BASTION TECHNOLOGIES

Two Is One, One Is None: A Discussion on Redundancy

RAMS XIII
Huntsville, AL
November 30th/December 1st, 2021

Marion Whatley, Bastion Technologies Inc.

Objective

BASTION TECHNOLOGIES

"Goldilocks" situations of redundancy:

- Too Little – Single points of failure.
- Too Much – More doesn't mean better.
- Just Right – The "Best" amount of redundancy

Concepts

BASTION TECHNOLOGIES

- In engineering, redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or fail-safe.

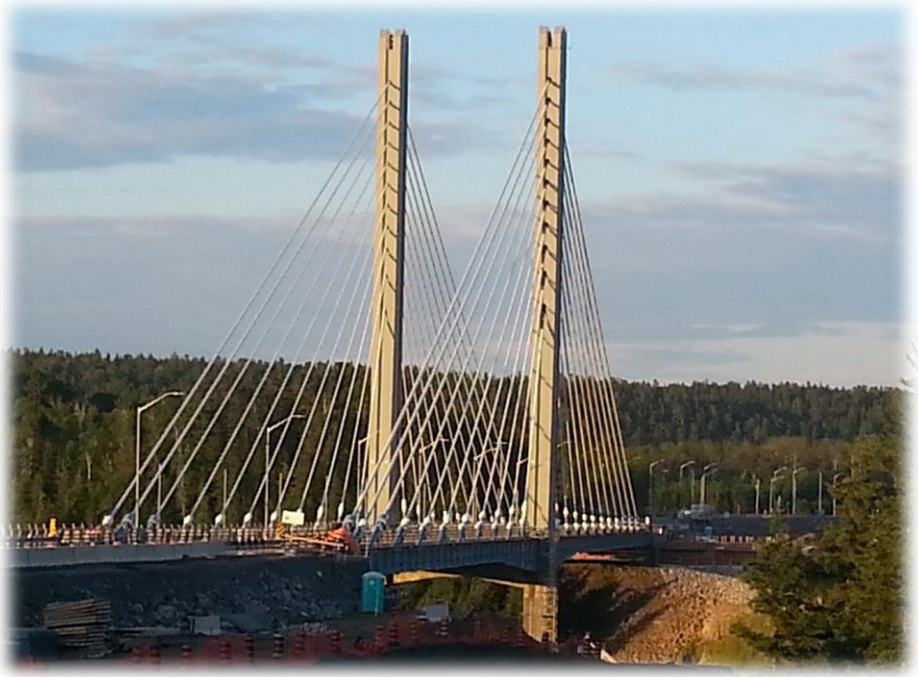
- A Single Point of Failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working.

- A Common Cause Failure (CCF) event is a failure where two or more items fail within the mission time from a common failure mechanism.

“Too Little”

