INL/CON-06-11067
PREPRINT

Rationale and Development of a Security Assurance Index With Application Toward the Development of a World Risk Index

2006 Risk Conference

M.M. Plum
G.A. Beitel

June 2006

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint should not be cited or reproduced without permission of the author. This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the United States Government or the sponsoring agency.

Rationale and Development of a Security Assurance Index with Application toward the Development of a World Risk Index

M. M. Plum and G. A. Beitel, PhD
Idaho National Laboratory, Idaho Falls, Idaho, USA

Abstract

Assurance categories were previously developed to support the Department of Homeland Security's efforts in the mitigation of Cyber Control System events. Defined according to the risk of life and economic loss, the minimum range is designated by policy; whereas, the maximum limit seems to be constrained only by limits and interdependencies of the event. Use of this life / assets scale has proven to be helpful in managing risk due to the scales ease in use, communication, and understanding. Suggestions have been made that this scale could be applied to all events of terror, disaster, and calamity of an international scale, with equally good results. This paper will present the history of some existing scales of disaster and assurance, the rationale behind the development of the original Security Assurance Index, and our proposed scale of disaster and calamity as a World Risk Index.
Keywords: World Risk Index, Security Assurance, risk management, risk scale.

1 Introduction

Since 9-11, the United States has been allocating a tremendous amount of resources for the prevention of future terrorist attacks. Within the month, the President established an executive-level Office of Homeland Security (OHS) with a mission to "develop and coordinate the implementation of a comprehensive national strategy to secure the United States (its people and physical assets) from terrorist threats or attacks." Within the year, the Homeland Security Act of 2002 created the Department of Homeland Security (DHS)

which integrated many federal agencies into one organization with the purpose of protecting the homeland. Although DHS supersedes the function of OHS, the overall mission remains the same.

In its mission of protection, deterrence, and mitigation, DHS has organized its activities according to threats, targets, and recovery assets. Threats include the weapons of bioterrorism, nuclear, and cyber assets; targets include centers of population, critical infrastructure, and national icons: and recovery assets include emergency planning, evacuation planning, and medical response. Because DHS does not have the resources to protect, deter, and mitigate, its primary purpose is to integrate the many existing federal agency activities and enable them to more effectively deal with threat, target, and mitigation activities. For this reason DHS established the Control System Security Program, managed by the Idaho National Laboratory (INL) to "reduce the risk to the Nation's critical infrastructure from cyber attacks on control systems."

To develop a program in reducing risk from terrorist attack on control systems, the risk of attack must first be calculated. Risk is classically calculated as a "combination of the probability and the consequence of a hazard (or threat event)"[1]:

$$Risk = Probability\ (of\ Attack) * Consequence\ (of\ Attack) \qquad (1)$$

Logically, if either probability or consequence of attack is zero, risk will be zero. In general, the probability of attack (best expressed as a probability per unit time or frequency) on a control system is typically very low (approaching 10^{-9} or even 10^{-12} events per year) and it may be very high (10^{3} or even 10^{6} events per day). On the other hand, the consequences may be insignificant and they may be catastrophic. Given this range in risk outcomes, understanding the impact of risk reduction activities is a primary goal in managing terrorist risk to control systems. Likewise, communicating the risk of these very low probability / very high consequence events is also difficult.

To help manage the risk of cyber attack on control systems, INL developed a Security Assurance Index (SAI) to communicate risk. While presenting this scale for review, other risk management professionals suggested that the SAI could be modified to communicate world risk events. Thus, the purpose of this paper is: 1) to present the development and use of INL's SAI, and 2) to propose the development and use of a World Risk Index (WRI) to communicate the risk of events that threaten the world's population.

2 Control System Risk and Development of the SAL

INL has been tasked by DHS "to reduce the risk to the Nation's critical infrastructure from cyber attacks on control systems." Control systems have been recognized as a significant threat and security issue due to the power a control system provides a malfeasant or criminal element. This power is inherent due to a control systems function which is to manage and control the behaviour of other systems, subsystems, and their components. Thus, the

incorrect operation of a control system impacts the function of the entire system. Worse, a control system could be used to deliberately damage the system, damage other interdependent systems, and possibly use the system as a weapon against people.

