**ANALYZING SUPPLY CHAIN RESILIENCE USING TEMPORAL FAULT TREE ANALYSIS**

***Ernest E. Edifor1, David Lascelles1 and Graham Dixon2***

*1Manchester Metropolitan University, Manchester, UK*

*2Esprit Warehousing Ltd, UK*

# Introduction

Supply chain disruptions are inevitable because the world of business is dynamic and susceptible to environmental, political, economic, technological changes etc. As supply chains evolve to adapt to the changing world of business, they get complex and hence more efforts needed to analyse it to reduce the risks of disruptions. The question then is how can new or existing businesses reduce the risks associated with their supply chains? Over the past few decades, various solutions have been proposed to tackle this question. A promising solution suggests the use of a quantitative probabilistic safety assessment technique called Fault Tree Analysis (FTA).

FTA is backward-deductive technique used heavily in the engineering field to analyse the reliability of systems by determining how various component failures of the system can propagate to cause a total system failure. However, traditional FTA is unable to capture the dynamic behaviour (or sequential dependencies) inherent in real-world systems. This limitation can lead to inaccuracies in the results produced by FTA when used on some real-world scenarios.

In this paper, a recent improvement to FTA called Temporal Fault Tree (TFT) is used to analyse a supply chain with the aim of improving its resilience. First, there is a brief description and application of the logical gates in TFT. Using analytical approaches, these gates are used to model and analyse (logically and probabilistically) the risk drivers of a hypothetical supply chain network. Finally, a discussion of the results is made to provide some insight into how the supply chain can be improved to make it more resilient. The main contribution of this paper is the development of TFT-based techniques to analyse real-world supply chain risk drivers more accurately to improve supply chain resilience.

# Literature review

The business environment is continuously increasing in complexity, specifically with factors of risk becoming heavily interrelated (Manuj and Mentzer, 2008). Subsequently, appropriate resilience to risk is becoming more challenging as the task of detecting the catalyst of failure is more time consuming and problematic (Craighead et al., 2007; Simchi-Levi et al.,2015). Not only do internal risk factors have a potentially significant harmful effect on any company, the resulting systemic knock-on effects impact the wider supply chain, causing the interrelated links between the elements of the business environment to change in a way that may be even harder to understand (World Economic Forum, 2018). This in turn has significant implications for investment priorities, resource allocation and placement within the context of a risk mitigation strategy (Chopra and Sodhi, 2004; Tang, 2006). This has led to an increased focus on supply chain resilience and the development of conceptual frameworks to facilitate a better understanding of its antecedents and dynamics (Pettit et al., 2010; Ponis and Koronis, 2012).

One fundamental theme emerging from the literature on supply chain resilience is the need for optimisation of the resilience of a supply chain strategy or configuration (Machado et al., 2009). Many models are available to optimise supply chain design in the context of risk. Several are heuristics based (e.g. Baumgartner and Thonemann, 2010; Pan and Nagi, 2010). Such linear approaches fail to capture the dynamic nature and complex network of relationships in a supply chain. A promising alternative is the utilisation of Fault Tree analysis to simulate the cause and consequences of a disruption in a supply chain (Ziegenbein and Baumgart, 2006).

FTA (Vesely et al., 2002), developed over 6 decades ago, is a Probabilistic Safety Assessment (PSA) technique. It is a top-down approach of determining how the basic component failures of a system can propagate to cause an entire system failure. Traditionally, FTA uses the Boolean gates AND and OR to model relationships between two or more events. The AND gate is fired when all the events have occurred and the OR gate is fired when at least one of the events have occurred. A fault tree diagram is a graphical representation of the events (faults) of a system and the relationship between them. Once a fault tree of a system is constructed, two main types of analysis – logical and probabilistic – can be performed. Logical (or qualitative) analysis involves the determination of the necessary and sufficient combinations of events that can cause the top-event (i.e. undesired system state). Probabilistic (or quantitative) analysis involves the calculation of the failure probabilities of the events (including the top-event). A detailed description of FTA is presented in (Vesely et al., 2002).

