Abstract

Malicious acts aimed directly against humans, or indirectly at their critical infrastructures, is a real and present danger. However, how does society quantify danger levels? And is danger different from risk? Classic risk assessments require probability assessments, a highly speculative task for rare events. A “Danger Index”, proposed by Randall Larsen in a recent book, is investigated here. In this exploratory research paper, this metric is examined in the context of current views of risk, and investigates its potential application to telecommunication settings. The danger index is deemed to have potential for assessing critical telecommunication infrastructure protection, avoiding difficult, and often impractical, probability assessments.

1. Introduction

Malicious acts aimed directly against humans, or indirectly at societies critical infrastructures, is a real and present danger. In spite of this however, most compromises to telecommunication critical infrastructure are often accidental and non-malicious [1]. How can we quantify the danger? Not easily. According to the Mitre Corporation, risk is defined by the following:

“Risk is a measure of a project's inability to achieve system life cycle objectives. It comprises two components: the probability of failing to achieve particular system life cycle objectives, and the consequences of failing to achieve those objectives.” [2]

So risk can be defined by:

\[ Risk = Likelihood \times Severity \]

If likelihood is a probability and severity is in dollars, the result is risk in dollars. Risk assessments requiring likelihood, or probabilities, have little utility for rare events. Why? We cannot rationally assess probability. Such probabilistic analysis attempts may also diminish focus of the root cause of potential outages, and may detract from remediation. In the 9-11 telecommunication outage case, the issue was one of “over-concentration” or creation of a large mega-single-point-of-failure (M-SPF). Guessing at the chance of untoward events that jeopardize this overconcentration of assets is a guessing game, while methods to reduce risk deal with asset distribution.

2. Case in point: 9-11 telecom outages

A large telecommunications outage resulted from the collapse of the world trade centers. Collateral damage from the building collapses also damaged critical water utility infrastructure that in turn resulted in the following:

- Over 4,000,000 data circuits disrupted
- Over 400,000 local switch lines out

Pathology of the event:

- Towers collapsed
- Some physical damage to adjacent TCOM building
- Water pipes burst, and in turn disrupted telecommunication facility power and power backup facilities

What was the a priori probability of such an event and ensuing sequence?

\[ P = Pr\{Successful \, hijack\} \times Pr\{Building \, Collapse\} \times Pr\{Water \, Damage\} \]

Infinitesimal perhaps? Such infinitesimal probabilities might lead operators to ignore or minimize remediation efforts. Clearly, in hindsight, placing all
these telecommunication assets in a single building was dangerous. An alternative definition of risk that helps address the intractable nature of assessing probabilities is given by:

\[
Risk = \text{Threat} \times \text{Vulnerability} \times \text{Severity}
\]

Here, probability is defined as the product of threat and vulnerability. However, although systems may be assessed for vulnerability, how does one assess threat to telecommunications infrastructure? Scholars are not happy with this definition either:

“The literature of risk analysis is replete with misleading definitions….Of particular concern is the definition of risk as the multiplication of impact, vulnerability, and threat.” [3]

With this as background, we examine the danger index, proposed in 2007.

3. Danger index

Larsen’s danger index [4] involves four variables: intention, capability, vulnerability, and consequence. He further proposes that danger can be measured by a multiplicative score:

\[
\text{Danger} = \text{Intention} \times \text{Capability} \times \text{Vulnerability} \times \text{Consequence}
\]

As each variable has a range of [0, 10], the danger index has a range of [0, 10,000]. For a comparison of this index to the classical definition of risk, see Figure 1. Here we find that danger is equivalent to both definitions of risk, introduced in Sections 1 and 2.

\[
\text{Risk} = \text{Likelihood} \times \text{Severity}
\]

\[
\text{Risk} = (\text{Intention} \times \text{Capability} \times \text{Vulnerability}) \times \text{Consequence}
\]

\[
\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Severity}
\]

\[
\text{Danger} = \text{Risk}
\]

Figure 1. Comparison of Danger and Risk

4. Danger index and telecom infrastructure

In a telecommunication infrastructure setting, the four variables of the danger index are presented, and some considerations for assessing each are presented.

Consequence

- Size of outage
- Duration of outage
- Economic impact

Vulnerability

- Weakness or a state of susceptibility which opens up the infrastructure to a possible outage due to attack or circumstance
- Adherence to design, operations, and maintenance best practices

Intention

- Benign intention (installation, operations and maintenance)
- Malicious intention (intentional, high value of target)

Capability

- Skill of exploiting or triggering personnel (could be detrimental in two situations -- low skill for benign intention and high skill for malicious intention)
- Knowledge of vulnerability
- Tools, devices to exploit or trigger vulnerability into a disruptive event

To be of use, the danger index should be able to be applied to such telecommunication infrastructure settings as:

- Wireless 2G+/3G Base Station
- Central Offices
- Cable Head End
- Fiber optic transmission systems

In the next section, the danger index will be applied to central office, wireless, and fiber transmission systems.

