*Science and Engineering Ethics (2004) **10**, XX-XX*

Evil Intent and Design Responsibility*

Bart Kemper, *Kemper Imageering, Inc.*

Keywords: weapons of mass destruction (WMD), explosion, public safety, disaster, attack, design responsibility

ABSTRACT: *Mass casualty attacks in recent years have demonstrated the need to include "evil intent" as a design consideration. Three recent actual or potential weapons of mass destruction (WMD) attacks did not involve nuclear bombs or other devices designed as weapons, but rather benign objects used with evil intent. Just as unplanned events such as hurricanes, earthquakes, fires, and user misuse have been codified into design requirements based on the likelihood and potential impact of the event, "evil intent" has to become part of the design process for buildings, vehicles, equipment, and other items. The endstate should be reasonable additions to existing codes and standards such that it is clear what is and is not designed for. In the absence of specific design guidance, professionals with appropriate expertise can assess potential for "evil intent" and provide recommendations to design out or warn against this potential harm to public safety, particularly when codified requirements are not present.*

Evil Intent and Design Responsibility

Mass casualty events in recent years have demonstrated the need to include "evil intent" as a design consideration. Three recent actual or potential weapons of mass destruction (WMD) attacks did not involve nuclear bombs or other devices designed as weapons, but rather benign objects used with evil intent. Most current design codes and practices do not consider sabotage, deliberate attacks, deliberate misuse of the design, collateral damage from attacks targeted elsewhere, and other actions that could be considered the result of "evil intent." Notable exceptions include the nuclear industry and military facility design. Recent events indicate that "evil intent" should be considered along with earthquakes, fires, hurricanes, and other unpredictable possible design conditions.

* An earlier version of this paper was presented at the "Ethics and Social Responsibility in Engineering and Technology" meeting, New Orleans, 2003.

Address for correspondence: Bart Kemper, PE, Kemper Imageering, Inc., **STREET ADDRESS, CITY ZIP CODE,** USA; email: bkemper@bigdogz.com.

1353-3452 © 2004 Opragen Publications, POB 54, Guildford GU1 2YF, UK. http://www.opragen.co.uk

Design Responsibility

As described in Shigley & Mitchell,[1] the need to be addressed, or "design intent", is generally the driving factor in a given engineering design, whether it is a building, a vehicle, or an equipment item. "Safety and reliability" are often a close second to design intent, since a design that cannot perform as required in a reliable, predictable, and sufficiently safe manner is generally of little use. Many factors, including fire, weather events such as hurricanes or blizzards, geometric tolerances, corrosion, fatigue, transport and storage, and even user misuse and abuse, are typically considered in the pursuit of a safe and reliable design.

Procedures for designing out hazards exist. The U.S. Department of Defense's "Standard Practice for System Safety" outlines such a procedure in detail. It instructs design engineers to "identify all risks, assess the possibility of the risk and potential impact, then either design it out or mitigate the risk and provide warnings of the residual risk."[2] This standard applies to catastrophic failures of components, fire, earthquakes, maintenance issues, operator error, and any other circumstance that could impact the safe operation of a given system, as well as issues such as weapons effects and sabotage, where applicable. However, it provides only the procedure for managing the risks once they are identified and quantified, not a standard measure for any of these potentially hazardous events.

Martin and Schinzinger[3] detail how engineers, as design professionals, have a special moral obligation to safeguard the public. For Professional Engineers it is also a legal requirement, as in Chapter 8 of the Louisiana Revised Statutes.[4] This includes addressing how a design may perform under special circumstances such as an earthquake. The creation of weapons of mass destruction (WMDs) from benign objects is perhaps the most extreme example of evil intent. While the likelihood of this kind of use is very low, the threat to the public is high enough to warrant consideration.

"Intent" is defined by the 'Lectric Law Lexicon as "determination or resolve to do a certain thing, or the state of mind with which something is done."[5] In defining "crime," the plain language dictionary in Nolo.com states that acts carried out with an antisocial or "evil" intent are usually considered worthy of punishment.[6] This differentiates "misuse," which includes any use of a design for an application other than the design intent, and "abuse," which is using the design for the correct application but in an incorrect manner and with a specific desired outcome that is harmful.

WMD is defined militarily in FM 3-0 *Operations* as "weapons capable of a higher order of destruction and/or of being used in such a manner to destroy large numbers of people…including nuclear, biological, chemical, or radiological weapons."[7] Under Title 18 of US federal law it also includes "any destructive device," which is "any explosive, incendiary, or poison gas; bomb; grenade; rocket having a propellant charger of more than four ounces; missile having an explosive or incendiary charge of more than one-quarter ounce; mine; or devices similar to any of the preceding."[8] Weapons of mass destruction, therefore, include not just nuclear devices but car bombs, large fires, and other devices that could threaten the public.