A prime example of control system's power is provided by the interrelationships of a critical infrastructure such as water, electricity, or mass transit system and the community that depends on them. Thus, not only is it possible to damage a critical infrastructure asset using a control system, this control would create secondary effects such as economic disruption, injuries, and death. Given these interdependencies, consequences from a control system attack are significant: 1) if control systems are prevalent within infrastructure, 2) if these control systems are insecure, and 3) if the knowledge of cyber and control systems is within the terrorist's capability.

In the process of risk management, we have discovered that communicating risk is difficult. Our experience suggests that risk is usually communicated as a qualitative measure (low, medium, high) versus a quantitative measure (probability, consequence, and probable loss). From our observations, this difficulty in communication is a result of three issues: 1) lack of incident data, 2) lack of knowledge on attacker capabilities, and 3) the ever changing environment of cyber and control system technologies. Given this overall general lack of knowledge, when risk is calculated, it is usually distributed over a wide range of possible outcomes, depending on the available data, the bias of the evaluators, and intent of the risk evaluation.

2.1 Problem Statement

Risk management includes the activities of assessing, evaluating, and mitigating risk. In efforts to reduce risk, risk must be effectively communicated between people of different interests, skills, and objectives. Most importantly, if we are to reduce risk, we must be able to measure and communicate the effects of risk reduction. This is our primary problem, "How can we effectively communicate control system risk?"

2.2 Initial Communication Requirements

In solving this problem, we determined that we needed a communication tool. A tool is a good solution as it provides a process, method, and standardization. To acquire this tool, we identified a list of "must have" requirements through an informal and iterative process of generation and review:

- risk must be communicated by a scale of measure
- The risk measure must be calculated with minimum information
- The risk measure must be calculated across many infrastructure sectors
- The scale must be easy to use, communicate, and understand
- The scale must become indispensable to the risk management process
- The scale may be similar to the DHS scale

Often, the fastest way to acquire a tool is buy it off the shelf and adopt a process already in use. For this reason, we allocated time to identify other scales in risk communication and review their advantages and disadvantages. We left open the option of whether we would adopt, adapt, or develop our own scale. During this review, it became obvious that risk scales (as well as all other scales) are simply human constructs of reality or perceived reality. Some scales provide better constructs than others, but the success of any scale that communicates risk would be measured by its popular use. Knowing this, it was imperative that our risk scale would have those attributes to insure adoption.

2.3 Review of Scales in Risk Communication

For the purpose of organizing the discussion, we have organized the scales into three separate reviews: 1) the existing DHS Scale, 2) scales in natural disaster risk, and 3) scales in security and safety risk. We are not aware of any formal organization for scales used in communicating risk.

2.3.1 The DHS Scale

The DHS communicates and advises the US public on security risk using their Homeland Security Advisory System[2]. A risk value is determined by threat and vulnerability assessment information; however, because consequences are not included in the analysis, risk is implied by the vulnerability, threat, and potential consequence. This implied risk is communicated using a simple color scale:

- Red – Orange – Yellow – Blue – Green
- The highest risk level, Red, signifies "severe risk of terrorist attacks"
- The lowest risk level, Green, signifies "low risk of terrorist attack"

The advantages of this scale are its ease in understanding, similar to any scale that uses red to alert danger and blue or green to alert an all safe condition. However, although easy to communicate, it is commonly agreed that this scale is ignored and fallen out of general use. Although there may be many reasons for this, our primary criticism is the lack of a published method to determine risk (i.e., when does a "red" alert change to an "orange" alert). Furthermore, because the entire nation is put on alert versus regional or local alert, people tend to ignore information when they are not part of the threat situation. Thus, although the scale communicates risk effectively, it has not been administered correctly.

We concluded that even if we could fix this scale as a quantitative scale of measure, the process of modifying and approving these modifications would be difficult. However, the color code system has advantages in communication.

