Available online at www.sciencedirect.com

ScienceDirect

IFAC-PapersOnLine 49-12 (2016) 372–377

Scenario Research of Complex Manufacturing Systems' Vulnerability

V. Kul'ba*, L. Busk Kofoed, D. Kononov*, O. Zaikin*****

*V.A. Trapeznikov Institute of Control Sciences
65, Profsoyuznaya str., Moscow, 117997, Russia (e-mail: kulba@ipu. ru)

**Department of Architecture, Design &Media Technology,
Aalborg University Copenhagen, A.C. Meyers Vænge 15, DK-2450 Copenhagen SV
(e-mail: lk@create.aau.dk)

***Warsaw School of Computer Science
ul. Lewartowskiego 17, 00-169 Warsaw (e-mail: ozaikin@poczta.wwsi.edu.pl)

Abstract: This article proposes new analysis methods for complex manufacturing systems as part of the scenario research methodology of complex systems developed by the authors. A new concept of modeling of complex systems' vulnerability is suggested. A method for analyzing of crisis situations in behavior of complex manufacturing systems, including distributed systems is developed. A concept for determining complex systems' vulnerabilities is suggested. The strategic development model of PJSC "Gazprom" was considered. Scenario calculations of model behavior were conducted. The major vulnerability factors in the structural organization of the Company were revealed.

Keywords: Scenario research, complex manufacturing system, resistance, vitality, vulnerability.

1. INTRODUCTION

Company abilities, competitiveness, and other characteristics directly depend on approved development strategy. Effective means of implementation of this strategy is the introduction of intelligent manufacturing systems (IMS). IMS represent complex system organization of manufacturing interactions, research and development centers that supports effective functioning process and development of modern enterprise. IMS contains a security subsystem (SS) of functioning and strategic development of complex manufacturing system (CMS). The most important research parameters are stability, resistance, survivability, and vulnerability of CMS. The following terms are used below.

Target operation mode – the desired state, and/or direction of the operation and strategic development of CMS.

Stability of operation – system parameter, the ability of system to work in the target operation mode (TOM) despite the implementation of external influence on its elements.

Resistance – system parameter, the ability of system to work in the TOM despite either external influence or/and synergistic change modes of operation of its components. The main characteristic of system resistance is the time to reach the limit state of operation for CMS in the implementation of threats. Increasing this value reduces the risk of emergency situations (Kononov et al., 1999).

Survivability – system parameter, the ability of system to function under internal and/or external influence taking into account the possibility of its recovery.

Vulnerability – system parameter, characterizing the possibility of applying damage of any nature that violates the described system TOM.

These concepts should be used in the organizational, technical and production systems when (as opposed to technical) there is a risk of the "human factor". Note: If the old classic prognostic was mainly to monitor trends, the new, post-classical requires not only form, but also to anticipate development alternatives. Typically, there are several development options and scenarios for CMS in the face of changing circumstances. Each of them is a forecast of its behavior in time. It is hardly possible to select one of them, the most realistic. However, you can analyze the outcomes or characteristics of each scenario corresponding to a specific program of activities, estimating possible losses based on the system performance criteria (Zenter, 1982).

A priori, the nature, extent and the possibility of eliminating of these damages depend on the existing structure, operational conditions and means of influence. Thus, the vulnerability is directly related to the stability and survivability of a complex system.

This paper proposes a new approach to the study of "windows of vulnerability" for CMS, presented in the form of organizational and economic system. It is made by means of scenario analysis. Under scenario research we understand a way to investigate a complex system when the main tool is the construction and analysis of the spectrum of scenarios in its various strata, and the purpose of the research is a synthesis of the scenario with desired properties. The formalization of the appropriate methodology is given in (Kononov et al, 2001).

Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2016.07.633

2. THE VULNERABILITY OF COMPLEX SYSTEMS

The complex manufacturing system is characterized by a large number of essential parameters of the operation and development. Therefore, it is advisable to isolate its various components or strata to simulate system behavior.

For a CMS formal analysis it is proposed to use a method of presenting it in the form of organizational and economic system with a typical hierarchical stratification. Its premise is a natural hierarchy of activities, organizational, legal, etc. backgrounds of the CMS. The proposed analysis strategy is based on the methodology of scenario research (Schultz and Kul'ba, 2012).

Let us distinguish strata to describe the dynamic model.

Technology stratum is a technology complex (including logistics) that CMS owns or/and uses for its operation and development.

