**Threat Capability and Resistance Strength: A Weight on a Rope**

*Threat Capability and Resistance Strength in the FAIR taxonomy are among the more abstract and difficult concepts to get a firm grasp on. The standard seeks to fix ideas with the analogy of a weight on a rope. This note models that analogy in detail and uses it to explore these concepts.*

The FAIR taxonomy [1] uses the term “vulnerability” in a special way that differs significantly from how it is used by CERT and many network and software scanners. “Vulnerability” in FAIR is “the probability that a threat event will become a loss event.” The usual meaning of “vulnerability” in information security is a flaw or suboptimal configuration in software or hardware. The taxonomy breaks Vulnerability into two component drivers, Threat Capability and Resistance Strength. (I’ll use initial capitals to make it clear where FAIR-defined words are meant. I’ll also use the standard abbreviations Vuln, TCap, and RS.) Note that since Vulnerability is a probability, it is a number between 0 and 1, or 0% and 100%.

Threat Capability is defined as “the probable level of force that a threat agent is capable of applying against an asset,” leaving it to analyst to identify what kind of “force” is to be considered for the scenario at hand, and how to quantify it. “Probable level” is a hint that TCap is a probability distribution, though it could be a single number in a simple case. Resistance Strength is defined as “the strength of a control as compared to a baseline unit of force.” The accompanying discussion in the standard emphasizes that RS is to be measured on the same scale as TCap, which is helpful to the extent that one understands force for the TCap. To help fix ideas for all three concepts, the standard offers the example of a weight (the Threat Agent) on a rope (which is a control that protects an asset – maybe your toes beneath the weight). The force is gravity, the measure of force is pounds-force or Newtons, and the Resistance Strength is the tensile strength of the rope, and so it too is measured in pounds or Newtons. The Vulnerability is then the probability that a specific weight, or population of possible weights, will exceed the tensile strength of the rope.

Let us model this scenario to see if it can help us understand these three ideas better. First we define the scenario.

**Scenario Description**

Purpose: To assess the risk posed by weights on a construction site being hoisted over a partially-completed building.

Assets: A building under construction, materials and equipment on the site, life safety of the workers.

Threats: Heavy construction materials, such as steel beams and loads of wet concrete to be hoisted.

Threat Event: A load being hoisted over the building or the site.

Loss Types: Structural integrity of the building, availability of the building on the site for further work, availability of the building for delivery to the owner on the contracted date (using the C-I-A loss categories).

Risk Scenario: A construction load being hoisted into position breaks its rope (Threat Event) and crashes into the building or the site, damaging the building, materials, and equipment, and causing injury or loss of life (Loss Event).

Threat Community: The set of loads planned to be hoisted, ranging from a very light load to 35 kiloNewtons (7875 pounds of force to us Yanks), with an uncertainty of +/- 5 kN (one standard deviation).

Threat Agent: The specific member of the Threat Community we’ll start with is the maximum weight of 35 kN +/- 5 kN.

Control: a steel rope with a specified tensile strength of 40 kN (9675 pounds), with an uncertainty of +/- 3 kN (one standard deviation). We’ll assume the specification is one standard deviation lower than the mean breaking strength of 43 kN.

**Analysis**

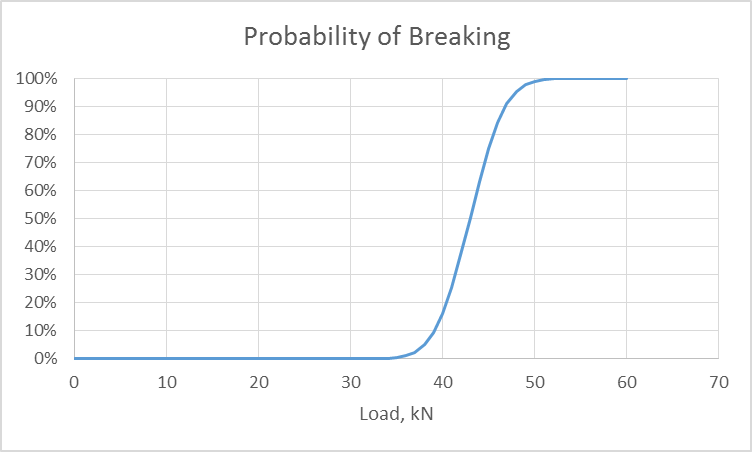
The problem is to determine how likely it is that the load exceeds the strength of the rope, or in FAIR terms the probability that a Threat Event becomes a Loss Event. That is precisely the FAIR Vulnerability. In any given hoisting operation, we have a load of uncertain weight imposing a force on a rope of uncertain tensile strength. If the load exceeds the rope strength, the rope breaks and we have a Loss Event. We need to determine how likely it is (the probability) that the uncertain load will exceed the uncertain tensile strength.

