A Bayesian Network Analysis of System Failure in the Presence of Low-Probability External Correlating Events

Jack K. Horner
P.O. Box 266
Los Alamos NM 87544 USA
email: jhorner@cybermesa.com

Abstract

Using a simple Bayesian network model of the electrical power backup for the Fukushima Daiichi reactor control systems as an example, I show that systems with multiple independent backup modes (MIBMs) can be disastrously sensitive to seemingly low-probability external events, even when the intrinsic joint failure rate of the backup subsystems is practically zero. This counterintuitive behavior frames a design rubric which I call the "External Correlator Test" (ECT): a determination of the acceptability of the cumulative probability of system failure in the presence of an external correlating distribution.

Keywords: autonomous systems, Fukushima, power-law distribution

1.0 Introduction

On 11 March 2011, a magnitude 9 earthquake generated tsunami waves that struck the Fukushima-Daiichi nuclear facility on the east coast of Japan. At least one of these waves was estimated to be 14 meters high and overwhelmed the Fukushima defenses, which were only designed to withstand waves of a maximum 5.7 meters high. Electrical power to the reactor controls, including electricity from all emergency electrical backup systems at the site, ceased. The resulting facility blackout caused the loss of all instrumentation and control systems in Reactors 1-4. Loss of coolant was followed the release of radiation into the surrounding area. A region with a radius of approximately 30 miles, centered on the complex, is now uninhabitable ([5]).

Fukushima reactor control was largely autonomous. By convention, autonomous systems are expected to respond in desirable ways to all external stimuli; they often manage pathological events through multiple independent backup modes (MIBMs). Catastrophic failures in systems that contain MIBMs would seem to have very low probabilities, yet occur with unexpectedly high frequency. How can we understand this sensitivity of such system failures to low-probability disaster scenarios, and what can be done during system development to help mitigate their occurrence?

Significant aspects of risk management can be modeled as a "betting" regime ([7]). Any rational betting regime must at least be consistent with probability theory ([7]). Any probabilistic system can be modeled as a Bayesian network (BN; [2],[8]). A BN is a system of conditional probabilities ([3], p. 23) mapped onto a

directed graph ([4]) of system entities. BNs are widely used in decision-assistance systems, including

- health-allied diagnosis
- automotive Built-In-Test
- spam filters
- intelligence analysis

2.0 Method

I first model the Fukushima-Daiichi electrical power backup systems with BNs, then abstract a criterion of design adequacy from that example.

3.0 Results

3.1 A closer look at Fukushima Daiichi

The Fukushima Daiichi nuclear power complex contained six General Electric (GE) Mark I boiling water reactors (BWRs). The Mark I has been extensively tested and ~30 are in use around the world ([16]).

Power to the reactor controls is normally generated within the site. The site has three independent electrical power backup sources: an external commercial electrical supply, diesel-powered generators, and batteries. The reactor controls fail if all three electrical sources fail.

None of these three backup systems depends on any other. Each of the backup systems has a nominal intrinsic probability of failure of $\sim 5 \cdot 10^{-4}$ per year, given preventive maintenance. Thus, by the law of independent events, the probability of all three failing from intrinsic events is $(5 \cdot 10^{-4})^3 = \sim 10^{-10}$ per year -- for all practical purposes, "zero".

Figures 1 and 2 depict BNs showing the essentials of the backup electrical power system for reactor controls in the Fukushima Daiichi complex. The models include representations of

- some failure modes of the system
- sources which could supply electrical power to the reactor controls
- reactor control
- probabilistic ("quasi-causal", [6]) relations among the above

Figure 1 is a "naïve", and Figure 2, a "tsunami-augmented", model of that system. The models are implemented in the *Netica* ([1]) BN development and runtime framework.