Classical FTA is unable to capture dynamic real-world events that have sequential dependencies which leads to inaccuracies in the logical and probabilistic analysis (Dugan, Bavuso and Boyd, 1992; Gulati and Dugan, 1997). Many attempts have been made to address this problem. A notable improvement of FTA is Dynamic Fault Tree (DFT) analysis (Dugan et al., 1992) that, proposes novel gates to capture sequential dependencies. However, DFTs are crafted mainly for probabilistic analysis. A more recent improvement which is herein refer to as Temporal Fault Tree (TFT) analysis (Walker, 2009) improves FTA by providing new dynamic logical gates that enable comprehensive logical (Walker, 2009) and probabilistic analysis (Edifor, 2014). The usefulness of this dual analytical capability for supply chain risk assessment is discussed in this paper.

# Problem description

Ziegenbein and Baumgart (2006) provide a promising quantitative technique using FTA to assess the probability of occurrence of a supply chain disruption. In their discussion, they classify supply chain risk drivers according to the Supply Chain Operation Reference (SCOR) categories of plan, source, make, deliver and environment, which are then analysed using the traditional FTA method (Figure 1).



Figure 1: Fault tree adapted from Ziegenbein and Baumgart (2006)

From the diagram, it is evident that the Make category fails when both Machine 1 and Machine 2 fail or when Machine 3 alone fails. In the case where both Machine 1 and Machine 2 would need to fail in order to trigger the failure of the Make category this assessment is logically accurate. However, if Machine 1 is a primary device and Machine 2 is a controller that detects the failure of Machine 1 and activates a standby device, then the assessment that both Machines 1 and 2 would need to fail in order to trigger the failure of the Make category is inaccurate. This is because the controller activate the standby machine immediately the primary machine fails so the Make category does not fail when the controller fails subsequently. However, if the controller fails before the primary machine fails, the make category fails because when the primary machine fails, the controller has failed and is unable to activate the standby machine. This sort of machine configuration is not uncommon in real-world systems. The aim of this paper is thus to analyse such real-world events more accurately. In this paper, the assumption is made that all events are non-repairable; i.e. once an event has occurred, it remains in the failed state.

# Assessment of supply chain risk

In addition to the traditional Boolean gates AND and OR, TFT uses three dynamic gates in its analysis. These are Priority-AND (PAND), Priority-OR (POR), Simultaneous-AND (SAND) and sometimes, parameterised-SAND (pSAND) as seen in Figure 2.



Figure 2: Logical gates (AND, OR, PAND, POR, SAND, pSAND)

Figure 2a represents an AND gate; the output event *Q* is triggered when all input events *A, B* occur. For example, if a business has two production plants, *P1* and *P2*, from which all their products are made, the failure of *P1* AND *P2* will lead to the business failing to fulfil its targeted production level. Figure 2b is the OR gate; the output event *Q* is triggered when at least one of the input events *A, B* have occurred. For example, if a business uses a haulier, *H*, to deliver goods to its retailers, *R* via two motorways, *M1 and M2,* then the business will fail to deliver goods to *R* when *H* fails OR (*M1* AND *M2* fail). Failure of *H* could be due to industrial action, liquidation etc., failure of *M1* and *M2* could be due to motorway disruption etc.

The PAND gate is used to represent scenarios where an input event occurs strictly before another input event to trigger an output event. As shown in Figure 2c, the output event *Q* occurs when event *A* occurs strictly before the subsequent event *B*. For example, assume a business has two main suppliers *S1*, *S2,* which supply 85% and 15% of a commodity respectively. If there is a shortfall in supplies from *S1*, an administrative officer *AO* puts in a request to *S2* to provide additional volume to make up the shortfall. In this case, a possible cause of failure in deliveries would be *AO* failing before *S1* – i.e. *AO* PAND *S1*. When *S1* fails and *OA* has failed prior to this event, the system fails because *S2* would not be triggered to deliver additional supplies.

