Journal of System Safety
eEdition
A publication of the System Safety Society

Vol. 43, No. 6 • Nov.-Dec. 2007

In the Spotlight

Source-Mechanism-Outcome: A Simple, Yet Effective Hazard Description Model

by Donald Swallow, Madison, Alabama

Pages 1 | 2 | 3

Hazard description models are important because they help system safety practitioners identify hazards and describe them in a way that is readily understood by others, which facilitates identifying effective mitigation measures. Without going into specific examples, hazard models historically have suffered from two shortfalls. First, they can be too complex, either in the way the components of a particular model are described or in the terminology used. Second, they are structured so that they cannot be applied to all classes of hazard. However, there is a model that is not overly complex and is flexible enough to describe most hazards: the source-mechanism-outcome model (S-M-O or SMO).

The first component of the model is simply the "source." A source is an activity, condition or circumstance that has the potential to do harm to an asset. An asset is defined as "something of value that must be protected." Assets include, but are not limited to, personnel, facilities, equipment, operations, data, the public and the environment, as well as the system itself. So when one begins to describe the hazard, one identifies what it is that has the potential to cause harm. Things that cause harm could be electrical power exposure, sharp edges, hydraulic pressure, height above the ground, temperature extremes, fire, radiation, explosives, hazardous material leaks or spills, operator error, fatigue, utility outage, potholes, *ad infinitum*.

The next component of the model is the "mechanism," that process or sequence of events that allows or enables the source to cause the harm. The mechanism might be described in simple terms, or it may require a complex multi-linear diagram to understand it.

Finally, there is the "outcome," that harm which the source brings about through the mechanism to the asset.

In a simple example, one may define a hazard as "being burned." Using the SMO model, heat is the *source*, the *mechanism* is the asset's (a person's) contact with the heat source, and the *outcome* is the burned skin. Bear in mind that in this example, there may be a range of injuries or damages with one outcome. The outcome of a burn could be skin redness and pain, blistering, extensive skin damage or even death. The structure of the model will become clearer as we look at its history and some more detailed examples.

"In a simple example, one may define a hazard as 'being burned.' Using the SMO model, heat is the source, the mechanism is the asset's (a person's) contact with the heat source, and the outcome is the burned skin."

History of the SMO Model

The first mention of the SMO model in the literature of system safety is in a compilation of one-page "tutorials," called the *System Safety Scrapbook*. These were authored by Pat Clemens, a long-time system safety practitioner and a past president of the Board of Certified Safety Professionals, who has developed and implemented many system safety programs in both government contracting and in the private sector. During the 1980s, under Pat's leadership, the safety office of Sverdrup Technology, Inc. produced a series of *System Safety Scrapbook* sheets. These sheets were published on an as-needed basis, and each dealt with a single aspect of system safety practice. Their purpose was to reinforce concepts presented in formal system safety classroom training, to foster improved communication in matters of system safety analysis and to sharpen basic "system savvy" and analytical skills. One of these sheets, number 84-3 (the third sheet issued in 1984), contains the first recorded mention of the SMO model. This sheet pointed out that when listing hazards, we often name a hazard according to the severity component of its risk, and we describe the consequence of the hazard rather than the hazard itself. The SMO model was created to counteract this tendency. The example given in this sheet is the hazard identified as "Fatal Highway Crash." In fact, this "hazard" is the consequence of many real hazards, such as excessive speed, worn tires, etc. To avoid this, the sheet encourages the practitioner to make the description of each hazard tell a story, a "little scenario that addresses the Source, the Mechanism and the Outcome (i.e., Consequences) that characterize the harm that is threatened by the hazard." In the Sheet 84-3 example, the scenario is, "Worn tires leading to blowout at high speed resulting in loss-of-control crash and driver fatality" [Ref. 1].