BASTION TECHNOLOGIES

The 2016 Nipigon River Bridge Closure

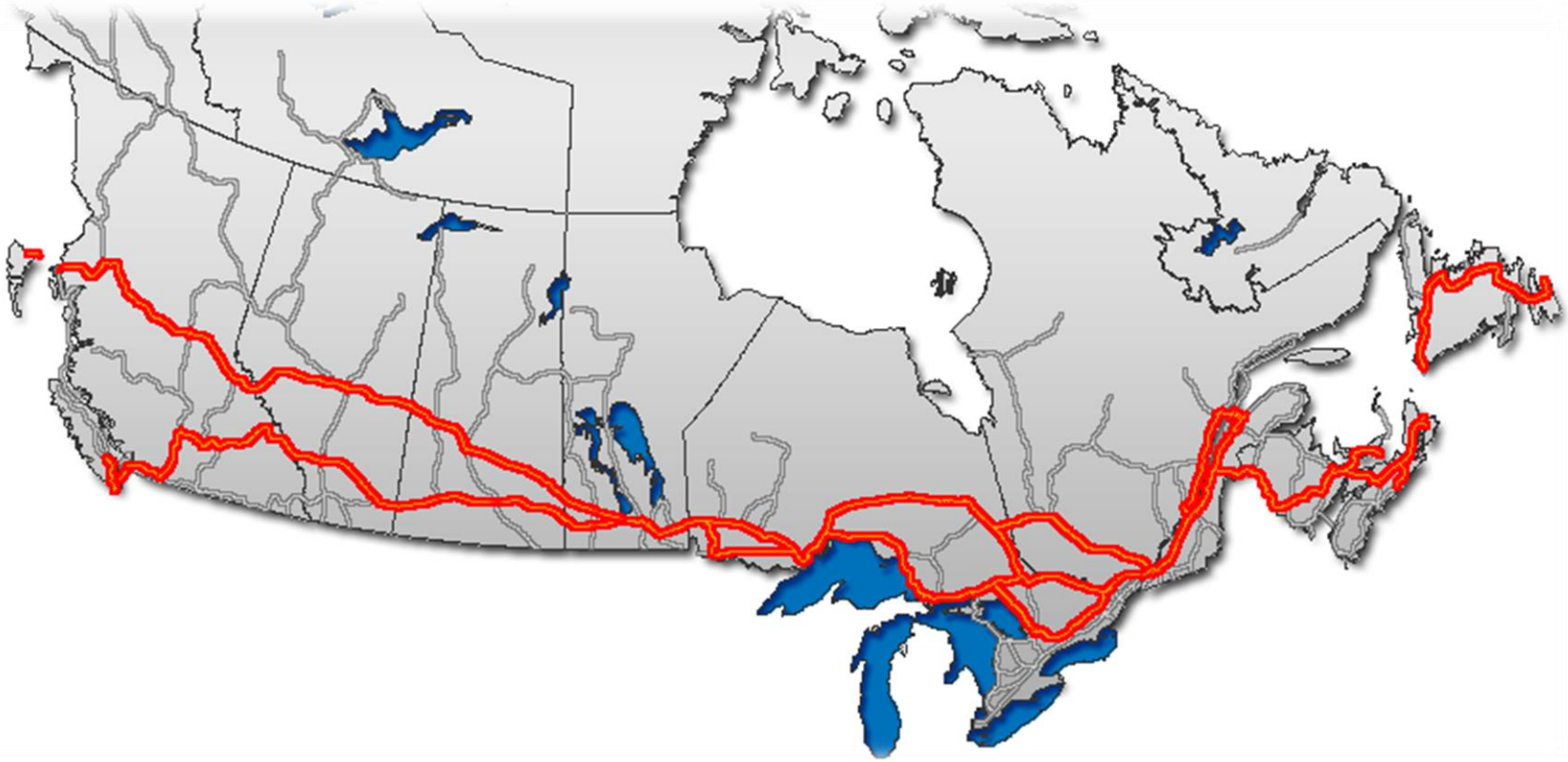


“Too Little”

The 2016 Nipigon River Bridge Closure

BASTION TECHNOLOGIES

The Trans-Canada Highway



“Too Little”

The 2016 Nipigon River Bridge Closure (cont.)

BASTION TECHNOLOGIES

The Trans-Canada Highway

"Too Little"

The 2016 Nipigon River Bridge Closure (cont.)