5. Examples of danger index applied to telecom infrastructure

One aspect of vulnerability is concentration of infrastructure assets. An example of concentration is shown in Figure 2, where distributed and concentrated PSTN topologies are shown for the same architectural infrastructure. The principle motivation of concentration is economy of scale – less facilities and ease of maintenance means savings and quick recovery from small failures. However, larger events
which threaten the concentration decision are difficult to assess, such as threats due to:

![Distributed Topology vs. Switches Concentrated](image)

Figure 2. Distributed vs. concentrated telecom assets

For the following danger index assessments, the authors graded each dimension and arrived at a consensus. First, the consequence of a catastrophic event to the concentrated central offices is much greater than the distributed case. Additionally, the intent for a malicious act is increased for the centralized case. This is reflected by a higher danger index for the concentrated case (22.7% versus 6.3%), as seen in Tables 1 and 2.

Wireless infrastructures consist of mobile switching centers, base station controllers, base stations, databases, and transmission facilities, as seen in Figure 3 and Table 3. We assessed the danger index of a hypothetical base station. With 2000 customers affected, the consequence is small. However the intention is appreciable because of opportunity for vandalism. The vulnerability and capability for damage are large, leading to a danger index of 3.0%.

A SONET fault tolerant ring serves many users, so the consequence of failure is very high. However its vulnerability is low because of the fault tolerant nature of the ring architecture. The vulnerability of a fault tolerant ring is depicted in Figure 4 and Table 4. The intention might be moderate, but the ring is hard to find, consequently capability is low. This results in a danger index of 1.4%.

These are but a few examples of how the danger index can be applied to telecommunication system architecture. Ostensibly, a service provider would conduct many such assessments. The assessments can then be rank ordered by danger index to help in risk management decisions.

### Table 1. Danger index for distributed architecture

<table>
<thead>
<tr>
<th>Distributed COs</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence</td>
<td>5</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>6</td>
</tr>
<tr>
<td>Intention</td>
<td>3</td>
</tr>
<tr>
<td>Capability</td>
<td>7</td>
</tr>
<tr>
<td>Danger Index</td>
<td>630</td>
</tr>
</tbody>
</table>

### Table 2. Danger index for concentrated architecture

<table>
<thead>
<tr>
<th>Concentrated COs</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence</td>
<td>9</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>6</td>
</tr>
<tr>
<td>Intention</td>
<td>6</td>
</tr>
<tr>
<td>Capability</td>
<td>7</td>
</tr>
<tr>
<td>Danger Index</td>
<td>2268</td>
</tr>
</tbody>
</table>
Table 3. Danger index for a base station

<table>
<thead>
<tr>
<th>Base Station #118</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence</td>
<td>1</td>
</tr>
<tr>
<td>2,000 users impacted</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>10</td>
</tr>
<tr>
<td>Tower highly visible with fence around small footprint</td>
<td></td>
</tr>
<tr>
<td>Intention</td>
<td>3</td>
</tr>
<tr>
<td>Value of target low to terrorist, but susceptible to vandals</td>
<td></td>
</tr>
<tr>
<td>Capability</td>
<td>10</td>
</tr>
<tr>
<td>Firearm or quick entry possible</td>
<td></td>
</tr>
<tr>
<td>Danger Index</td>
<td>300</td>
</tr>
<tr>
<td>3.0% normalized to 100%</td>
<td></td>
</tr>
</tbody>
</table>

Table 4. Danger index for a SONET ring

<table>
<thead>
<tr>
<th>SONET Ring 32</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence</td>
<td>9</td>
</tr>
<tr>
<td>270,000</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>2</td>
</tr>
<tr>
<td>Fault tolerant ring. Outage requires (1) two fiber cuts, (2) one fiber cut and node failure, or (3) two node failures . Requires good O&amp;M to replace/repair if ring goes to protect mode</td>
<td></td>
</tr>
<tr>
<td>Intention</td>
<td>4</td>
</tr>
<tr>
<td>Value of target moderate to high for terrorists, vandals or thief’s might mistake for copper</td>
<td></td>
</tr>
<tr>
<td>Capability</td>
<td>2</td>
</tr>
<tr>
<td>Hard to locate fiber, nodes in buildings</td>
<td></td>
</tr>
<tr>
<td>Danger Index</td>
<td>144</td>
</tr>
<tr>
<td>1.4% normalized to 100%</td>
<td></td>
</tr>
</tbody>
</table>

6. Conclusions

The application of the danger index is highly situational, facility by facility. Considerations include engineering, installation, operations, and maintenance. It also must include knowledge regarding security (physical, logical layers, etc). Additionally, the degree of adherence to best practices, such as NRIC1 [5] for Cable, Internet, Wireline, Wireless, and Satellite telecommunication infrastructures is paramount in understanding vulnerabilities.

Additionally, any organization applying risk or danger assessments need rules and consistency in assigning [1, 10] scores in each of the four danger index dimensions. A normalized danger index looks feasible, practical and useful for TCOM risk assessments, as it avoids guesses at probabilities.

7. References


1 National Reliability and Interoperability Council, a U.S. Federal Advisory body commissioned by the Federal Communications Commission.