SMO next appeared in NASA Reference Publication 1358, *System Engineering "Toolbox" for Design-Oriented Engineers*, in 1994. This publication, authored by B.E. Goldberg, Pat Clemens and others, was produced by the Marshall Space Flight Center in Huntsville, Alabama. SMO was included in the section on preliminary hazard analysis authored by Clemens. It stated,

> "(4) Detect and confirm hazards to the system. Identify the targets threatened by each hazard. A hazard is defined as an activity or circumstance posing 'a potential of loss or harm' to a target and is a condition required for an 'undesired loss event.' Hazards should be distinguished from consequences and considered in terms of a source (hazard), mechanism (process), and outcome (consequence). A team approach to identifying hazards, such as brainstorming (sec. 7.7), is recommended over a single analyst. If schedule and resource restraints are considerations, then a proficient engineer with knowledge of the system should identify the hazards, but that assessment should be reviewed by a peer…." [Ref. 2]

The SMO concept was again published in 1998 by the National Institute for Occupational Safety and Health in a publication called "System Safety and Risk Management: A Guide for Engineering Educators". [Ref. 3] This publication, co-authored by Clemens and Dr. Rodney Simmons, was an instructional module included in Project SHAPE (Safety and Health Awareness for Preventive Engineering), a collaborative project between NIOSH, professional engineering societies and engineering schools, to enhance the education of engineering students in occupational safety and health. Page III-3 of this publication defined a hazard as "a threat of potential harm" and described the SMO model in similar fashion as the Systems Engineering Toolbox did.

In 1998, Clemens included Sheet 98-1 in the System Safety Scrapbook titled: "Describing Hazards? Think Source / Mechanism / Outcome." In it, he gave a more detailed definition of these three elements of a hazard description. It reads:

> "A hazard description contains three elements that express a threat:
>
> - a source — an activity and/or a condition that serves as the root
> - a mechanism — a means by which the source can bring about the harm
> - an outcome — the harm itself that might be suffered." [Ref. 4]

He goes on to say:

> "An open-topped container of naphtha may be a source, but without a mechanism and an outcome, is it a hazard? Suppose it's in the middle of a desert — no ignition sources and no personnel within several miles? Not much of a hazard. Relocate it to the basement of an occupied pre-school facility near a gas-fired furnace. Source, mechanism and outcome now become clear — and it's a hazard." [Ref. 4]

And one last time to make the point, in 2003, Clemens highlighted the SMO model again in Scrapbook Sheet 03-01. He finished that sheet with this "bottom line" insight:

> "If the reviewer/interpreter can't understand the hazard *description*, there's a good chance the analyst didn't understand the *hazard*! Describe hazards using a simple paradigm as a model.
> Make it *simple*, but make it *complete*!
> *Source / Mechanism / Outcome will do the job most every time!*" [Ref. 5]

next page »

Journal of System Safety
eEdition
A publication of the System Safety Society

Vol. 43, No. 6 • Nov.-Dec. 2007

In the Spotlight

Source-Mechanism-Outcome: A Simple, Yet Effective Hazard Description Model

by Donald Swallow, Madison, Alabama

Pages 1 | 2 | 3

The SMO model has also been accepted by the authors of prestigious textbooks. A recent text presents and explains source, mechanism and outcome quite well [Ref. 6]. In addition, the model has recently found its way into drafts of U.S. Department of Defense directives, as system safety practitioners who have been exposed to it, including the author, have found it useful for describing hazards in the process of identifying and assessing them. The SMO model is being included in system safety management plans and program plans, and it has been proposed for inclusion in Military Standard 882, *Standard Practice for System Safety* [Ref. 7].

Detailed Examples

The following detailed example comes from the author's experience working on the U.S. Army's RAH-66 Comanche helicopter program, which shows how the application of SMO can even clarify hazards that we think we know very well. Every helicopter pilot and helicopter system safety engineer knows the term "wire strike." So when the hazard is identified for system safety purposes, one is tempted to use just that term as the hazard description. Actually, "wire strike" is just the mechanism in the SMO model. In the case of the Comanche, when the author joined the program, the hazard description was, "The demonstration and validation aircraft will not have wire-strike protection. For the engineering and manufacturing development aircraft, the lower wire-strike protection has not been defined." However, this describes the hazard in terms of the lack of hazard mitigation, not in terms of the source, the mechanism and the outcome of the hazard. With a little encouragement from the author, the hazard description was changed to, "Flight into wires may result in catastrophic loss of aircraft and loss of life." With this description at least the mechanism and outcome were touched on. However, the full application of SMO yields a description like the following (source, mechanism and outcome are labeled):