BASTION TECHNOLOGIES

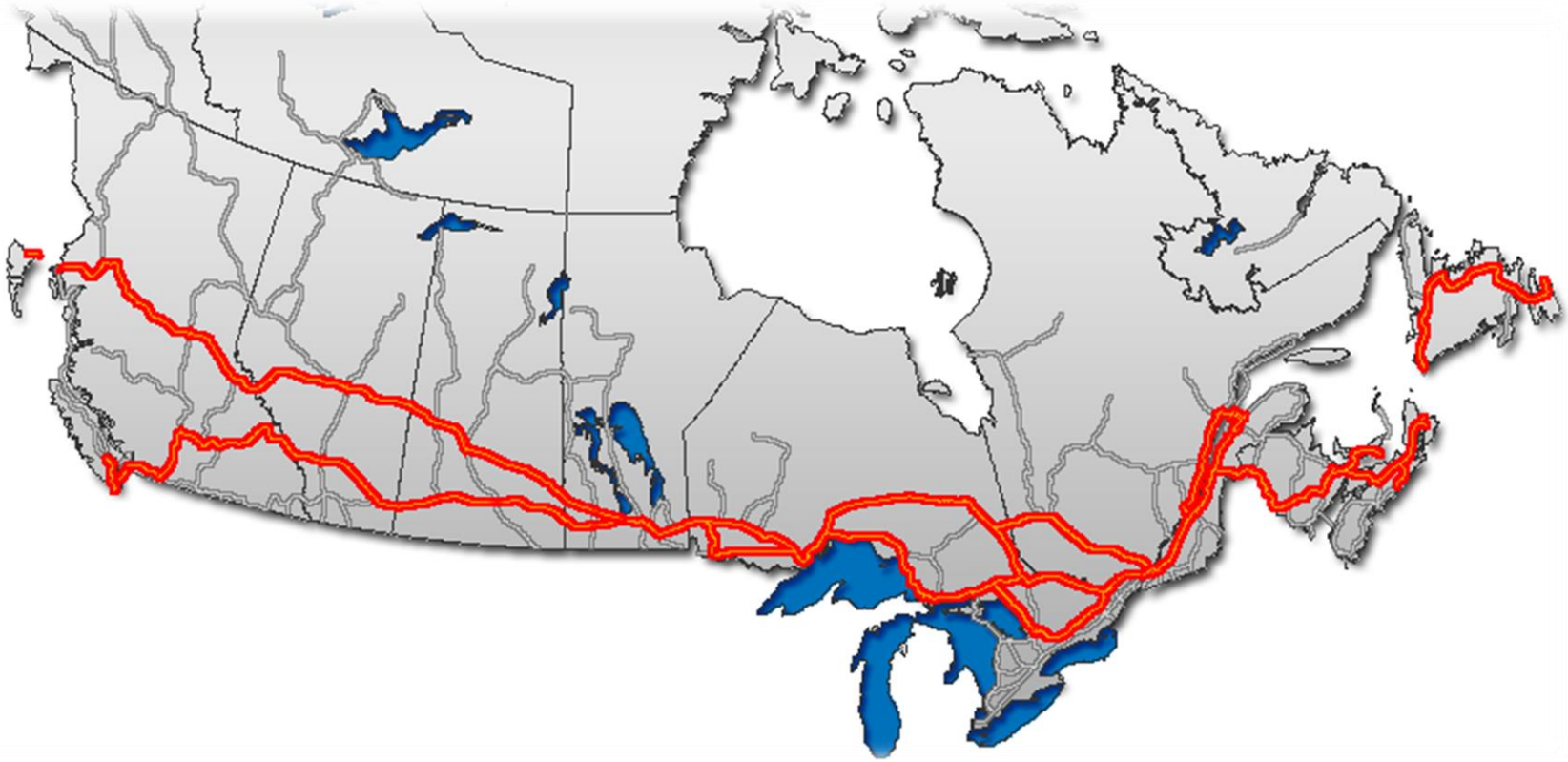
- Received winter damage January 2016, resulting in indefinite closure of the bridge.
- All road traffic stopped for 17 hours, until a single lane was reopened and used for alternating traffic between directions.
- As of the next day, 15-20 minute wait to cross single-lane.
- Estimated for that day over $100 million of goods within Canada delivered by truck were delayed by this closure.

“Too Little”

The 2016 Nipigon River Bridge Closure (cont.)

