploring was discussed during this topic.

In April, Bob Schmedake presented a review of articles on "Dynamic Fault Tree" concepts. He provided some examples of this technique performed using the RELEX fault tree software.

The Virtual Chapter is an outstanding opportunity for networking and learning from other practitioners of system safety engineering. Meeting attendance is as simple as a log-in and a phone call. No matter where you are, you can attend a Virtual meeting. We will also have members of our chapter at the Atlanta Conference this August, and we invite you to get to know us.

For more information on Virtual Chapter meetings, contact Chapter President Jimmy Turner at ts41930@yahoo.com.
Journal of System Safety, eEdition


Article Submission | Advertising | Subscriptions & Membership | Copyright

Journal of System Safety is published six times a year (four print and two electronic editions) by the System Safety Society for the transmission of technical material and news of topical interest to those associated with the practice of system and product safety. Information, recommendations, statements and opinions expressed herein are those of the individual authors and advertisers, and do not necessarily represent those of the System Safety Society. Certain material is published for the purpose of stimulating independent thought on controversial matters or on problems of vital concern to safety professionals. Although caution is taken to ensure accuracy, the publishers or editors cannot accept responsibility for correctness or accuracy of the information presented.

All articles and papers published in Journal of System Safety remain the property of the original authors, and are protected under U.S. and international law. For copying and republishing permission, please contact the original authors. For more information on copyrights, copying and republishing, please see http://copyright.gov/.

ARTICLE SUBMISSION
Journal of System Safety welcomes article submissions from its readers. Technical manuscripts, "Opinion" and other submissions should be sent to:
Clifton Ericson, JSS Technical Editor
6406 Medallion Drive
Fredericksburg, VA 22407
USA
540-786-3777
Email: journal@system-safety.org

Authors should include the following:
(1) one printed copy of the manuscript, double spaced; (2) electronic file in Microsoft Word, Adobe InDesign or ASCII (plain text) format; (3) a statement of copyright ownership; (4) a short (one paragraph) author profile; (5) the author's name, address, daytime phone and fax number, email address, affiliation and professional status. For more information on submissions, please email journal@system-safety.org.

All submissions are subject to peer review.

If authors wish to have their materials returned, they should send a specific request, along with a self-addressed, stamped envelope.

ADVERTISING POLICY
Journal of System Safety welcomes advertising compatible with the objectives of the System Safety Society, subject to the approval of the Technical Editor. The acceptance of advertising does not imply endorsement by the Society or Journal of System Safety.

Ad prices in the printed JSS are as follows:
Full-page ad — $800
Half-page ad — $400
Quarter-page ad — $225

For electronic ads:
Small ad = 150 x 75 pixels = $20
Medium ad = 150 x 350 pixels = $110
Large ad = 150 x 600 pixels = $210

For information on advertising rates and submission guidelines, please contact:
Clifton Ericson, JSS Technical Editor
6406 Medallion Drive
Fredericksburg, VA 22407
USA.
540-786-3777
Email: journal@system-safety.org

SUBSCRIPTION AND MEMBERSHIP INFORMATION

For information on subscription rates and membership, contact:
System Safety Society
P.O. Box 70
Unionville, VA 22567-0070 USA
Tel: 540-854-8630
Fax: 540-854-4561
Email: systemsafety@system-safety.org
Web: http://www.system-safety.org

Copyright © 2011 by the System Safety Society. All rights reserved. The double-sigma logo is a registered service mark of the System Safety Society. Journal of System Safety and the System Safety Society name are registered service marks of the System Safety Society. Other corporate or trade names may be trademarks or registered trademarks of their respective holders.

(ISSN-0743-8826)
Vol. 48, No. 3 • May-June 2012

Journal of System Safety is produced by:
Panorama Creative Group
1770 N. Audubon Drive
New Albany, IN 47150
USA
Publisher: Dave Davis

Technical Editor:
Clifton Ericson
6406 Medallion Drive
Fredericksburg, VA 22407
540-786-3777
Email: journal@system-safety.org

Technical Advisors:
Russ Mitchell (Burlington, Vermont)
Melissa Emery (Huntsville, Alabama)
Malcolm Jones (Reading, U.K.)
Rani A. Kady (Abu Dhabi, UAE)
William E. McMinn (Damascus, Maryland)
Dev Raheja (Washington DC)

Associate Editor:
Dr. Rod Simmons (Abu Dhabi, UAE)
Copy Editor: Dara Chadwick
QA: Laurene Scalf
Production Editor, eJSS: Norman Bell

System Safety Society Contacts:

OFFICERS:
Gary Braman, ISSS President
Sikorsky Aircraft Corporation
256-327-5356
gbraman@sikorsky.com

Robert Schmedake, ISSS Executive Vice President
Boeing
314-232-0552
robert.a.schmedake@boeing.com

Dr. Rod Simmons, ISSS Treasurer
The Petroleum Institute,
Abu Dhabi, UAE
+971.55.800.6652
rod_simmons@me.com

Jean Sauerman, ISSS Executive Secretary
Raytheon Missle Systems

Chapter News
Mark Your Calendar
About this Journal
Puzzle

President's Message

From the Editor's Desk
TBD

Practical Software
Airworthiness/Safety and Computer
Resources Criteria for Airworthiness Qualification of Military Unmanned Aircraft Systems

Medical Safety: Death by Medicine
System Safety in Healthcare
Hazards in Patient Monitoring Alarm Systems
Design-based Safety
The Great Deception
Unintended Consequences:
Cessna Crash
Technical Fellows' Corner

Technical Editors:

Contact JSS

Always OPEN for business!
Each issue of the eJSS is available at www.system-safety.org/jss/ejss.php

Download printable PDF of this page
Warren Naylor,
Past President
Northrop Grumman Electronic Systems
410-765-6910
warren.naylor@ngc.com

Office Manager: Cathy Carter
systemsafety@system-safety.org
540-854-8630

DIRECTORS:
Chuck Muniak
Education and Professional Development
Syracuse Safety Research
cmuniak@stevens.edu
315-663-7606

Gerry Einarsson
Chapter Services
einargk@rogers.com
613-824-2468

Dave Shampine
Conferences
URS
dave.shampine@urs.com
540-663-9588

Bob Fletcher
International Development
rwfletcher@sympatico.ca
613-837-4129

Clifton A. Ericson
Publicity and Media
EG&G Technical Services
cliftonericson@cs.com
540-663-9591

Saralyn Dwyer
Member Services
APT Research, Inc.
sdwyer@apt-research.com
256-327-3377

Mark Geiger
Govt. and Inter-Society Services
OPNAV Safety Liaison Office
mark.geiger1@navy.mil
703-695-4703

Michael Allocco
Mentoring and R&D
michael.allocco@faa.gov
202-385-4714

CHAPTER POINTS OF CONTACT:
Go to complete listing on the Society web site.
Taking flight

The aviation industry has long embraced the concept of system safety in its operations. This month, we'll take a look at some of the key components affecting aviation safety.

If you need help, highlight one or more words in the list and click on "Find Words." If you click on "Rescramble," a new version of the puzzle will be generated.

Note: Your browser must have Java enabled to view the Word Search Puzzle.