> [Source] The mission of Comanche requires it to fly close to the earth's surface using nap-of-the-earth, contour and low-level flying. Flight in this environment means the crew must detect and avoid horizontally strung mechanical, electrical transmission and communication cables (wires). [Mechanism] Crews may fail to detect wires due to degraded visibility, poor navigation or loss of situational awareness. Crews may fail to avoid wires due to not detecting them or failure to follow established procedures for crossing wires. Failure to detect and avoid the wires results in the aircraft flying into the wires. Wires of sufficient diameter will not break and may become trapped or entangled in the main rotor, the electro-optical sensor system, the turreted gun, the external fuel-armament management system and its ordnance, antennas, the landing gear if it is extended, or the weapon's bay doors and their ordnance if they are open. [Outcome] This results in serious damage to whichever of these components the wire strikes. Further, the aircraft may become caught on the wire, resulting in losing control of the aircraft and uncontrolled flight into terrain. This will result in serious damage to or destruction of the aircraft and serious or fatal injuries to the crew.

Now, one can see the source, the mechanism and the outcome of the hazard. And because these are clearly and thoroughly described, it is much easier to identify and implement mitigators to reduce the risk of this hazard. In this example, mitigation includes improved night vision devices to help the crews see the wires. Detection devices can be developed to spot wires using lasers, or infrared or electromagnetic signatures, and to alert pilots to their presence. Improved mapping of wires, combined with extremely accurate navigation systems, can also help crews avoid wires. Improved heads-up displays and controls would help pilots keep their eyes focused outside, looking for wires and other hazards to navigation. The design of the aircraft structure can be improved to allow for wires to be shed on contact instead of caught in the structure. Antennae, landing gear and other external structures can be retracted when not in use. Or, external structures can be designed to break free when they contact wires to allow the aircraft to continue flight. Wire-cutting devices can be designed and placed to optimize cutting the wire if it cannot be avoided.

The strength of the SMO model is that it can be adapted to describe hazards in such a way as to make them easier to understand and manage. The clarity that comes from applying the model is also valuable in the time it saves by eliminating extended debates over the validity of a hazard. When the source, the mechanism and the outcome have been thoroughly described, there is no question whether a hazard is truly a hazard, and whether the analyst's assessment of the outcome is reasonable.

In the application of the model, one often finds that a particular combination of source and mechanism may have the potential to cause harm to more than one asset. An effective way to deal with these multiple outcomes from one source and mechanism is to treat each outcome, each harmful impact on an asset, as a separate hazard (Figure 1).

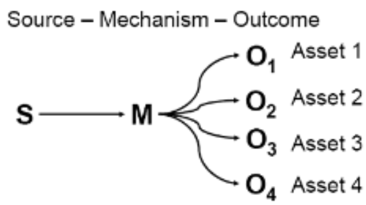

Figure 1 — Single Source and Mechanism with Multiple Outcomes.

The importance of this becomes obvious when each potential mitigator is identified and its effectiveness in reducing the risk to each asset is weighed against the cost and feasibility of the mitigator. In some cases, however, outcomes may be tightly linked; for instance, "death or serious injury to personnel" is linked to "serious damage to or loss of aircraft" when a hazard mechanism includes aircraft impact with the ground. In this case, these two outcomes might best be treated as components of a single hazard.

Another example shows how the SMO model might deal with multiple sources but one mechanism and outcome (Figure 2). The fundamental hazard illustrated in Figure 3 is that a combination of environmental stressors (fatigue, operations tempo, high winds, lack of training, family situation, heat, noise, vibration, degraded visual environment, night vision goggles, seat discomfort, etc.) reduce a helicopter pilot's capacity to deal with the task loading (hovering and maneuvering in close proximity to obstacles, simultaneous mission operations, weapons management, selecting target coordinates, airborne target handover, firing weapons, changing radio frequencies, etc.) as the mission proceeds. This brings the crew to the point where their workload exceeds their capacity to handle the work, and they lose situational awareness (LOSA) — they become incapable of performing a safety-critical task, such as seeing and avoiding an obstacle, maintaining control of the aircraft or correctly handling an emergency. The final result is impact with the terrain or obstacles, serious damage to or loss of aircraft, and serious or fatal injury to the crew.