2.3.2 Scales of Natural Disaster Risk

Many scales are used to communicate risk of natural disasters. However, all of the scales we reviewed measured specific threats versus a general threat. We

have listed the better known scales[3] that are used to communicate the risk of many natural threats common to the US over the course of the year:

- Fujita (F1 – F5) measures tornadoes
- Richter (1 – 8) measures earthquakes
- Modified Mercalli (I – XII) measures earthquakes
- Saffir-Simpson (Cat-1 – Cat-5 / white to red) measures hurricanes
- Torino (0 – 10 / white to red) measures near-earth objects

Similar to the DHS scale, all of these scales organize threat on an increasing scale where a higher number indicates a greater threat (and risk). Likewise, all of these scales require the user to estimate probability to calculate their personal risk to life, limb, and property given their individual situation. However, it is common for local authorities to evaluate local threat information from which they communicate risk warnings or even mandate actions to be taken by the local population.

Most of these scales color code each category to communicate the threat and implied risk visually. Like the DHS scale, most of these scales use a minimum number of levels, often five, which minimizes and simplifies the communication process. The exception to these rules seems to be those events where the consequences could extend beyond a region such as the threat posed by near-earth objects. Near earth objects have the capability of impacting humanity on national, continental, and world scale. However, because disasters of world-wide scale are not often experienced by humans, scales of calamity are not typically communicated on a daily basis (the Torino scale was the least recognized scale). However, we noted that the Torino scale might be appropriate for certain terror events where weapons of mass destruction (bioterrorism, nuclear events) could have national and world-wide effects.

Given these observations, our overall suggestion is that many of these scales would communicate risk more effectively if they calculated risk versus ranking the events by a threshold of wind speed or ground movement. For this reason, we maintained our requirement of communicating the risk as the outcome of event probability and consequence.

2.3.3 Scales of Security and Safety Risk

Our review of scales in safety and security suggests that these scales have a very narrow application and are typically used only within industry sectors and their associated professions. In general, safety scales are developed to increase the safety of a final product and support best practices in design and operation. Typically, best practice requires a minimum of analysis to: 1) identify the vulnerabilities in construction, manufacturing, and use, 2) provide fault trees, event trees, and failure rates to calculate probabilities, and 3) organize the results into predetermined categories. Given this process, most of these scales are used only by the design, safety, and industrial engineers within the associated

industry. We did not find any situation where the risk of an engineered system was communicated to the general public.

The ANSI/ISA (American National Standards Institute / Instrument Society of America standard S84.01-1996) Security Integrity Index (SIL) is a good example of a safety scale which measures the risk of "failure on demand" for safety instrument systems[4]. Similar to other scales mentioned, a minimum number of levels (SIL-1 to SIL-4) refer to the "level of hazard or economic risk". However, as in the previous scales investigated, SIL does not calculate risk as it is classically defined; rather, the engineer is required to estimate a probable, worst case scenario to understand the risk of the engineered failure rate.

All of the security scales we identified were related to food security and its associated risk to famine. In general, these scales are used to communicate the risk of famine and help prioritize risk relief efforts. Interestingly, most of these scales calculate and communicate famine risk as potential deaths. And although famine is quite different than a cyber terror event (a long term event versus an event of short duration), probabilities and consequences are being calculated to determine probable deaths and consequences (risk). For many reasons, there is no widely accepted scale, although the Famine Codes, Food Security Assessment Unit, and Famine Intensity Scale have been used to over the last 100 years to communicate pending famine calamities[5]. Of these, the most promising famine scale has been proposed by Paul Howe and Stephan Devereux where famine is measured by "intensity" and "magnitude"[6]. We noted that, again, most of these scales communicate risk using four or five levels where the higher numeric values refer to higher famine risk and consequences.

2.4 Addition to Our Communication Requirements

Our review of the most commonly used risk scales confirmed our initial requirements for good communication. However, the primary drawback of most of these scales is they do not rank risk; rather, they rank threats and imply risk. For our purpose, this issue proves to be a serious omission given our experience in communicating the control system risk and the complexity of the technology. For this reason, we added one more requirement to supports our primary CSSP mission:

- The scale must quantitatively measure risk (to be able to reduce risk)

Bottom line, our scale must communicate risk on the control systems of this country's critical infrastructure. Given a sufficiently rigorous process, we could assure DHS on the risk posed by a control system given its configuration, associated vulnerabilities, target attractiveness, and the potential consequences. From this concept of assurance, we named our scale - Security Assurance Index (SAI). Because a scale demands levels, we would classify risk by levels; hence, the Security Assurance Level (SAL).