The POR gate, represented in Figure 2d, is triggered when an event *A* occurs strictly before a subsequent event *B* but the subsequent event *B* need not occur for the gate to be triggered. Unlike the PAND gate where the output event is not triggered until all input events have occurred, in the POR gate, the output event is triggered when the first (leftmost) input event occurs. From the previous example for the PAND gate, if the maximum shortfall *S2* can supply if *S1* fails is 80%, then, for a shortage in supply to occur, *S1* must fail before *S2* or if only *S1* fails. In this case, the failure triggering expression can be expressed as *S1* POR *S2*.

The SAND gate, in Figure 2e, models the situation where two or more events occur at exactly the same time; *A* and *B* need to occur at exactly the same time to trigger *Q*. In the real world, it is difficult to find a practical example of the SAND gate because it is statistically nearly impossible for two or more events to occur at the exact same time (Merle et al., 2010). This has led to the creation of another gate called parameterised-SAND (pSAND) (Edifor et al., 2013). The pSAND gate represents the scenario where an event is triggered when two or more events occur within a specific period. pSAND is represented in Figure 2f; *Q* happens when *A* and *B* occur within a specific time frame. The time frame is represented by a “*d*” in the diagram; e.g. *d>0.1* means the duration between the events is 0.1 (days, hours, minutes, seconds etc.) Suppose a fruit juice business uses two products apple and mango to produce three juices – apple, mango and apple and mango juice. Both products are distinctly sourced from two suppliers *S1* and *S2* respectively. Assume both products are required to produce the apple and mango juice, the failure of *S1* and *S2* to supply within 2 days will lead to no production. After 2 days, arrangements are made for supply from other companies. With this scenario, there will be no production of apple and mango juice when both *S1* and *S2* fail within 2 days – i.e. *S1* pSAND *S2*.

A logical expression can be derived from the fault tree by using the following symbols ‘.’, ‘+’, ‘<’, ‘|’, ‘&’ and ‘&d’ for AND, OR, PAND, POR, SAND and pSAND respectively. Meaning, *A* AND *B* can be represented as *A*.*B*, *A* POR *B* as *A*|*B* and *A* pSAND *B* as *A* &d *B,* where “d” is the duration between *A* and *B*. Before constructing a fault tree, a top-event (i.e. system failure) must be identified. This could be supply disruption of an item, failure in order fulfilment etc. Once the top event has been identified, the direct sub-system failures that triggers the top-event must be identified. The sub-system failures can be decomposed by identifying their failures, propagate downwards until all the ending nodes in the fault tree are basic failures (known as basic events). Events that are not basic events or top-events are usually the intermediate events. The basic rules for constructing a fault tree are provided in (Vesely et al., 2002).

Each set of logical combinations of events that can cause the top-event is called a cut sequence. Through the use of the Boolean laws and the Temporal Truth Table (Walker, 2009), the logical expression can be reduced to its smallest, simplest form resulting in a combination of what is termed minimal cut sequences (MCSQ). The MCSQ is a combination of the basic events that are necessary and sufficient to trigger the occurrence of the top-event. In order to be necessary, each basic event in the MCSQ is needed to trigger the top-event. To be sufficient, each MCSQ, without the inclusion of other events, should trigger the top-event. The result of the logical analysis highlights the single points of failure of the system, which is extremely useful in resource allocation within a risk mitigation strategy. Logical analysis also enables development of more robust supply chain configurations.

The probabilistic analysis involves the evaluation of the probability of the top-event occurring and the contribution of various events to occurrence of the top-event. Various failure data (corresponding to the failure distribution) will therefore need to be assigned to each individual event. Some analytical and simulation techniques (Edifor, 2014) have been developed for these evaluations; the former is restricted to exponential distribution while the latter is not limited to any failure distribution. The sensitivity analysis and risks for each basic or intermediate event can be calculated as part of the probabilistic analysis. These calculations provide analysts with information regarding critical aspects of the system that may require more resource allocation, attention or backups.