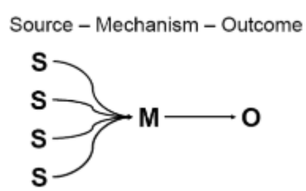

Figure 2 — Multiple Sources with a Single Mechanism and Outcome.

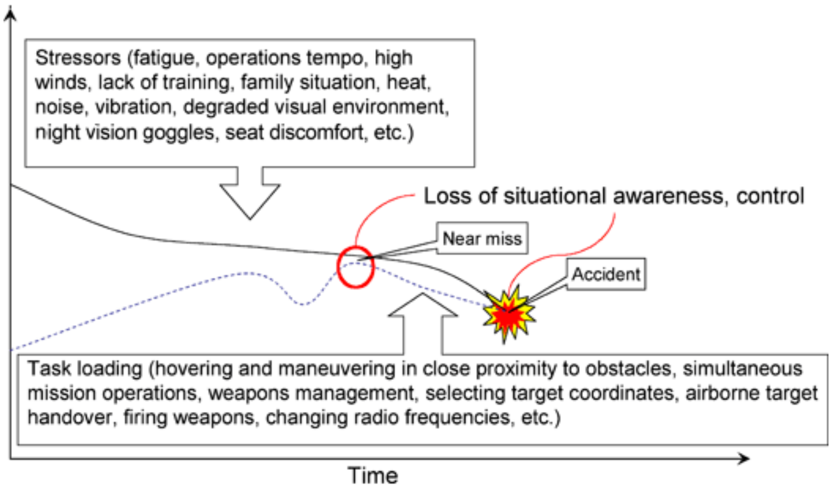

Figure 3 — Interaction of Stressors and Task Loading to Produce an Accident.

Many of the stressors are factors that the pilot or his leadership should manage using the principles of risk management. These factors include training, operations tempo, extended deployment, family and financial issues, illness or death of a family member, pass-over for promotion, etc. Other stressors can be addressed in the aircraft design. These include excessive heat or cold in the cockpit; helmet weight distribution and discomfort; seat discomfort; noise; excessive vibration in the cockpit; excessive dust; irritating odors; bulky, heavy aircrew life-support equipment; flight control geometry; restricted arm and leg movement; display screen size; display word size and color; display icon and graphic size, brightness, color, definition; needed information not displayed; information overload; glare of displays on windscreen at night; and accessing controls and displays with gloved hands.

« previous page | next page »

Journal of System Safety
eEdition
A publication of the System Safety Society

Vol. 43, No. 6 • Nov.-Dec. 2007

In the Spotlight

Source-Mechanism-Outcome: A Simple, Yet Effective Hazard Description Model

by Donald Swallow, Madison, Alabama

Pages 1 | 2 | 3

The general mitigation for this hazard is to reduce environmental stressors as much as possible in order to sustain an adequate level of aircrew alertness and effectiveness, and to help the pilots keep their workload as low as practicable using cockpit automation and well-designed controls and displays that allow the pilot to focus on flight-safety-critical tasks and spend minimum time on less critical tasks. However, while this hazard description follows the SMO model, it is obviously too much to include in one hazard with so many sources contributing to one outcome through one mechanism.

The obvious solution is to break out the sources of the hazard so that each hazard has only one source. So, for example, one hazard might be focused on a stressor, a source, called "excessive heat." It might read, "Excessive heat in the cockpit, combined with other environmental stressors and task loading, brings the crew to the point where they cannot cope with the task load and lose situational awareness (LOSA). This results in failure to see and avoid obstacles or loss of control of the aircraft, resulting in impact with the terrain or obstacles and serious damage to or loss of aircraft, and serious or fatal injury to the crew."