2.5 Another Observation of the Risk Scales

Another interesting observation in this review was the mathematical relationships between the threshold limits of each level. Although not strictly held, the thresholds between levels are determined using by a logarithmic scale. Whether we were talking about energy to move earth (Richter), power of wind (Fujita), or the probability in safety failure (SIL), the range within a level is defined by the logarithm of the lower boundary. This is also true of other scales in physical phenomena such as light and noise.

Mathematical in nature, this response to increasing stimulus was first postulated by Gustav Fechner in the 19th century as natural and human. Fechner, a German experimental psychologist, suggested from his observation of the human senses, that "within limits, the intensity of a sensation, S, increases as the logarithm of the stimulus, R,[7]" or,

$$S = k \log R \qquad (2)$$

Known as Fechner's Law, it has been shown to be applicable to "just noticeable differences," right and wrong, average error, visual distance, visual brightness, and weights. Our observation is that risk may also be communicated on a scale of "noticeable differences" similar to other sensations. Further studies are needed to prove this out.

2.6 Observations in Risk Communication

Besides the problems in communicating risk, another nagging problem was associating threat possibilities to risk possibilities. This problem is entirely determined by the distribution of probable scenarios and their probable consequences. For example, an F-5 tornado may land only on unpopulated areas for 4 or 5 miles; whereas, it is possible that the same F-5 tornado may land on many densely populated areas and maintain its ferocity for 100 miles or more. In a worst case / best outcome scenario, this event may create only $100k in loss; whereas in a worst case / worst case scenario, $1B or more of loss may occur. This wide range in consequences not only depends on the random probability of the event, but also on human response in defense, security, safety, and recovery.

Given these wide ranges in probabilities and consequence, it is conceivable that risk can range by 4 or 5 orders-in-magnitude. Thus, this observation would suggest that Katrina could have resulted in a $100M loss if it would have fallen on a remote Texas coastline; rather, it landed on New Orleans, creating an economic loss exceeding $125B[8]. In summary, our communication tool must be able to communicate the possibilities of wide ranges in risk outcome.

To communicate this complexity in scenarios and probabilities, we proposed that we could calculate a probable outcome, a single value, to describe this distribution of risk. For example, if we assumed a logarithmic distribution of possible outcomes, we could calculate a median value to describe a probable outcome. This assumption proved to be relatively accurate because we know consequences are not perfectly random and normally distributed; rather, the

human actions in survival, response, and intervention tend to skew the outcomes to lower consequences. Thus, to calculate a probable outcome of a distribution of consequences, we have been using the following equation to calculate the median of an assumed logarithmic distribution:

$$median = EXP (((LN (lower) + LN (upper)) / 2) \quad (3)$$

From our experience, the risk from terrorist initiated control systems may be less random than we originally thought. Both initiating events and consequences are not random by their very nature. Instead, these events and actions are mostly controlled by people or engineered systems. Terrorists select targets that are worth their "investment" in time, money, and people. They plan and train to increase the success of an attack. Conversely, attacks fail (for reasons other than errors, mishaps, and chance) due to security, defense, and response actions of the target. Security, defense, and response planners also plan and train for the threats of attack. These activities reduce the risk by lowering the potential consequence. Thus, given the complexity of attack and defense investments, actions, and response, we continue to assume that a reasonable range of possible consequences continues to be between 3 or 4 orders-of-magnitude.

The significance of this observation is that we have come to conclude that for our basis of design risk, the range of possible outcomes will be defined as a logarithmic distribution of 4 orders-in-magnitude once we have identified the worst case / worst outcome scenario.

2.7 Development of the Security Assurance Index

As previously stated, the risk posed from control systems can be calculated as a mathematical expression of probability and consequence (see Equation 1). Although the objective of this paper is not to discuss how we calculate control system risks, we felt it important to discuss issues in determining risk given the range of consequences for any given scenario.