Like a B-minus sociology student, we shall naively assume that all probability distributions are normal (Gaussian), and casually ignore the infinitesimal probabilities of negative weights and negative tensile strengths. Given that, here is the probability distribution of the biggest planned load (Threat Agent).



The density function peaks at 35 kN, which is also the 50% point on the cumulative distribution, as it should.

The tensile strength has a similar probability distribution, but I find it more natural to think of it in terms of its cumulative distribution – that is, what is the probability of breaking at or below any given load – rather than its density function. Here it is:



Notice that the cumulative curve is a similar shape to the one for the load but shifted a bit to the right (we should hope that the strength is at least a bit greater than the load).

Here is what we do to figure the Vulnerability. (Plus one point if you smell a Monte Carlo simulation coming.)

**Procedure**

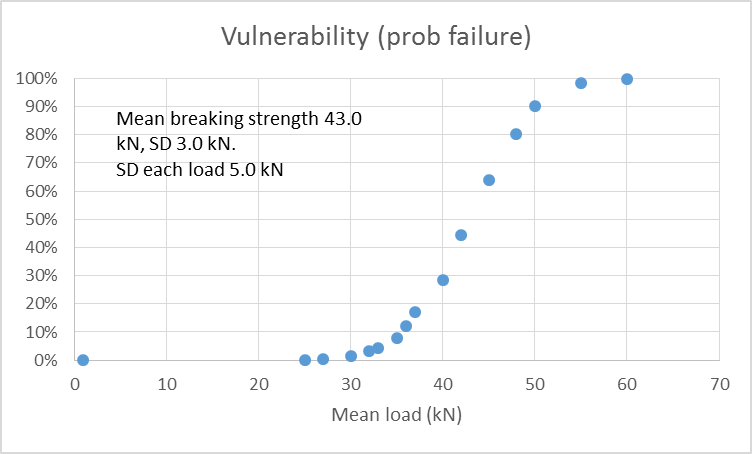
1. Generate a random variable according to the density function of the load (normal, mean 35 kN, standard deviation 5 kN).
2. For each realization of the load random variable, look up the probability of the rope breaking, and record it. For 40 kN, it is 0.16.
3. Do this a bunch of times, say 1000.
4. Average the thousand probabilities you got in step 2.

The answer is a single number, the probability of the rope breaking, averaged over the probable load weights for the given load (Threat Agent) and rope strengths. This is the Vulnerability, the probability for this load size (Threat Agent) that a Threat Event becomes a Loss Event. The number I got was 0.079. (There will be some run-to-run variation in a MC simulation.)

(Another procedure is to generate two random variables, one for load and one for strength. You record a 1 if load is greater than the strength and 0 otherwise. The average of the 1’s and 0’s is the answer. This is the method Jack Jones uses in his video on the CXOWARE web site. It gives the same answer but I find the procedure above easier to understand. It can be shown that the two procedures are equivalent.)

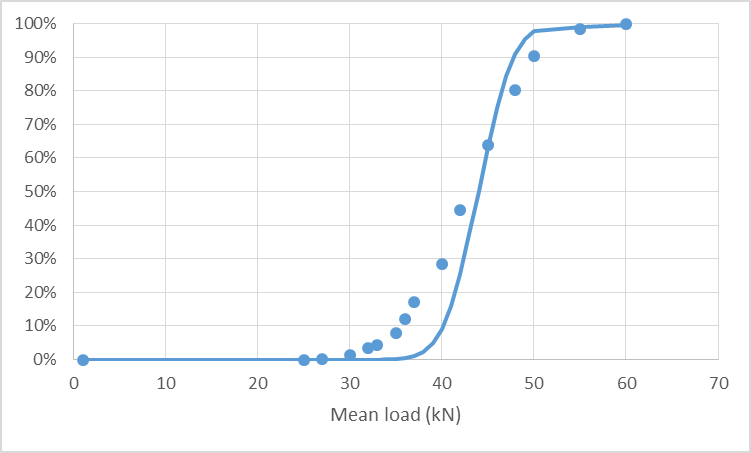
**Vulnerability for Various Threat Agents**

We could repeat the analysis for a whole range of loads we see lying around in the construction site. In FAIR words, there are other Threat Actors in the Threat Community, and they have different Threat Capabilities. After putting away my steel-toed work boots, I did that. Here’s what I got. Each dot represents the probability of breaking for a load whose mean size is shown on the x axis. The standard deviations of all the loads is 5.0 kN.



We see that the probability of failure (Threat Event becomes a Loss Event) increases with the load (that’s reassuring) and gets pretty high as we approach the specified tensile strength of the rope of 40 kN (that is too).

This set of points looks an awful lot like the curve for the rope, but it’s not the same. Here are both sets of data plotted on the same chart.



