DEPENDABILITY BASED CONCEPT OF SUPPLY CHAIN RESILIENCE

L. BUKOWSKI J. FELIKS

AGH University of Science and Technology, Faculty of Management, email:jfeliks@zarz.agh.edu.pl
Cracow, Poland

Abstract
The paper proposes a general concept of logistic systems resilience and describes a new resilience tree. In this vector based approach, the term resilience is composed of four main elements: fault detection, fault removal, fault prevention and fault tolerance. A framework for evaluation of supply chain systems’ resilience was developed, based on fuzzy logic and a system of rules of the „if … then” type, that were appropriately weighted.

Keywords:
Resilience, Dependability, Fuzzy Logics

1. INTRODUCTION
In the last 20 years, we can distinguish six main trends in supply chain management:
- Lean supply chain – seeking reduced costs;
- Flexible supply chain – ability to change;
- Agile supply chain – ability to change quickly;
- Responsive supply chain – increased speed and flexibility supported by IT;
- Leagile supply chain – seeking reduced costs & ability to change quickly;
- Resilient supply chain – seeking reduced risks.

In the recent few years, resilience became more and more important as a “medicine” for the vulnerability of complex global networks in a risky environment. Many interesting papers were written on assuring an adequate level of logistic systems resilience. However, there is still a lack of a framework type approach that could be the foundation of building an expert system to support the design and evaluation of supply chain and network resilience. This paper attempts bridge this gap by presenting a new concept of supply chain resilience based on a dependability approach.

2. RESILIENT SUPPLY CHAIN
Supply chain resilience is a multi-dimensional phenomenon. Supply networks are becoming more complex, dynamically changing webs. A supply chain may be very lean and efficient but if it is unable to quickly find an alternative route of delivery, it will be susceptible to system shocks and disturbances. Many of the processes of supply chain management may unwittingly contribute to the creation of a system that, while responsive and efficient in the steady state, is so tightly coupled that it cannot prevent the escalation of threats and also has insufficient slack to cope with the demands of an unexpected event once it occurs [1].
MIT research group [2] defines resilience as “the ability to react to unexpected disruption and restore normal supply network operations.” Sheffi [3] examined the ways in which companies can recover from high-impact disruptions and focused on actions to lower vulnerability and increase resilience. These include:

- reducing likelihood of disruptions through monitoring and detecting weakest signals, demand-responsive supply chains, supply-chain wide collaboration, redundancy;
- operational flexibility through standardization of parts facilitating interchangeability, postponement or mass customization strategy to respond to unpredictable demand changes, customer and supplier relation management and multiple sourcing.

M. Christopher and H. Peck [4] define supply chain resilience as “the ability of the supply chain to return to its original state or move to a new, more desirable state after being disturbed”. Most define resilience as the ability to deal with unexpected events successfully after they have actually occurred. Christopher and Peck distinguish five broad elements of supply chain resilience:

- Supply chain understanding (pitch points, bottlenecks, critical path);
- Supply base strategy (risk awareness, audited monitoring);
- Design principles (keep several options open! – efficiency vs. redundancy, decoupling point, critical nodes);
- Collaboration (knowledge shared by partners, Supply Chain Event Management - SCEM);
- Supply chain agility (visibility, communication, velocity, acceleration);
- Supply chain risk management culture (nothing is possible without leadership from the top of the organization!)

Supply chain resilience is the ability and capacity to withstand systemic discontinuities and adapt to new risk environments. So supply chain resilience can be defined as not only the ability to maintain control over performance variability in the face of a disturbance but also a property of being adaptive and capable of sustained response to sudden and significant shifts in the environment. Having explored different aspects of supply chain resilience, it would appear that the characteristics of resilient supply chains are [1]:

- Agility, speedy reaction to sudden changes in demand or supply, in addition to
- Speed and cost-effectiveness;
- Adaptability over time as market structures and strategies evolve;
- Alignment of interests of all firms or units in the supply network, so that individual members optimize the chain’s performance when they maximize their own interests.

3. DEPENDABILITY BASED CONCEPT OF RESILIENCE

Dependability [5] of a system is the ability to deliver service that can justifiably be trusted. The service delivered by a system is its behavior as it is perceived by its user(s); a user is another system (physical, human) that interacts with the former at a service interface. The function of a system is what the system is intended for, and is described by the system specification. Dependability is an integrative concept that consists of three parts: the threats to, the attributes of, and the means by which dependability is attained.

Dependability encompasses the following attributes:

- Availability - readiness for correct service;
- Reliability - continuity of correct service;
Safety - absence of catastrophic consequences on the user(s) and the environment;
Confidentiality - absence of unauthorized disclosure of information;
Integrity - absence of improper system state alterations;
Maintainability - ability to undergo repairs and modifications.