In Figures 1 and 2

- boxes represent system entities of interest
- upper portion of a box indicates the name of the entity
- lower portion of a box identifies the probability, expressed as a percentage, that the entity is in the named state
- an arrow from Box A to Box B means the probability of the states of entity B depends on the states of entity A
- prior probabilities ([9], Section 1.3) of the system entities are defined in tables (not shown)

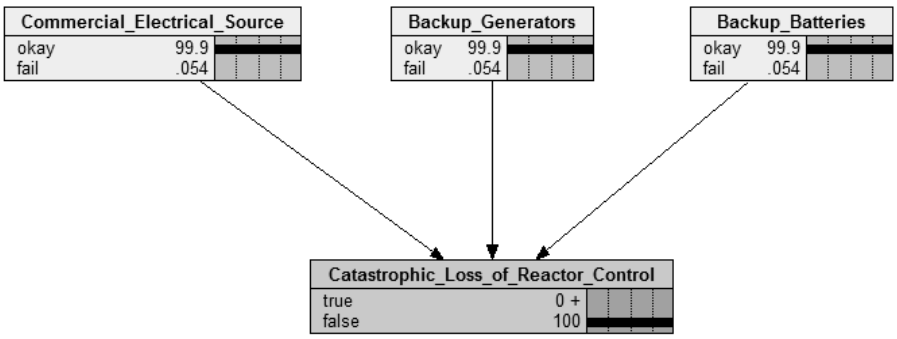

Figure 1. "Naïve" model. In this model, there is no correlation of the failures of the electrical sources; each source has an intrinsic failure probability of 0.054%. The probability of catastrophic loss of control is therefore $(5.4 \times 10^{-4})^3 = \sim 10^{-10}$ per year, which may be acceptable.

Figure 2, the "tsunami-elaborated" model, is Figure 1, plus a tsunami probability explicitly modeled as a Pareto (power-law; [3], p. 193) probability density function (pdf)

$$P(h) = (a/b)(b/h)^{a+1} \qquad \text{Eq. 1}$$

where

P(h) is the probability of a tsunami of height h (in meters), per year

a is a distribution "shape" parameter, here set to 1.0

b is a distribution "location" parameter, here set to 0.01

Eq. 1, with parameters set as noted, is a reasonable fit to tsunami occurrences on the Japanese east coast ([10]).

The probability of reactor control failure, given a tsunami with height > 6 meters, can be determined by evaluating the joint *cumulative* distribution function (cdf) corresponding to Eq. 1 and the MIBMs, for h > 6 meters.

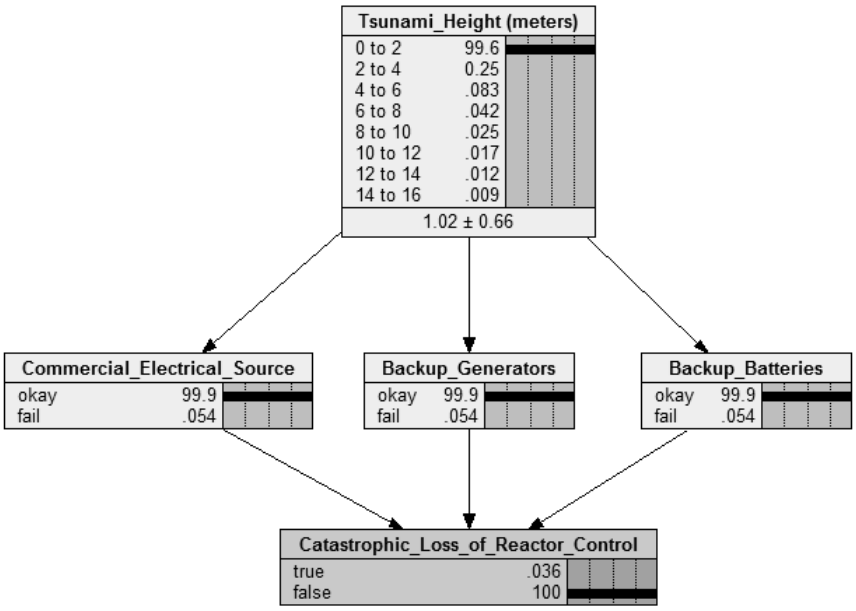

Figure 2. "Tsunami-augmented" model. The"naïve" model, extended with a (Pareto) tsunami-height distribution, forces correlation of the failure of all three electrical sources. The prior probabilities of the "okay/fail" distribution of the electrical source nodes are defined to be the *same* in the naïve and tsunami-elaborated models. The resulting system probability of catastrophic failure is ~10^{-4} per year, a 6-order-of-magnitude increase over that probability in the naive model, which may be unacceptable. The bottom of the "tsunami box" shows the mean ± one standard deviation of the tsunami distribution.