In determining the probability of a successful control system attack, we must identify and acknowledge the varying degrees of influence. For example, there are probabilities in whether an attack can be initiated or not, probabilities in how the attack is initiated, and probabilities in how the attack progresses. These probabilities may be calculated assuming the following technical and human influences:

- Control system configuration and its inherent vulnerabilities
- Administration of the control system's maintenance, security, safety, etc
- Site Attractiveness and impact or access to other attractive sites
- The potential attackers, their intent, capabilities, resources, etc
- The site's and community response once an attack has been initiated
- Environmental variables that may impact an initiated attack

Likewise, the probabilities in attack consequences are dependent on the many variables for each target as well as the interdependencies and outcome of the other secondary and unintended effects: These could include:

- Human losses, including death and injury to on- and off-site populations
- Economic losses, including capital, inventory, and environmental
- Market disruptions, including short- and long-term effects
- Environmental variables that may impact the outcome of attack
- Other more difficult to assess consequences such as loss of national confidence, influence, freedoms, morale, safety, and emotional stress

As terrorism goes, the worst case / worst outcome scenario would be the total loss of US population. (Note: although the authors are not suggesting that this could be possible given the U.S.'s geographical size, isolation, and systems in defense, security, and response, we propose this outcome as an extreme consequence, an outcome *ad nauseam* to define the upper boundary for the purpose of scale development. We assumed a scenario for the total loss of American lives. Our estimate of 300M is higher than the 2000 population census so that the scale remains relevant for the near future.)

Assuming 300M citizens as the upper boundary in loss, our rationale allows us to assume a low range consequence of 4 orders-of-magnitude less and a logarithmic median as our probable outcome (discussed in section 2.6). Assuming this is our worst assurance level, successive assurance levels are produced by reducing the each level one order-of-magnitude (discussed in Section 2.5) to fully develop a Security Assurance Index (SAI). (Note: the numerically ascending assurance levels are of interest to the CSSP; alpha designation indicates risk levels below the interest of the CSSP.)

Table 1. Security Assurance Index – US Centric View - Loss of Life

	range of lost life		
Assurance level	**Low-range**	**median life lost**	**high-range**
SAL 9	3,000,000		
SAL 8	300,000	9,486,833	300,000,000
SAL 7	30,000	948,683	30,000,000
SAL 6	3,000	94,868	3,000,000
SAL 5	300	9,487	300,000
SAL 4	30	949	30,000
SAL 3	3	95	3,000
SAL 2	0.3	9	300
SAL 1	0.03	1	30

SAL A	0.003	0.1	3
SAL B	0.0003	0.01	0.3
SAL C	0.00003	0.001	0.03
SAL D	0.000003	0.0001	0.003
SAL E	0.0000003	0.00001	0.0003
SAL F	0.00000003	0.000001	0.00003
SAL G	0.000000003	0.0000001	0.000003

Likewise, levels of assurance were defined for economic losses. Although these values are specific to the US economic situation, they could be easily modified to the economic losses of other countries. These economic losses were calculated on the economic value of life, injury, asset, consumable, and environment losses, as well as irreplaceable loss of historical, social, and religious sites and artifacts. (Note: although evaluating economic losses can generate much debate [i.e., the value of life], economic losses are an important measure of loss, especially if no life has been lost yet significant damage has occurred.) Using the US centric loss of life table, a similar US centric schedule of economic loss was calculated.

Table 2. Security Assurance Index – US Centric View – Economic Loss

Range of economic loss

assurance level	Low-end	Median economic loss	high-end
SAL 9	**7,125,000,000,000**		
SAL 8	**750,000,000,000**	32,413,538,837,961	**1,400,850,000,000,000**
SAL 7	**75,000,000,000**	3,455,294,849,937	**159,187,500,000,000**
SAL 6	**7,350,000,000**	404,726,991,316	**22,286,250,000,000**
SAL 5	**720,000,000**	49,075,452,112	**3,345,000,000,000**
SAL 4	**33,750,000**	3,735,440,486	**413,437,500,000**
SAL 3	**3,375,000**	626,979,366	**116,475,000,000**
SAL 2	**337,500**	79,962,100	**18,945,000,000**
SAL 1	**33,750**	9,704,389	**2,790,375,000**
SAL A	**3,375**	1,140,197	**385,200,000**
SAL B	**338**	114,020	**48,150,000**
SAL C	**34**	12,748	**4,815,000**
SAL D	**3**	1,275	**481,500**
SAL E	**0.3**	127	**48,150**
SAL F	**0.03**	13	**4,815**
SAL G	**0.003**	1	**482**