Security is the concurrent existence of:

a) availability for authorized users only,
b) confidentiality, and
c) integrity

The above attributes may be emphasized to a greater or lesser extent depending on the application: availability is always required but to a varying degree, whereas reliability, safety and confidentiality may or may not be required. The extent to which a system possesses the attributes of dependability should be interpreted in a relative, probabilistic sense, and not in an absolute, deterministic sense. Due to the unavoidable presence or occurrence of faults, systems are never totally available, reliable, safe or secure. Definitions of availability and reliability emphasize the avoidance of failures, while safety and security emphasize the avoidance of a specific class of failures (catastrophic failures, unauthorized access or handling of information, respectively). Reliability and availability are thus closer to each other than they are to safety on one hand, and to security on the other; reliability and availability can be grouped together, and collectively defined as the avoidance or minimization of service outages.

Correct service is delivered when a service implements the system function. A “failure” is an event that occurs when the delivered service deviates from correct service”. A system may fail either because it does not comply with the specification or because the specification did not adequately describe its function. A failure is a transition from correct service to incorrect service, i.e., to not implementing the system function. A transition from incorrect service to correct service is called service restoration. The time interval during which incorrect service is delivered is a service outage. “An error is that part of the system state that may cause a subsequent failure”: a failure occurs when an error reaches the service interface and alters the service. “A fault is the adjudged or hypothesized cause of an error”. A fault is active when it produces an error, otherwise it is dormant. A system can fail in different ways referred to as failure modes. As shown in Figure 1, the modes characterize incorrect service according to three viewpoints: a) the failure domain, b) the perception of a failure by system users, and c) the consequences of failures on the environment.

**Fig. 1** Failure modes [5]
A system consists of a set of interacting components, therefore the system state is the set of its component states. A fault originally causes an error within the state of its components. An error is detected if its presence in the system is indicated by an error message or error signal that originates within the system.

The means by which dependability of systems is attained build on a set of four techniques:

- **Fault prevention**: how to prevent the occurrence or introduction of faults;
- **Fault tolerance**: how to deliver correct service in the presence of faults (e.g., redundancy);
- **Fault removal**: how to reduce the number or severity of faults (e.g., corrective or preventive maintenance);
- **Fault forecasting**: how to estimate the present number, the future incidence, and the likely consequences of faults.

**Fault prevention** is attained by quality control techniques employed during design and manufacture. Operational physical faults are prevented by shielding, radiation hardening, etc., while interaction faults are prevented by training, rigorous procedures for maintenance and "foolproof" packages. Malicious faults are prevented by firewalls and similar defenses.

**Fault tolerance** is intended to preserve the delivery of correct service in the presence of active faults. The use of sufficient redundancy may allow recovery without explicit error detection. This form of recovery is called **fault masking**. A widely-used method of fault tolerance is to use multiple devices in multiple channels, either sequentially or concurrently. When tolerance of operational physical faults is required, the channels may be of identical design, based on the assumption that hardware components fail independently. The channels implement the same function via separate designs and implementations, i.e., through design diversity.

**Fault removal** is performed both during the development phase, and during the operational life of a system. Fault removal during the development phase of a system life-cycle consists of three steps: verification, diagnosis and correction. Fault removal during the operational life of a system is classified as corrective or preventive maintenance. Corrective maintenance is aimed at removing faults that have produced one or more errors and have been reported, while preventive maintenance is aimed at uncovering and removing faults before they might cause errors during normal operation. The latter faults include a) physical faults that have occurred since the last preventive maintenance actions, and b) design faults that have led to errors in other similar systems. Corrective maintenance for design faults is usually performed in stages: the fault may be first isolated (e.g., by a workaround or a patch) before the actual removal is completed. These forms of maintenance apply to non-fault-tolerant systems as well as fault-tolerant systems, that can be maintainable on-line (without interrupting service delivery) or off-line (during service outage).

**Fault forecasting** is conducted by performing an evaluation of system behavior with respect to fault occurrence or activation. The evaluation has two aspects: (1) qualitative, or ordinal, evaluation that aims to identify, classify and rank the failure modes or the event combinations (component failures or environmental conditions) that would lead to system failures; (2) quantitative, or probabilistic, evaluation that aims to evaluate in terms of probabilities, the extent to which some of the attributes of dependability are satisfied; these attributes are then viewed as measures of dependability. The methods for qualitative and quantitative evaluation are either specific (e.g., failure mode and effect analysis for qualitative evaluation, or Markov chains and stochastic Petri nets for quantitative evaluation) or they can be used to perform both forms of evaluation (e.g., reliability block diagrams, fault-trees).