BASTION TECHNOLOGIES

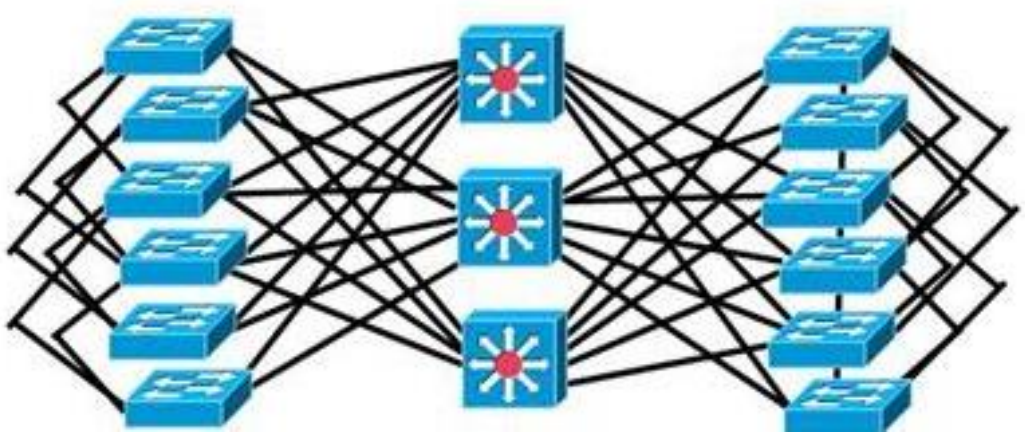
The Trans-Canada Highway



“Too Much”

BASTION TECHNOLOGIES

Additional Redundant
Trains of Communications
on Space Vehicles



“Too Much”

Additional Redundant Trains of Communications

BASTION TECHNOLOGIES

- From an outsider’s perspective, adding redundant trains into a system would increase the reliability of that system by a factor equal to the number of redundant trains, or does it?
- The aerospace industry often has limitations on weight, space, cost, and schedule, so a better understanding of the impact that redundancy has on reliability can result in more appropriate design decisions.
- 2017 RAMS presentation, “How Much Redundancy is too Much Redundancy?” by Adam Harden.

"Too Much"

Additional Redundant Trains of Communications (cont.)

BASTION TECHNOLOGIES

Analysis utilizing redundant train combinations of communication line system on an imaginary space vehicle:

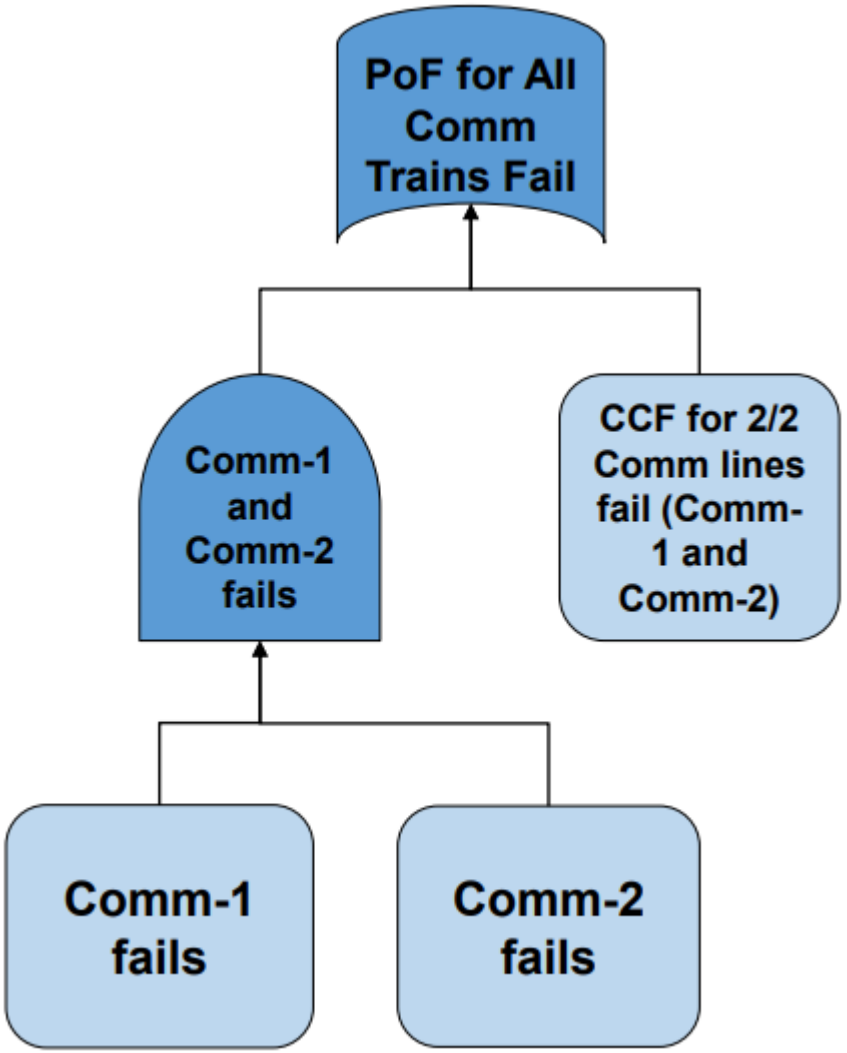
- A "Success" is any one train succeeds (meets its criteria).
- The reliability and probability of failure (PoF) of each combination will be determined from one up to eight trains.
- Perform comparison of the different combinations to demonstrate the returns on reliability.