2.8 Comments on Using the SAI and Assigning a SAL

Because we use these tables to communicate risk, it is important that we measure and interpret risk in an equal, fair, and consistent approach. Failure to do so would result in a loss of confidence and its adoption.

An important step in communicating risk concerns the design of the evaluation. Any evaluation must be designed according to the number of sites to be evaluated, the potential attack scenarios of each site, and the information available on each site. Our experience suggests that exhaustive and thorough evaluations are not required; rather, inclusive evaluations best serve process, especially when resources are scare. We define inclusive as including those sites that would appear to be most attractive targets and those sites should be most attractive (this assumes perfect information). Once the list of sites have been identified, an evaluation process is developed that can be applied equally; thus, the evaluation must consider information of the lowest common denominator. Lastly, a sufficient set of reasonable yet imaginative attack scenarios must be defined to be applied to this list. In general, although it possible to have hundreds of attack scenarios, it is best to limit this exercise to five or ten worst case scenarios with accompanying range of possible consequences. Note that this evaluation process may have to be modified to account for unexpected outcomes in information gathering and calculated risk outcomes.

Once calculated, this risk value or range in risk values can be assigned a SAL using either Loss of Life or Economic Loss tables. If the median falls within 20% or 30% of the SAL median, this site and scenario can be ranked fairly easily. However, if the calculated median falls equally between the medians of the SALs, one should consider the distribution of risk around the calculated value. Would risk have a tendency to be greater than we calculated? Or would it be less?

Additionally, we also consider both risk measures (Loss of Life and Economic Loss) when assigning the SAL. Because we want to error on the conservative side, we always defer to the scale that assigns a higher SAL. For example, if the our loss of life is expected to be 15 to 20 yet the economic losses are expected to be more than $10B, we would classify this site as a SAL 4 instead of a SAL 2. On the other hand, if our economic losses are anticipated to be no more than $100M yet we could expect 100 deaths, we would classify this site as a SAL 3 instead of SAL 2.

3 A Proposed Scale of World Disaster

So far, we have discussed the development and use of INL's security assurance index. However, using the SAI to evaluate the risk of terrorism outside the US would pose significantly different and unintended results, especially for those countries with smaller populations and incomes such as the Netherlands (15.7M, $389B), Estonia (1.4M, $4.9B), or Bermuda (0.1M, $2.5B). Nonetheless, this issue has not discouraged many risk management professionals to suggest that a similar scale could provide a useful tool in communicating risk of natural and

human initiated disasters and calamities. Thus, this is the final purpose of this last section.

3.1 Purpose for an World Risk Index

Similar to our problem in communicating the risk of control systems, a World Risk Index (WRI) would communicate the issues of risk from pending, probable, and actual disasters.

Ideally, a WRI would communicate the risk faced by all world communities concerning bioterrorism, pandemics, weapons of mass destruction, natural disasters, celestial disasters, and even global warming. Presented in a generic and easy to understand index, we would agree that a WRI would contribute to the communication of many situations of risk facing humanity today.

3.2 The Proposed World Risk Index

Similar to the CSSP's SAI, our proposed WRI would communicate risk. However, the authors have identified two critical issues would have to be resolved for any scale to find international adoption. The first issue is finding and defining a unit of measure acceptable by all societies. Measures of value tend to be very contentious due to differing value systems within each society. The second issue is defining a relevant risk event.

3.2.1 Defining a Relevant Risk Event

One may ask"Why is it important that a risk event be defined?"