Based on this terminology, we propose to define dependability and resilience as:

- **Dependability** – readiness for safe (absence of catastrophic consequences) and correct service under normal (ordinary) work conditions.
• **Resilience** - readiness for safe (absence of catastrophic consequences) and correct service under abnormal (uncommon) work conditions.

So that we describe resilience as dependability in presence of abnormal situations (e.g. attacks, accidents, disasters).

4. **FRAMEWORK FOR EVALUATION OF SUPPLY CHAIN RESILIENCE**

To achieve a satisfactory level of resilience, we propose the following procedure, consistent with the 3 Rs: Recognition, Resistance and Recovery. Every supply chain or network type logistic system exposed to potential, external, “abnormal” type threats should be designed and implemented so as to allow its use according to the algorithm shown in Figure 2. This implies the need to equip the logistic chain or logistic network with a continuous monitoring system that enables quick and effective fault detection. In the event that a risk is detected, a fault prevention subsystem would be activated to prevent the negative effects of events that led to the activation. Risk detection would trigger the fault prevention subsystem to prevent the negative effects of the risk that triggered the activation. If the fault prevention subsystem fails (e.g., in the event of unforeseen risk or defects in the working of the subsystem), the fault tolerance subsystem should work (e.g., by starting surplus (redundant) structures that take over the damaged parts of the original system).

![Algorithm for ensuring supply chain resilience](image)

**Fig. 2** Algorithm for ensuring supply chain resilience (N – no; Y – yes)

In case of failure of all of the above-described subsystems, a complete reconstruction of the logistic system is necessary using the methods of reengineering.

This approach can provide an expert system for assessing the level of resilience of any logistic chain or network. The schematic diagram of this system is shown in Fig. 2.
Classical fuzzy sets with trapezoidal membership functions were used in building the resilience R evaluation system. Linguistic variables fault detection (FD), fault tolerance (FT), fault removal (FR) and fault prevention (FP) were assigned five classes by defining for three of them ranges of trapezoidal membership functions. Membership in class 1 in the case of the variables indicates the highest level of fault detection, fault tolerance or fault prevention. Five level (very high, high, moderate, low, very low) linguistic variables are proposed for Malicious faults evaluating the FD, FP, FT, FR parameters. The values of these variables may be set by experts and their uncertainty expressed with the use of fuzzy logic such as triangular membership functions.

Fault detection (FD); Fault tolerance (FT); Fault prevention (FP), Fault removal (FR)

Class number;
Class_1; Very high (>99,99%);
Class_2; High (99,7% – 99,99
Class_3; Moderate (98% - 99,7%);
Class_4; Low (90% - 98%);
Class_5; Very low (< 90%);

Expert knowledge on the impact of the various parameters on resilience is expressed in the form of “if … then” rules. A single rule is stated as:

if x is A then y is B       (w)

where A and B are linguistic variables (in this case FD, FP, FT, FR). The part of the rule associated with the word “if” is called the predecessor of the rule and the part occurring after the word “then” is the conclusion. The w factor in the parentheses indicates the weight assigned to a specific rule. Complex fuzzy statements may be expressed as “if … then” rules. The knowledge encoded in a rule base is derived from human experience and intuition as well as on the basis of theoretical and practical understanding of the properties of the studied object. The main task of this deduction system is to calculate the approximate value of the output variable (R in this case) based on the share of each rule from the rule base with an appropriate factor determining the “validity” of the rule. Fuzzy logic based systems are a kind of expert system built on a knowledge base that contains inference algorithms in the form of a rule base. What distinguishes fuzzy inference in terms of concept from conventional inference is the lack of an analytical description. The approximate inference mechanism transforms knowledge from the rule base into a non-fuzzy form. The non-fuzzy form of the result is obtained in the process of defuzzification. There are several known methods of defuzzification – center of gravity, center of gravity with extender border sets, first maxima and last maxima.
Defuzzification is interpreting the membership degrees of fuzzy sets into a real value [7]. A rules base for a system with four inputs and one output, where every variable was divided into 5 linguistic categories (VeryLow, Low, Moderate High and VeryHigh), includes 625 elements. The correctness of selection of rules as well as the shape and ranges of the membership function is verified with a simulation. Unfortunately this system currently is still in phase of testing and trial verifications.

5. CONCLUSION

A new multi-dimensional concept of supply chain resilience was proposed. The use of fuzzy sets to evaluate the level of resilience seems to be the appropriate. The next step will be the implementation of this concept to risk management of complex logistics networks with the example of supply of iron ore for the steel industry.

LITERATURE