Another hazard focused on a task load factor might read, "The alphanumeric keyboard configuration of the Control Display Units results in extended attention on data entry. This, combined with other task loading and environmental stressors, brings the crew to the point where they cannot cope with the task load and lose situational awareness (LOSA). This results in failure to see and avoid obstacles or loss of control of the aircraft, resulting in impact with the terrain or obstacles and serious damage to or loss of aircraft, and serious or fatal injury to the crew." To use a familiar analogy, the hazard of "breaking the camel's back," is broken down to eliminating or reducing the weight of each straw. Each source can be addressed by the various design teams and ultimately reduce the risk from the overarching mechanism and outcome of the hazard.

> "Because it is so flexible, the SMO model has been successfully applied to the hazards of a wide assortment of systems, and included in many system safety directives."

Using the SMO Model with Other Hazard Identification Tools
The SMO model can also be useful in conjunction with other hazard identification tools. For example, in DoD aviation programs, functional hazard analysis is being used more and more. This method identifies the functions of a system and its subsystems, then evaluates the safety impacts if the function fails or is degraded. The result is a rather extensive list of hazards that is closely tied to the requirements of the system. However, while this method does produce some good information about the safety of the system, it does not always identify what causes the function to fail.

This is where SMO can help. For a function to fail or degrade, there must be a source for the failure. If there are multiple sources, then there are actually multiple hazards. There is, as well, a mechanism or mechanisms that produce the function failure or degradation. The failure of a function should also produce an outcome or outcomes if more than one asset is involved. The outcome with the greatest risk is the assessed severity of the hazard. Thus, we see that while there are various effective tools used to identify a hazard, the SMO model is useful to grasp a quick understanding of the nature of a specific hazard, or whether that hazard is even a valid hazard.

Conclusion
As the above examples show, the SMO hazard description model is a useful tool in the toolbox of the

system safety practitioner. It is simple, yet effective, in helping the practitioner understand the nature of a hazard once he or she has identified it using any hazard identification method. Using it, hazards are clearly and thoroughly described, making it much easier to identify and implement mitigators to reduce the residual risk. Because it is so flexible, the SMO model has been successfully applied to the hazards of a wide assortment of systems, and included in many system safety directives, instructions and training syllabi. This is why the Government Electronics and Information Technology Association's (GEIA) System Safety Committee (G-48) recommended the inclusion of the SMO model in the next revision of U.S. Military Standard 882, *Standard Practice for System Safety*.

About the Author

Don Swallom is currently a safety engineer for the United States Army Aviation and Missile Command Safety Office, Aviation System Safety Division, at Redstone Arsenal in Alabama. He holds a Bachelor of Science in Engineering Sciences from the United States Air Force Academy and a Master of Science in Systems Management from the University of Southern California. Prior to his current position, he served as a helicopter pilot, staff officer and developmental engineer in the United States Air Force. His last Air Force assignment was as the chief of safety for the Arnold Engineering Development Center, the world's largest complex of aerospace ground testing facilities. He collaborated on the system safety chapter of the *Handbook of Human Systems Integration* (John Wiley and Sons, 2003). He makes his home in Madison, Alabama.

References

1. Clemens, P.L. *System Safety Scrapbook*, Sheet 84-3, 10th Ed. A-P-T Research, Huntsville, Alabama, 2004.
2. Goldberg, B.E., *et al.* "System Engineering 'Toolbox' for Design-Oriented Engineers," NASA Reference Publication 1358, Marshall Space Flight Center, Alabama, 1994.
3. Clemens, P.L. and R.J. Simmons. "System Safety and Risk Management: A Guide for Engineering Educators," National Institute for Occupational Safety and Health, page III-3, Cincinnati, Ohio, http://www.cdc.gov/niosh/topics/SHAPE/pdfs/safriskengineer.pdf (Accessed March 12, 2006).
4. Clemens, Sheet 98-1.
5. Clemens, Sheet 03-01.
6. Ericson, C.A. *Hazard Analysis Techniques for System Safety*, page 93, John Wiley and Sons, Hoboken, New Jersey, 2005.
7. Military Standard 882E (Draft), *Standard Practice for System Safety*, pp. 5, 9, 27, 78, 80, Department of Defense, Washington DC, Feb. 1, 2006.

« previous page