## Case Study

An analysis of a hypothetical case study is considered to practically demonstrate the technique proposed in this paper. Kelso is a chemical plant that produces various chemicals for hospitals, universities and related sectors. It has two main chemical suppliers (Supplier-A and Supplier-B) and a haulier (Haulier-A) that transports the supplies from the suppliers to the company’s only plant. Kelso’s contract is such that, 75% of its chemicals are supplied by Supplier-A and 25% by Supplier-B. When both suppliers are unable to deliver their contracted volumes, Kelso’s administrator, who is based in the plant, requests the shortfall from Supplier-C with a lead-time of 2 days via a second Haulier (Haulier-B). Haulier-C delivers Kelso’s packaging from a Supplier-D. The supply contracts and supply configuration is such that if Administration fails its duties (e.g. due to employee sickness, industrial action, etc) before Supply-A fails to supply goods there would be no supply of goods from Supply-C. In addition, there would be failure in the supply of goods if Supply-A and Supply-B fail within 2 days. Finally, a failure of Supply-A and Supply-B before Supply-C or just the failure of Supply-A and Supply-B would lead to a failure in supplies.

A fault tree depicting the above scenario is presented in Figure 3 (note that the top-event is failure in order fulfilment). MotSX is motorway disruption to Supplier-X; VehSX is a vehicle failure (of a haulier) to Supplier-X; SupX is Supplier-X; Adm is the administrator.



Figure 3: Fault tree of Kelso

For the above fault tree, the top-event (failure in order fulfilment), can be expressed as

$$Top =\left(MotSA+VehSA+\left(Adm<SupA+SupA\&SupB\right)\right).\left(MotSC+VehSC+SupC\right)+(MotSD+VehSD+SupD)+\left(SupC\right)$$

Using the Euripides algorithm (Walker, 2009), the minimal cut sequences (MCSQs) from the above expression are:

$$Top =SupD+VehSD+MotSD+\left(SupA.SupB\right)+\left(MotSA.SupC\right)+\left(MotSA.MotSC\right)+\left(MotSA.VehSC\right)+\left(SupC.VehSA\right)+\left(MotSC.VehSA\right)+\left(VehSA.VehSC\right)+\left(\left(Adm<SupA\right).SupC\right)+\left(\left(Adm<SupA\right).MotSC\right)+\left(\left(Adm<SupA\right).VehSC\right)$$

The MCSQs above are the combinations basic events that distinctively lead to the top-event occurring; it can be considered as the most effective configuration of Kelso’s supply network. Immediately, it is clear that the single points of failure are Supplier-D (SupD), Haulier-C’s vehicle to Supplier-D (VehSD) and the motorway VehSD uses (MotSD). However, the expression does not provide any indication of which events are critical and contribute most to the occurrence of the top event, that is, failure in order fulfilment. To determine the contribution of each event to the occurrence of the top event, each event need to be assigned failure rates. Again, for the sake of demonstration, the failure data (restricted to exponential distribution) in Table 1 are assumed.

|  |  |
| --- | --- |
| *Event* | *Failure rate per hour* |
| VehSA, VehSB, VehSC, VehSD | 2.354E-8 |
| MotSA, MotSB, MotSC, MotSD | 3.251E-4 |
| SupA, SupD | 4.114E-8 |
| SupB, SupC | 2.332E-7 |
| Adm | 2.324E-5 |

Table 1: Failure data of events

Based on the availability of these failure data, the dynamics of the top event can be evaluated using formulae provided in (Edifor, 2014). Figure 4 is a graph showing the probabilities that Kelso will fail to fulfil its order from within the first hour to 10000 hours (approximately 417 days); these probabilities are 3.252E-04 and 9.971E-01 respectively. From the graph, it is clear that the likelihood of failing to fulfil orders within 417 days is almost certain whiles there is less likelihood of failure within the first hour.