A primary concern would be that resources usually follow policy. Assuming a WRI could be defined and assuming it is accepted, a broad interpretation of "risk event" could strain the resources for risk management and mitigation. This may be especially true of those human initiated events associated with continuing struggles and war between nations, peoples, and ideologies. The one-time use of a weapon of mass destruction on a city of non-combatants could be an event that demands international response; whereas, the same weapon associated with continued war may not. Both scenarios are concerned with the risk of a weapon of mass destruction on humanity; however, a WRI might prove to be more divisive.

Our suggestion is any risk event should be defined as a single, definable action, of natural or human influence, that results in negative consequences against the people, communities, or nations of the world. Assuming this definition, the remainder of this paper is devoted to the development of a WRI.

3.2.2 The Proposed Unit of Measure for International Risk

Currently, an SAI evaluation measures risk on two scales: 1) loss of life and 2) economic loss. Although we have found both scales useful in measuring risk reduction in US control systems, it is likely that the risk of economic loss will not fit the context of risk management on a world stage.

Economic loss is contentious simply because there is no common, international measure for economic value. Although we could devise a system of continuous risk evaluations given the change in monetary exchange rates, local economic issues of many countries may not be appreciated on a world stage due to differing value systems. In response, economists have made efforts to define more meaningful economic measures using concepts of purchasing power parity equivalents. However, although it may be an interesting exercise to determine economic loss using a Big Mac[9], this measure would be an unfair representation of social and economic values where Big Macs do not exist.

On the other hand, life and quality of life measures have become universal. Fertility, life expectancy, disease, and death rates measure issues that pervade all societies and ideologies. And although the value of life on earth may be different within societies, the fact is that life is a common unit of measure to all people. Thus, when a natural disaster has a consequence in killing 120,000 people, all people and nations seem to understand this scale of impact with clarity.

In a relatively easy exercise, the US centric view in loss of life has been adjusted to fit a world centric view. (To create a scale of lasting scale measure, we have rounded up the world population to 10B.) Similarly, a WRI would be composed of ten world risk levels (WRL) flexible enough in breadth and scale to adjust to continued world population growth as well as its potential demise. Furthermore, a log value of the median life lost can be calculated to determine a partial and more accurate WRL ranking.

Table 3: World Risk Index – Loss of Lives

	range of lost life		
World Risk Level	**low-range**	**median life lost**	**high-range**
WRL 10	100,000,000	1,000,000,000	10,000,000,000
WRL 9	10,000,000	100,000,000	1,000,000,000
WRL 8	1,000,000	10,000,000	100,000,000
WRL 7	100,000	1,000,000	10,000,000
WRL 6	10,000	100,000	1,000,000
WRL 5	1,000	10,000	100,000
WRL 4	100	1,000	10,000
WRL 3	10	100	1,000
WRL 2	1	10	100
WRL 1	0.1	1	10

Historically, most of the world's most risk events fall within the WRL 3 through WRL 6 levels where 100 to 100,000 people are killed from the natural events of cyclones, tsunamis, earthquakes, and volcanic eruptions. Of more interest would be those events of famines, pandemics, and near-earth objects that

could kill 1M to 100M people. It is a stretch of the imagination to think of human initiated events of this scale; however, a creative imagination in weapons of mass destruction could create these outcomes.

Objections to this proposed WRI would probably come from countries of smaller populations. For example, the risk of 10,000 potential deaths would have a tremendously different impact on Bermuda (pop 65,365, 15.3% loss) versus its impact on the US (pop 300M, a 0.0035% loss). Both losses would impact the country tremendously; however, Bermuda would suffer by 3 or 4 orders-in-magnitude.

To account for the influence of population, the scale could be weighted according to the subject country, region, or state contribution to the world population. Modifying the above scale to a percentage of population lost for a selected country, region, or state, this scale could be applied to a germane geo-political interest:

Table 4: World Risk Index – by % Loss of Population

	range of lost life		
World Risk Level	**low-range**	**% median life lost**	**high-range**
WRL 10	1.00%	31.6%	1000.0%
WRL 9	0.10%	3.2%	100.0%
WRL 8	0.01%	0.32%	10.0%
WRL 7	0.001%	0.032%	1.0%
WRL 6	0.0001%	0.0032%	0.1%
WRL 5	0.00001%	0.00032%	0.01%
WRL 4	0.000001%	0.000032%	0.001%
WRL 3	0.0000001%	0.0000032%	0.0001%
WRL 2	0.00000001%	0.00000032%	0.00001%
WRL 1	0.000000001%	0.000000032%	0.000001%
WRL 0	0.0000000001%	0.0000000032%	0.0000001%