For small loads (TAs), the probability of the rope breaking is greater than the probability of the rope breaking for the average of the load. Why? Because a load of say 35 kN average has some probability of being more than 35 kN, which has a bigger break probability. The opposite is true for large average loads, above about 45 kN. The curve for the dots is flatter than the curve for the rope because it includes the uncertainty in Vuln of the sizes of the loads as well as the uncertainty in the rope strength.

**Vulnerability for the Threat Community**

Each dot in the previous chart represents a specific member of the Threat Community, a specific Threat Agent. In our scenario, it is a load or group of loads with a certain average weight and a certain standard deviation. The dot is the Vulnerability for that load size (TA).

Now suppose we want to generalize to the whole Threat Community. After all, the job is to finish the building, not just to hoist one kind of load. In surveying the job we might see that there or a 50 or 100 kinds of small loads, and only a few of the very largest loads. In that case we would do this:

Take a census of loads to be hoisted. This is the Threat Community.

Classify them into a reasonable number of relatively homogeneous subsets. Each is a Threat Agent. Estimate their means and standard deviations. Count the number in each subset.

For each TA, do the MC simulation like we did above for the 35 kN load, and so get the probability of failure (Vulnerability, conditional for that particular TA).

Compute the weighted sum of these conditional Vulnerabilities. The weights are relative frequencies of occurrence of the various TAs (subsets). Each hoisting job counts as one.

The weighted sum is the Vulnerability for the entire Threat Community. It is just a number, like 0.01 or 0.50 or 0.97. Unlike Threat Event Frequency or Annual Loss Expectancy itself, it is not a distribution.

What do you expect to find? You expect that the Vulnerability to the entire TC is less than the worst-case TA. This may be confusing. As risk managers, what should we plan for, the entire TC (which gives us a happier number) or the worst-case TA? Well, that depends on your scenario. Obviously if your scenario is a mix of TAs you expect to encounter, the Vuln is going to be lower than for the worst-case TA. You think, in your risk-averse mind, “Gosh, I need to plan for the worst case.” But now is the time to think carefully (well, again, not for the first time!). This is the root of disagreements about whether risk should be assessed based on the worst case or the whole range of expected possibilities. (Another problem with “worst case” is that it is usually ill-defined, if defined at all. There is practically no limit how bad a worst case can be. Leaving it to the analyst will lead to uncontrolled biases, inability to compare results, and lack of reproducibility.)

Yes, you need to be aware of, and understand the consequences of, the (plausible) worst case. But that is not an accurate description of your expected overall experience. Yes, the worst-case could happen, and sooner or later it will happen, and it needs to be accounted for in the analysis, but it is a mistake to over-weight it.

How do we properly weight the worst case with all of the non-worst cases? The answer is with Threat Event Frequency. If the scenario is the worst-case TA, then the TEF is presumably lower than if the scenario is for the entire Threat Community. If the scenario is for the entire Threat Community, not just the worst-case TA, then the worst-case TA will be in there, with its appropriate weight, along with all the lesser TAs in the TC. In the end, when you roll the results up to the Annual Loss Expectancy, the worst-case TA will be in there, appropriately weighted. In other words, Yeah, it could happen, but not that often.

Which scenario to choose for analysis depends on what you need to know for making decisions. In the case of our construction site, it may well be that the scenario that management needs to understand is the worst plausible TA (who cares about the lesser ones?). In another situation, maybe it is a broader Threat Community. What you get depends on what you want, all of which goes to show how critical it is to define the scenario carefully, and get agreement it is the right one.

**Safety Factors**

Nobody in his (or her) right mind would, I hope, even consider hosting a 40 kN load on a 43 kN rope, or even a much smaller load. In fact I am sure there are workplace safety regulations about that.

Now suppose you are a regulator whose job it is to place a limit on the permissible load for a certain-size rope. Limits are commonly stated as the safety factor, the ratio of the rope strength (e.g.) to the permissible load (RS to TCap in FAIR terms). How do you do that? One way is to use the method described above as a first step to quantify the probability of failure. You would need reams of data on material testing. But it’s only an initial step because setting final rules will of course be as much a values-driven and political process as a technical one. Nevertheless it is interesting to think how such things can be done, and what kind of logic underlies safety factors of 1.5, 2, or more.

What would it mean to our industry if a safety factor (RS/TCap) of 1.5 or 2 were required by regulation?

**Further Questions**

If the analysis of the rope example aids your understanding of TCap and RS in cyber risk, it nevertheless raises some other questions. How can we understand “force” in cyber risk? What exactly are TCap and RS? And what exactly is the Threat Community, on which the whole analysis hinges? I’ll address some of these questions in future notes.

However, if nothing else is clear, I hope you believe now that FAIR is applicable much more broadly than only to information risk. In fact it can be applied to any risk scenario whose losses can be quantified in a single number, commonly dollars. Multi-dimensional risk is a whole different beast.

**References:**

[1] The Open Group, *Risk Taxonomy (O-RT),* version 2.0, document number C13K

New 5-4-15, rev 5-5, 5-11