Figure 4: Failure in order fulfilment from 1 hour to 10000 hours

At each point of the graph, the MCSQs and events contributing to the top-event occurrence can be evaluated. Table 2 is a summary of the top ten MCSQs (left) and events (right) contributing to the top event occurrence at 10000 hours; FV importance is the Fussell-Vesely Importance (Henley and Kumamoto, 1981) that shows the contribution of each event to the occurrence of the top-event.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *Order* | *MCSQs* | *Probability of failure* |  | *Order* | *Event* | *FV Importance* |
| 1 | MotSD | 0.9612 | 1 | MotSD | 0.9641 |
| 2 | MotSA.MotSC | 0.9240 | 2 | MotSA | 0.9269 |
| 3 | MotSA.SupC | 0.0022 | 3 | MotSC | 0.9268 |
| 4 | SupD | 0.0004 | 4 | SupC | 0.0022 |
| 5 | VehSD | 0.0002 | 5 | SupD | 0.0004 |
| 6 | MotSA.VehSC | 0.0002 | 6 | VehSD | 0.0002 |
| 7 | MotSC . VehSA | 0.00022 | 7 | VehSA | 0.0002 |
| 8 | SupA.SupB | 9.581E-07 | 8 | VehSC | 0.0002 |
| 9 | SupC . VehSA | 5.482E-07 | 9 | SupB | 9.608E-07 |
| 10 | VehSA . VehSC | 5.540E-08 | 10 | SupA | 9.608E-07 |

Table 2: Top ten contributing MCSQs (left) and events (right)

# Discussion

Motorway disruption to Supply-D is the most critical point of the supply chain; it features as a single point of failure (Table 2 – left) and as the biggest contributor to the top event (Table 2 – right). From the top ten list, Supply-A is the least contributor to the top event. This suggests that more resources should be channelled into making the supply of packaging more reliable because it is more likely to lead to failure in order fulfilment. An interesting point to deduce from the result is that, though VehSD is a single point of failure, its failure does not contribute much to the top-event as the failure of MotSA which is not a single point of failure. This could be because according to the failure data in Table 1, the former is relatively less likely to occur. The techniques that underpin TFT analysis make visible the interrelationships that exist between events and the probability of their occurrence. Such information is usually obscured in the complexity of many large real-world supply chain operations.

There are several benefits of using a dynamic technique, such as TFT, to model and analyse supply chain risk. As is obvious from Kelso’s example (though hypothetical), it can be used to (1) improve the supply chain network configuration (2) identify single points of failure in the supply chain network (3) pin-point critical aspects of the supply chain (4) identify combinations of supply chain network events that contribute most to the failure of the supply chain. Given some data on the severity of these events, the risks associated with each event can also be evaluated. FTA is flexible; whenever changes are applied to the supply chain network, the corresponding fault tree can be adjusted accordingly and re-evaluated to show how the changes impact the entire system.

# Conclusion

Supply chains are critical to business success therefore their resilience should be a priority for any business. However, analysing the resilience of a supply chain can be a daunting task. FTA, a technique popular in engineering has been used in analysing the supply chains, however, these analysis fail to capture some dynamic real-world scenarios.

In this paper, TFT analysis (a modification of traditional FTA), has been used to model and analyse a small supply chain network as a proof of concept. The potential benefits of this technique have been demonstrated and it is evident that TFTs can contribute to the improvement of supply chain network resilience.