Once the seawall has been topped, the probability that the electrical backup power sources will fail rises sharply. In the model shown in Figure 2, the backup systems were assumed to have a relatively high probability of surviving a 6-meter tsunami, but a very low probability of surviving a 15-meter tsunami (see Figure 3).

Prob(individual backup system failure)	Tsunami_Height
1.1e-5	0 to 2
1e-5	2 to 4
1e-5	4 to 6
0.1	6 to 8
0.5	8 to 10

0.9	10 to 12
0.99	12 to 14
0.99999	14 to 16

Figure 3. Probability of individual backup system failure as a function of tsunami height assumed in the model shown in Figure 2.

The probability of system failure of the system shown is ~0.0001 per year, sometimes interpreted as "a 1000-year event " (i.e., a 10% chance of failing in 1000 years). A backup system that would fail only once per 1000 years would seem robust enough. The reactor control failure probability in the presence of this tsunami distribution is *10^6 times greater*, however, than the probability of reactor control failure in the absence of the tsunami distribution. The cdf of what seem to be extremely rare events, therefore, can hugely amplify the probability of system failure, even though the probability of individual scenarios in the associated pdf is acceptably small.

Worse is true. Given the model described above, in 50 years of reactor operation -- the nominal design lifetime -- the probability of system failure at Fukushima Daiichi due to a 6+ meter tsunami is ~0.05. It is likely that most people would regard that probability as unacceptably high.

For comparison, as of August 2011, there had been ~10^{-3} radiation-releasing accidents per reactor-year in the nuclear power industry worldwide ([19]). The observed incidence of radiation-releasing accidents at sites with GE Mark I BWRs, excluding Fukushima Daiichi, is ~10^{-5} per reactor-year ([19]). The probability of system failure at Fukushima Daiichi due to tsunamis is therefore ~100 times the empirically expected system failure rate for sites with GE Mark I BWRs, excluding Fukushima Daiichi,.

3.2 A criterion of design adequacy

The models illustrated in Figures 1 and 2 are easily adapted to other systems that have MIBMs subject to external correlating distributions. Bayesian analyses similar to those of Section 3.1 have been applied to other systems with similar backup systems (e.g., the Space Shuttle ([12]), unmanned aerial vehicles (UAVs) operated in the absence of routine preventive maintenance ([13]), the Three Mile Island Accident ([18]), global threats to amphibians ([20]), and the proposed Keystone Pipeline ([11],[17])), with similar results.

What lessons can be learned from such examples?

First, an event, E, external to a system, S that has MIBMs can force a correlation of the failures of S's MIBMs. Second, the probability of system failure is determined by the joint *cdf* for E and the MIBMs. This cdf can induce a system failure probability that is several orders of magnitude larger than the probability of individual events in E's pdf. These considerations frame a criterion of design adequacy, which I call the External Correlator Test (ECT):

(ECT) Let S be a system with MIBMs and E be an external correlating distribution for S. The design of S is robust only if the system failure probability for S is acceptable, given the joint cdf of E and the MIBMs.