"Too Much"

Additional Redundant Trains of Communications (cont.)

BASTION TECHNOLOGIES

- The fault tree to the right presents the logic for failure of comm-1 and comm-2
- The PoF for the top gate is:
  - Common Cause Failure (CCF) for 2 of 2 Comm lines, OR
  - Comm-1 AND Comm-2 fail
- For this example, the CCF probability is the product of the independent failure probability and the alpha factor for the failure combination 2 of 2 for generic rate based events
- Similar logic is used to incorporate additional trains

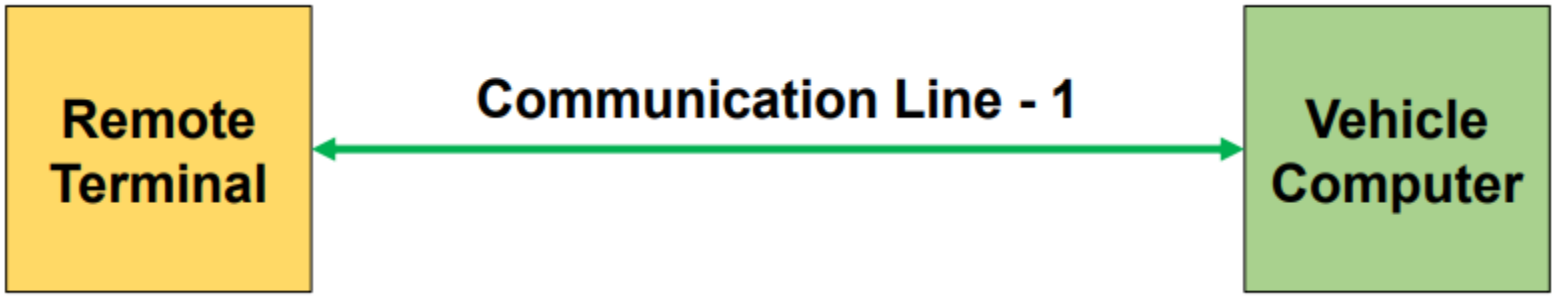


"Too Much"

Additional Redundant Trains of Communications (cont.)

BASTION TECHNOLOGIES

- The below diagram shows a 1-train line system that communicates data between a space vehicle's computer and a remote terminal connected directly to it.



- The table below presents the estimated reliability and Probability of Failure (PoF) of the communication line.

Success Criteria	Reliability	Failure Criteria	PoF
1 of 1	0.999	1 of 1	1.00E-3 (1 in 1,000)

"Too Much"

Additional Redundant Trains of Communications (cont.)