# References

* Baumgartener, K., Andre F., & Thonemann, U. W. (2010), ‘Supply Chain Design Considering Economies of Scale and Transport Frequencies’. *EJOR*, Vol 218 (3), pp.789-800.
* Chopra, S. and Sodhi, M. S. (2004), ‘Managing Risk to Avoid Supply-Chain Breakdown’, *MIT Sloan Management Review*, 46 (1), pp. 53-62.
* Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J. and Handﬁeld, R.B. (2007), ‘The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities’, *Decision Sciences*, 38 (1), pp. 131-156.
* Dugan, J. B., Bavuso, S. J., & Boyd, M. A. (1992), ‘Dynamic Fault-Tree Models for Fault-Tolerant Computer Systems’, *IEEE Transactions on Reliability*, 41(3), pp.363-377.
* Edifor, E. E. (2014), ‘Quantitative Analysis of Dynamic Safety-Critical Systems Using Temporal Fault Trees’, *PhD Thesis*, University of Hull.
* Edifor, E., Walker, M., & Gordon, N. (2013), ‘Quantification of Simultaneous-AND Gates in Temporal Fault Trees’, *Advances in Intelligent Systems and Computing*, Vol 224.
* Gulati, R., & Dugan, J. (1997), ‘A Modular Approach for Analyzing Static and Dynamic Fault Trees’, *In Reliability and Maintainability Symposium*, pp. 57-63.
* Henley, E. J., & Kumamoto, H. (1981), ‘Reliability Engineering and Risk Assessment’, Prince-Hall, Inc, New Jersey.
* Machado, V. H., Azevedo, S. G., Barroso, A. P., Tenera, A. and Machado, C. M. (2009), ‘Strategies to Mitigate Supply Chain Disturbances’, *In Proceedings of POMS2009*, 20th annual conference of production and operations management society: Orlando.
* Manuj I, & Mentzer,J.T (2008), ‘Global Supply Chain Risk Management Strategies’, *International Journal of Physical Distribution & Logistics Management*, Vol. 38 (3), pp.192-223.
* Merle, G., Roussel, J., Lesage, J., & Bobbio, A. (2010), ‘Probabilistic Algebraic Analysis of Fault Frees with Priority Dynamic Gates and Repeated Events’, *IEEE Transaction on Reliability*, 59 (1), pp.250-261.
* Pan, F. & Nagi, R. (2010), ‘Robust Supply Chain Design Under Uncertain Demand in Agile Manufacturing’, *Computers and Operations Research*, Vol 37 (4) pp. 668-683
* Pettit, T., Fiksel, J. & Croxton, K. (2010), ‘Ensuring Supply Chain Resilience: Development of a Conceptual Framework’, *Journal of Business Logistics*, Vol 31 (1) pp. 1-21
* Ponis S.T. & Koronis E. (2012), ‘Supply Chain Resilience: Definition of Concept and its Formative Elements’, *Journal of Applied Business Research*, Vol 28(5), pp 9-21
* Simchi-Levi, D., Schmidt, W., Wei, Y., Zhang, P. Y., Combs, K., Ge, Y., Gusikhin, O., Sanders, M. and Zhang, D. (2015), ‘Identifying Risks and Mitigating Disruptions in the Automotive Supply Chain’, *Institute for Operations Research and the Management Sciences* Vol 45 (5) pp.375-390.
* Tang, C. (2006), ‘Robust Strategies for Mitigating Supply Chain Disruptions’, *International Journal of Logistics*, Vol 9 (1) pp. 33-45
* Vesely W., Stamatelatos M., Dugan J., Fragola J., Minarick J., & Railsback J. (2002), ‘Fault Tree Handbook with Aerospace Applications’, Washington DC: NASA Office of Safety and Mission Assurance.
* Walker, M. (2009), ‘Pandora: A Logic for the Qualitative Analysis of Temporal Fault Trees’, *PhD Thesis*, University of Hull
* World Economic Forum (2018), ‘The Global Risks Report 2018’, accessed on 7th May 2018, from https://www.weforum.org/reports/the-global-risks-report-2018
* Yin, R. (2009), ‘Case Studies: Design and Methods’, 4th ed, Thousand Oaks: Sage Publications
* Ziegenbein, A., & Baumgart, J. (2006), ‘Supply Chain Risk Assessment-A Quantitative Approach’, accessed on May 12, 2016, from http://www.fucam.ac.be/redirect.php3?id=46721