4.0 Discussion and conclusions

The considerations of the preceding sections motivate several observations:

1. In general, enumerating all possible, or even the most likely, candidate external correlating distributions for a given system S is not a mechanical task, and which candidates should be considered will depend on the nature of S and on cost/benefit trades. However, there are several commonly occurring categories of external correlating events worth considering by default, including

a. natural disasters (e.g., hurricanes, tornados, floods, earthquakes, fire, solar flares, and tsunamis)
b. vibration
c. strong electromagnetic fields
d. temperature and humidity extremes
e. dust
f. accidental vehicle crashes
g. sabotage
h. control (e.g., of utilities, especially of electrical power) delivered through the Internet
i. whether robust systems engineering processes ([15]), including human factors considerations, were used during development and operation

2. The effects on system failure probability of *power-law* external correlating distributions are particularly susceptible to underestimation because the values of the *pdf* for *individual* backup-failure events often seem too small to matter -- the probability of a 15-meter tsunami, for example, is miniscule. But value of the cdf -- the integral (or in the case of a discrete distribution, the sum) of the pdf -- over the entire range of backup-failure scenarios can amplify system failure probability by several orders of magnitude, compared to the effect on system probability failure of individual events in the pdf of the external correlating distribution. Many natural disasters are power-law distributed ([14]), and thus their effects on system failure are easily underestimated.

3. As part of system design review (SDR, [15]), system safety design should be analyzed for system-failure-amplifying correlations of low-probability states/scenarios, in accordance with the ECT. BNs can cost-effectively support this kind of analysis.

5.0 Acknowledgements

This work benefited from discussions with Tony Pawlicki. For any problems that remain, I am solely responsible.

6.0 References.

[1] Norsys Software Corporation. *Netica* v4.16. http://www.norsys.com. 2011.
[2] Pearl J. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Revised Second Printing. Morgan Kaufmann. 1991.
[3] Hogg RV, McKean JW, and Craig AT. *Introduction to Mathematical Statistics.* Sixth Edition. Prentice Hall. 2005.
[4] Diestel R. *Graph Theory*. Springer. 1997.
[5] International Atomic Energy Agency. *IAEA International Fact Finding Expert Mission of the Nuclear Accident Following the Great East Japan Earthquake and Tsunami. Preliminary Summary*. http://www.iaea.org/newscenter/focus/fukushima/missionsummary010611.pdf. 1 June 2011.
[6] Pearl J. *Causality: Models, Reasoning, and Inference.* Second Edition. Cambridge. 2009.
[7] Kemeny JG. Fair bets and degree of confirmation. *The Journal of Symbolic Logic* XX (1955), 263-273.
[8] Jensen FV. *Bayesian Networks and Decision Graphs*. Springer. 2001.
[9] Sivia DS. *Data Analysis: A Bayesian Tutorial*. Oxford. 1996.
[10] University of Southern California. The Tsunami Research Center. http://www.tsunamiresearchcenter.com/.
[11] Horner JK. A Bayesian network assessment of earthquake risk to the Keystone Pipeline. Unpublished manuscript. 2011.

[12] Columbia Accident Investigation Board. Final Report. http://caib.nasa.gov/. 2003.
[13] Science Applications International Corporation. Global Hawk/Reaper Advanced Diagnostic Expert System Demo. Power Point briefing. 16 August 2007.
[14] Bak P. *How Nature Works*. Springer. 1996.
[15] International Standards Organization. *Reference Standard ISO/IEC 15288. Systems and software engineering —System life cycle processes.* Second edition. 1 February 2008.
[16] General Electric. *The Mark I Containment System in BWR Reactors*. http://www.gereports.com/the-mark-i-containment-system-in-bwr-reactors/. 2011.
[17] US Department of State. Keystone Pipeline Project. Final Environmental Impact Statement. Project Description. Section 2.2. http://www.keystonepipeline-xl.state.gov/clientsite/keystonexl.nsf/05_KXL_FEIS_Sec_2.0_Project_Description.pdf?OpenFileResource.
[18] The President's Commission on the The Accident at Three Mile Island. *Final Report of The President's Commission on The Accident at Three Mile Island.* 30 October 1979. http://www.pddoc.com/tmi2/kemeny/.
[19] European Nuclear Society. Nuclear power plants, worldwide. http://www.euronuclear.org/info/encyclopedia/n/nuclear-power-plant-world-wide.htm.
[20] Horner JK. A Bayesian network model of global threats to amphibians. Submitted to the *2012 International Conference on Bioinformatics and Computational Biology*.