BASTION TECHNOLOGIES

Success Criteria	Reliability	Failure Criteria	PoF	% Change in Reliability from a Single Train	% Change in Reliability from Each Additional Train
1 of 1	0.999	1 of 1	1.00E-03 (1 in 1,000)	NA	NA
1 of 2	0.99993	2 of 2	6.98E-05 (1 in 14,300)	93.0%	93.0%
1 of 3	0.999959	3 of 3	4.12E-05 (1 in 24,300)	95.9%	2.9%
1 of 4	0.999975	4 of 4	2.52E-05 (1 in 39,700)	97.5%	1.6%
1 of 5	0.999983	5 of 5	1.68E-05 (1 in 59,500)	98.3%	0.8%
1 of 6	0.999987	6 of 6	1.30E-05 (1 in 76,900)	98.7%	0.4%
1 of 7	0.999993	7 of 7	7.17E-06 (1 in 139,400)	99.3%	0.6%
1 of 8	0.999996	8 of 8	4.29E-06 (1 in 233,200)	99.6%	0.3%

Largest increase in reliability comes from the addition of a second train. Note that the percent change in reliability from each additional train is reduced at each interval, except from a group size of 6 to 7.

“Just Right”

BASTION TECHNOLOGIES

The “Best” Amount

Of Redundancy

“Just Right?”

BASTION TECHNOLOGIES

- The “Best” amount of redundancy is always evolving.
- Time - Infrastructure and systems built decades ago were sufficient at the time but with aging comes degradation of effectiveness.
- Costs – A safety feature from decades ago would be too costly or bulky to make standard before, can now fit in a fraction of the space and at a fraction of the cost.
- The “Human Element” – Navigate the waters.
- “Make” the “Best” of it.

“Just Right?” (cont.)

BASTION TECHNOLOGIES

Conclusion

BASTION TECHNOLOGIES

- Too Little – Infrastructure that relies heavily on truck deliveries without alternate transit points can lead to disaster.

- Too Much – Adding significant redundancy does not necessarily mean significant increases to reliability.

- Just Right? - Find the sweet spot.

Questions?

BASTION TECHNOLOGIES

POC: Marion Whatley

Marion.E.Whatley@nasa.gov

256-544-1384

Backup Chart "Too Much"

Additional Redundant Trains of Communications (cont.)

BASTION TECHNOLOGIES

- The table below presents the calculated Alpha Factor values, of specific failure combinations, for generic rate based events

Group Size	Success Criteria	Failure Criteria	Alpha Factor
2	1 of 2	2 of 2	6.88E-02
3	1 of 3	3 of 3	4.12E-02
4	1 of 4	4 of 4	2.52E-02
5	1 of 5	5 of 5	1.68E-02
6	1 of 6	6 of 6	1.30E-02
7	1 of 7	7 of 7	7.17E-03
8	1 of 8	8 of 8	4.29E-03

Backup Charts (Cont'd)

BASTION TECHNOLOGIES

BIBLIOGRAPHY

Chart 2 –
https://en.wikipedia.org/wiki/Redundancy_(engineering)
https://ntrs.nasa.gov/citations/20170012470

Chart 4 –
https://en.wikipedia.org/wiki/Nipigon_River_Bridge

Chart 5 & 6 –
https://en.wikipedia.org/wiki/Trans-Canada_Highway
https://www.google.com/maps

Chart 7 –
https://en.wikipedia.org/wiki/Nipigon_River_Bridge
https://www.cbc.ca/news/canada/nipigon-river-bridge-numbers-1.3398986

Chart 8 –
https://en.wikipedia.org/wiki/Trans-Canada_Highway

Chart 9 –
https://www.certificationkits.com/cisco-certification/cisco-ccnp-switch-642-813-exam-study-guide/cisco-ccnp-switch-high-availability-a-redundancy/

Chart 10 to 14 –
https://ntrs.nasa.gov/citations/20170012470

Chart 16 -
https://ascelibrary.org/doi/pdf/10.1061/%28ASCE%291532-6748%282002%292%3A3%2827%29
https://www.tspe.org/page/ThePEandPolitics

Chart 17 -
https://theieltsgenius.com/speaking-part-3-saying-depends/