CASE 1: Northern Oilfields of Iraq (2003)

The planned weapon was a chemical attack created by opening oilfield wellheads. The original design intent of the wellheads was to bring oil out of the ground.

During the combat phase of Operation Iraqi Freedom there was significant concern that Saddam's forces would use the oilfields in northern Iraq to create a chemical WMD. These oilfields are high pressure and "sour," meaning they naturally contain high levels of hydrogen sulfide gas (H_2S), which is deadlier than cyanide. Military protective masks are ineffective against hydrogen sulfide. It was known that Iraqi forces were rigging explosives in the oilfields to prepare to open the wellheads.

The attack method of a single or multiple releases was anticipated and analyzed by the National Ground Intelligence Center.[9] This attack would have exploited the oilfield design, which appears to have been conceived with little regard for potential harm to the local populace in the event of a catastrophic release. According to NGIC, the result for a multiple wellhead release was a hazardous area 10 km by 20 km in which only personnel with self-contained breathing apparatus could operate safely (see Figure 1). Within several hundred meters of a wellhead the exposures would be immediately lethal. Over a million Iraqi civilians in Kirkuk and surrounding villages would have been at risk of toxic and potentially deadly exposures. Because of the added hazard of H_2S, capping these open wellheads would have taken significantly longer than the capping operations that were undertaken in the aftermath of the first Gulf War.

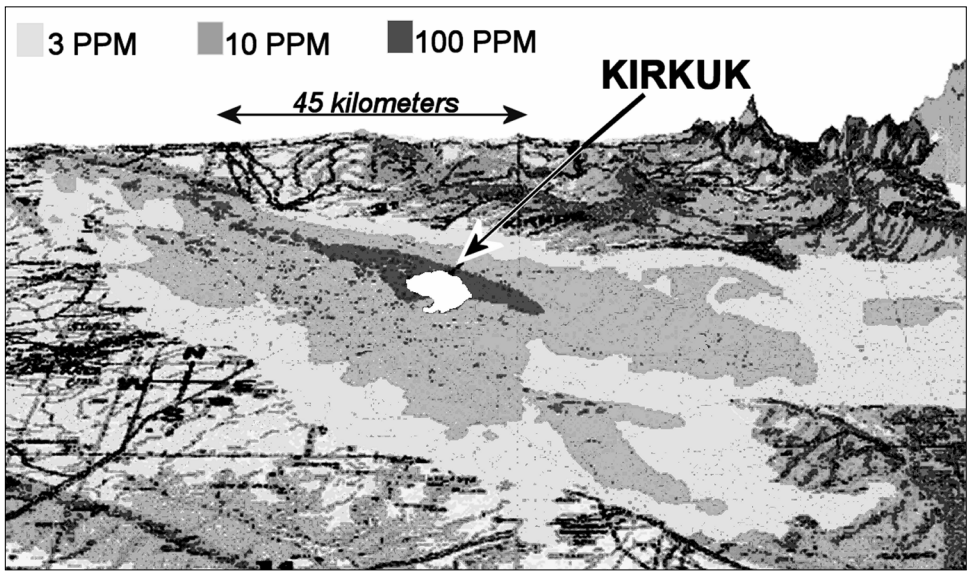

Figure 1. Potential hazard of multiple point release of hydrogen sulfide in northern Iraq near Kirkuk. 10 ppm is the threshold for 8-hour exposure without protection, 100 ppm is the threshold for immediate threat to health and life. For clarity, Kirkuk has been shown in white. Imagery by NGIC.

To put this kind of threat into action requires only a minimum amount of skill: simply attaching a chain to a capped well and pulling it open with a truck would suffice. Using an explosive could actually be counter-productive, as an ignited wellhead would burn off the deadly gas. The most significant barrier to successful implementation would be the number of wellheads that would have to be opened and the coordination required to do so without compromising the safety of the work crew. Even a single wellhead could be a threat. As reported in the CNN,[10] a single sour gas wellhead release in China killed 198 people, poisoned over 9,000, forced over 41,000 to flee, and created a 10 square mile "death zone" in December, 2003. This potential attack illustrates the threat that many industrial sites, including pipelines, petrochemical refineries and chemical plants, potentially present.

CASE 2: The Oklahoma City Bombing (1995)

The originally design intent of the weapon was to move personal items (a rental truck) and to fertilize plants (ammonium nitrate.) The resulting weapon was a explosion of an estimated 4,800 pounds of ammonium nitrate/fuel oil (ANFO) explosive transported by a 24-foot rental truck and parked near the targeted building. The Department of Civil Emergency Management's After Action Review (1996)[11] reports that the blast demolished a third of the Alfred P. Murrah Federal building, killing 168 and injuring 426.