Using this scale, a WRL 8 event would be a loss of 207 lives in Bermuda, 935,250 lives in the US, and 20,385,000 lives worldwide. Interestingly, because current predictions of the potential, world-wide H1N5 avian pandemic range within these consequences, H1N5 could be simply stated as a WRL 8 event. Given that most experts agree that this pandemic will eventually happen (it is only a question of when), this simple ranking provides a sound and easy to communicate basis as to why this pandemic should be of great concern to humanity.

4 Summary, Conclusions, and Recommendations

Generally speaking, most of the existing scales in risk to not communicate calculated risk; rather, they communicate threat thresholds, which in turn, imply potential consequences. The major disadvantage in this communication is that they require people to predict the probability of an event and require the people to calculate the risk given their personal situation. Thus, unless the public is well-informed on many issues of threats, probabilities, and consequences, people tend to understate or overstate risk depending on their concerns and biases. To remediate this problem, a scale must communicate risk as a function of event probability and the probability of consequence.

Based on other successful scales that communicate risk, we developed a Security Assurance Index (SAI) to address risk as a quantitative measure within the DHS Control System Security Program. Other risk management practitioners have suggested that this index could be modified to communicate issues of world risk. To this pursuit, we have presented two scales of World Risk Index (WRI), one based on the number of deaths, and another on the percentage of population killed. At this point in time, the authors prefer a scale based on the percentage of population impacted within a nation, continental region, or common community. Logically, this scale would be used to communicate mitigation and response measures according to the pending or actual consequences of a disaster.

Risk scales have many advantages over threat scales. Primarily, threat scales measure only physical attributes of an event; whereas, risk scales include these physical attributes, probable threats, and probable impacts. Additionally, ranges in consequences are incorporated in the risk evaluation process; thus, the probability of extreme events and outcomes are accounted for and contribute to the final risk ranking. However, the greatest advantage is the simple and clear message in communicating the potential and actual consequence of a disaster by a simple to understand ranking. Thus, an index of probable outcome alerts and communicates to the world communities the potential fate of an event, which in turn, may initiate a more timely and adequate response.

This primary issue in developing any WRI is finding a common measure for risk assessment. Without a doubt, the most common measure for risk is human life; other measures may find acceptance among some communities and not by others. Although this single measure may not capture the consequences of economic loss, environmental stress, and political change, a WRI may provide an initial tool from which the world's communities can find a common ground. From our experience, a good communication tool initiates a process and a standard from which the risk of potential disasters can be effectively managed. Although any scale may be imperfect, it is easy to argue that some communication is better than no communication, and hopefully, these efforts may be just enough to make a difference and change the outcome for the better.

References

[1] Bahr, N. J., 1997, *System Safety Engineering and Risk Assessment: A Practical Approach*, ISBN 1-56032-416-3, Taylor and Francis, Philadelphia, PA.

[2] http://www.dhs.gov/interweb/assetlibrary/CitizenGuidanceHSAS2.pdf

[3] http://en.wikipedia.org/wiki/Scale#Measuring_system

[4] "Techniques for Assigning A Target Safety Integrity Level", Angela E. Summers, Ph.D. originally published in ISA Transactions 37 (1998) 95-104.

[5] http://en.wikipedia.org/wiki/Famine_scale

[6] Famine Intensity and Magnitude Scales: A Proposal for an Instrumental Definition of Famine, (PDF) Howe, P. and S. Devereux, *Disasters*, 2004

[7] Fechner, G.T. (1861/1966). *Elements of Psychophysics* (Translated by H.E. Adler), Holt, Rinehart, and Winston, New York

[8] http://www.insurancenetworking.com/protected/article.cfm?articleId=3587&pb=ros

[9] http://www.economist.com/markets/bigmac/displayStory.cfm?story_id=5389856