Organizational stratum is a formalized description of the organizational and functional structure, i.e. information and management relations between stakeholders.

Legal stratum describes the legislative regulation of the activities the CMS operates under.

Economic stratum describes the relationship which is governed by the cost category. Here we select industrial and financial ties, contractual arrangements with counterparties, the possibilities of their modernization and development.

In a cultural stratum we consider company-specific ethnic, historical, religious and cultural features, which can significantly influence the development.

By the social strata we assign the necessary set of data describing the flow of social processes both within the CMS and in the environment. The social stratum shows the social structure, the nature of activities performed, specific economic and cultural relations, the main indicators of social development, etc.

Vulnerability model is developed using the original formalized language for investigation of a complex system suggested in (Schultz and Kul'ba, 2012). The main language components define the following hierarchy of concepts.

Model 1. Complex system components.

1) system substrate (set of elements) X;
2) system structure (links between the elements and their characteristics) $R^{(X)}$;
3) internal concept of the system (a set of properties and characteristics) $P^{(X)}$;
4) system element (internal) $E^{(X)}(B, r, p)$, where $B\subseteq X$, $r\in R^{(X)}$, $p\in P^{(X)}$;
5) internal state of the system (a set of system elements and relations between them) υ;
6) environment substrate: set of elements Y;
7) environment structure (links between elements) $R^{(Y)}$;
8) set of environment properties and characteristics $P^{(Y)}$;
9) system element of the environment $E^{(Y)}(B, r, p)$, where $B\subseteq Y$, $r\in R^{(Y)}$, $p\in P^{(Y)}$;
10) state of the system environment χ;
11) extended state of the system $\mathbf{z}=(\upsilon,\chi)$;
12) characteristics of the external environment $\zeta^{(Y)}$;
13) common characteristics of the system and environment $\zeta^{(X,Y)}$;
14) system concept (assignment + interests) Π.

Then, formal system S is a set of relationships between these components. Dynamic model of system S behavior sets the temporary connection between the components. Suppose we have time period $\Delta=[t_0, T]$.

Sequence $\Re(\Delta)=\{\mathbf{z}(t),\ t\in\Delta\}$ *of expert-significant events will be called as a step-by-step scenario of system S behavior on scenario horizon* Δ.

Note that when $t_0=T$ scenario represents the current extended system state. Decision-maker (DM) defines the expert-significant event (ESE). Functioning quality of a complex system (CS), i.e. compliance of system functioning to its purpose, as well as to system security will be called as area of security and purpose (ASP) $Q(\mathbf{z},t)$, which depends on the extended system state. The general definition of quality and safety of operation that defines the properties of TOM represents condition (Kononov et al., 1999)

$$\mathbf{z}(t)\in Q(\mathbf{z},t), \text{ when } t\in\Delta. \quad (1)$$

Conditions (1) are set depending on the subject area, the object of study, nature and conditions of operation, etc.

Scenario $\Re(\Delta)$ *will be called security scenario, if for all* $t\in\Delta$ *conditions* (1) *is true.*

For scenario set $M\Re(\Delta,\sigma)=\{\Re(\Delta,\sigma)\ \sigma\in\Omega\}$

we introduce measure $\rho(\Re(\Delta,\sigma), Q)$ of scenario $\Re(\Delta,\sigma)$ distance from set Q, by deviation

$$\eta_s(t)=\rho(\Re(\Delta,\sigma), Q, t) \quad (2)$$

at time t, as well as conditions of acceptable deviation in the form

$$\rho(\Re(\Delta,\sigma), Q)\leq\varepsilon, \quad (3)$$

where $\varepsilon\geq 0$ is acceptable deviation from condition (2), (3).

Let $\mathbf{a}$ is target vector and $\mathbf{b}$ is target direction (TOM). To generate deviations estimates we define the following scenario $\Re(\Delta)$ characteristics for situation as the sequence of ESE change on horizon $\Delta=[t_0,T]$:

– current distance of scenario $\Re$ from the target vector $\mathbf{a}$

$$d^{(t)}{}_E(\Re,\mathbf{a})= \rho_E(\mathbf{z}(t),\mathbf{a})=\|\mathbf{z}(t)-\mathbf{a}\|_E$$

characteristic can be used to monitor actual deviation of the current extended system state from TOM during scenario implementation and/or can be the current estimate of the proximity to the border of the system security operation;