The attack method was a car bomb, which has been used in terrorist attacks worldwide over the last 30 years. Other examples include the Khobar Towers in Saudi Arabia and the Marine Barracks in Beirut. The attack exploited the fact that a van truck could be parked relatively close to the building.

Carrying out the attacked required a modicum of training. McVeigh, one of the bombers, had learned how to make ANFO charges during his earlier training as a combat engineer in the U.S. Army. This is also common knowledge on farms and ranches, where fertilizers and fuel are mixed for the purpose of blasting tree stumps. Timing devices are relatively simple to build, and plans are available in print or on the internet. In 1998 Gene Corley testified before a U.S. House committee that the damage and loss of life from the explosion could have been reduced 50-80% "for the cost of thousands, not millions, of dollars," if seismic design had been used in the structural frame of the building.[12] This attack illustrates the vulnerability which almost any building must potentially address as well as there being cost effective remedies if applied in foresight.

CASE 3: The World Trade Center Attack of 11 September 2001

The weapon's original design intent was to fly passengers and cargo over extended distances. The weapon was a fire causing a structural collapse of a skyscraper, killing over 3000 tower occupants, aircrew, passengers, and first responders.

The attack method was crashing a large jetliner into the buildings. According to the FEMA report,[13] it required several elements. First, it required a large jetliner that had a

full fuel supply, such as a 767-200 leaving the US for a transatlantic flight. Second, it required gaining control of the aircraft by exploiting US security and the physical security measures aboard the aircraft. Third, it required personnel trained to navigate the plane to its target and fly it into the building at full throttle generally perpendicular to the building face, creating a sufficiently hot and widespread fire to cause the assumed desired intent. Finally, it required striking the towers high enough to allow for the required approach but low enough to place sufficient building mass above the impact area to assure a failure of the floor decks that would create a downward "domino effect" and result in total building collapse (see Figure 2).

The designers of the World Trade Center had anticipated that the building might be struck by an airliner due to pilot error during approach; consequently, the building was made to withstand being struck by a Boeing 707 with little fuel remaining. The designers, however, did not anticipate a deliberate attack motivated by "evil intent," nor the use of larger planes such as the Boeing 767, which was designed after the towers were built, nor the possibility that those planes would have full fuel tanks.

The degree of difficulty was high. The plans and history of the building were probably reviewed by the attackers in order to determine potential weaknesses to exploit. Plans of the World Trade Center were used in the 1993 attack and may have been used in the 2001 attack, given both groups' well-publicized ties to Osama bin Laden. Determining which commercial flights were available and suitable for the mission would have been fairly simple. However, training suicide pilots for this act took considerable technical training and resources as well as advanced planning. According to Reuters and other news reports, the FBI credits Khalid Shaikh Mohammed, a US-trained mechanical engineer who was captured in March 2003, with the September 11 attacks as well as others.[14] It appears Mohammed used detailed problem-solving techniques, typical of the engineering profession, to achieve his desired goals. While there are no public data available about the planning of this attack, it can be deduced that while the chain of events required to drop a tower could have occurred by happenstance, the fact that the required elements occurred twice – once in each tower of the World Trade Center – indicates the entire chain of events may have been by design. Even if the specific intent of creating a fire to cause failure of the connecting clips did not exist, Mohammed had the technical knowledge and training to anticipate this effect, and this failure mechanism is certainly now well publicized. This attack illustrates the danger engineer training applied with evil intent can present.

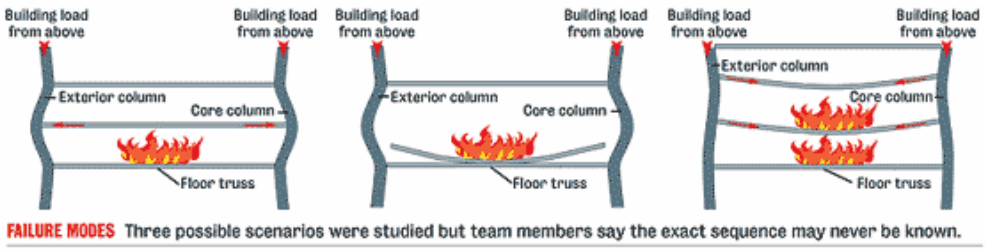

Figure 2. Three modes of failure due to the fires in the World Trade Center. Imagery by FEMA.

Engineering Response

Risk assessment and risk mitigation are part of design. Designing to protect against evil intent, like any other design consideration, has to be balanced against the likelihood and potential consequences of such use, and other design factors such as weight, cost, and functionality. Andrews and Moss detail several techniques such as Qualitative Risk Assessment (QRA), fault trees, and Failure Mode and Effects Analysis (FMEA) to examine a product or process reliability and then mitigate identified risks.[15] These techniques could be readily adapted to address evil intent, including sabotage, hostile misuse, and being an intended or unintended target of hostile acts, as part of the risk analysis and reliability assessment process.

As with any analysis, however, the results are only as good as the data provided. In the absence of clear guidelines or specifications, additional expertise may be required to fully assess vulnerability to, and potential consequences of, evil intent. Blast analyses, security reviews, and worst case analyses are tools that could potentially supply the responsible in-charge engineer with the data required for subsequent analysis. Some of this has already been incorporated into military engineering, such as Army TM-583-1, *Security Engineering Project Development*.[16] The same measures should be considered in civil, industrial, and other engineering applications, along with other design factors. Efforts should include warning the appropriate buyer or user of the vulnerabilities or hazards that have not been designed out. The recent ruling that families of the September 11, 2001, attack may sue the airlines and others for essentially failing to anticipate and stop the evil intent of others indicates that in the future, unexpected events such as fires, earthquakes, and user misuse and abuse, will require specific minimum design standards for a given situation.

As design professionals, engineer have the final say about a design's capabilities and vulnerabilities. Just as earthquakes, hurricanes, floods, and other unpredictable, even unlikely, events have been codified and incorporated into standard engineering practice, so should the various aspects of evil intent. The risks must be identified. If the risks cannot be designed out, they must be mitigated, and due warning of the residual risks must be given. The endstate should be reasonable additions to existing codes and standards that specify what is and is not addressed in the design constraints as well as some measure of standardization for threat and its design remedies. This would allow for reasonable risk assessment and risk mitigation decisions. The threat of a signficant attack directed at infrastructure is unlikely to disappear. Until this issue is addressed through codification, the use of other resources should be considered to assess design requirements and provide an engineering response that will safeguard the public.

REFERENCES

1. Shigley, J.E. & Mitchell, L.D. (1983) *Mechanical Engineering Design, 4th Edition*. McGraw Hill Book Company, New York, NY, pp. 6-8
2. U.S. Department of Defense (DoD), *MIL-STD-882D Standard Practice for System Safety*. 10 February 2000.

3. Martin, M.W. & Schinzinger, R. (1989) *Ethics in Engineering, 2nd Edition*. McGraw Hill Book Company, New York, NY, pp. 48-58.
4. Louisiana Revised Statutes 37:681-704 (2000), Chapter 8. Professional Engineering and Professional Surveying.
5. 'Lectric Law Library's Lexicon, Definition of Intent. Retrieved June 27 from http://www.lectlaw.com/def/i053.htm.
6. NOLO. "What Is A Crime," Online Legal Encyclopedia. Retrieved June 27, 2003 from http://www.nolo.com.
7. US Army Field Manual (FM) 3-0, *Full Spectrum Operations*, June 2001.
8. US Federal Code, Title 18, Part I, Chapter 44, Section 921, Definitions.
9. Barbarksky, R., Smith, H.T., Higgins, W., Newell, R., Herbelin, J. (2003, June) *Consequences of Iraqi Use of Oil as a Defensive Weapon.* National Ground Intelligence Center (NGIC).
10. CNN. (2003, December 27) China Seals Well After Leak. Retrieved 28 December 2003 from www.cnn.com.
11. Oklahoma Department of Civil Emergency Management (ODCEM) (1996) *After Action Report, Alfred P. Murrah Federal Building Bombing.*
12. Corley, Gene W., P.E., S.E., Ph.D. Testimony on Security of Federal Buildings on Behalf of American Society of Civil Engineers (ASCE), before House Committee on Transportation and Infrastructure (June 4, 1998).
13. Federal Emergency Management Agency (FEMA) (2002, May) *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations*.
14. Reuters. (2003, March 1) Khalid Sheikh Mohammet is Biggest Al Qaeda Catch. *KPBS News Room*. Retrieved 27 June 2003 from http://www.kpbs.org.
15. Andrews, J.D. & Moss, T.R. (2002) *Reliability and Risk Assessment*. ASME Press, New York, NY.
16. US Army Technical Manual (TM) 5-853-1, *Security Engineering Project Development*. May 1994.

Author Note: Bart Kemper, PE, is the principal engineer for Kemper Imageering, Inc. A significant portion of his work has been involved in industrial equipment design, product design, and the design and analysis of different security devices as well as performing reliability studies, blast analyses, and FMEA analyses on commercial equipment, including marine, offshore, and industrial facilities. He is also a US Army Reserve captain in the Corps of Engineers and was mobilized and deployed overseas in February 2003 in support of Operation Iraqi Freedom as a member of the 412th Engineer Command, headquartered in Vicksburg, Mississippi. A significant portion of his duties involved reviewing intelligence, analyzing potential courses of action, and evaluating risks with regard to Iraqi and Coalition activities in the northern Iraqi oilfields as well as base camp design and infrastructure engineering. This paper is unclassified and has been cleared for publication.