**Dynamic Advanced Fault-Tolerant Control of Mechatronic Systems**

Nodirbek Yusupbekov 1, Shuhrat Gulyamov1, Dilshod Mirzayev2, Nurbek Matyokubov1, a)

1 Tashkent state technical university named after Islam Karimov, Tashkent, Uzbekistan

2Tashkent State University of Economics, Tashkent, Uzbekistan

a) Corresponding author: [nm85@mail.ru](mailto:nm85@mail.ru)

**Abstract.** The paper presents a dual (bipartite) approach to the dynamic advanced control of fault tolerance in mechatronic robotic control systems under the following conditions throughout the entire life cycle of the designed system: evolving requirements for the reliability of individual components and the system as a whole; the need for both increasing and deliberate reduction of fault tolerance levels, depending on current operational demands. Implementation of the proposed approach enables the development of architectures and corresponding component bases for reconfigurable systems, providing temporary enhancement of fault tolerance for individual robots performing the most critical and responsible tasks at any given time, without requiring initial hardware-software redundancy for each robot.

**INTRODUCTION**

The key distinguishing features of dynamic fault tolerance management compared to conventional approaches are twofold. On the one hand, there is the evolution of reliability requirements for individual components and the overall control system throughout the entire life cycle of the designed system. On the other hand, the approach enables both increasing and deliberate reduction of the fault tolerance level, depending on current operational needs and task priorities.

The necessity to modify the required fault tolerance level after the system has already been commissioned arises from the high degree of uncertainty inherent in the tasks faced by modern robotic control systems. This applies not only to specialized autonomous robotics but also to industrial robots operating within contemporary digital manufacturing environments (Industry 4.0 / smart factories).

A defining characteristic of such production systems is the continuous reconfiguration of technological processes driven by the manufacturing of a wide range of highly customized and deeply personalized products. Under these conditions, manufacturers and integrators of robotic systems lose the ability to accurately predict and specify the fault tolerance requirements for each robot at the commissioning stage. At the same time, excessively conservative (overestimated) initial requirements lead to substantial cost increases in the equipment.

The proposed solution consists of the development of architectures and corresponding component bases for reconfigurable robotic systems, which will enable temporary enhancement of fault tolerance for individual robots performing the most critical and responsible tasks at any given moment, without requiring initial hardware-software redundancy for every single robot in the system.

**DYNAMIC FAULT TOLERANCE MANAGEMENT OF ROBOTIC CONTROL SYSTEMS**

Consider the application of dynamic fault tolerance management using the example of transport robots operating in a digital multi-variety (high-mix) mechanical engineering production environment. Assume that each robot under consideration is a four-wheeled mobile platform equipped with a manipulator (Fig. 1a). The payload capacity and working envelope of the manipulator enable automatic loading of workpieces with a mass of up to 7 kg, whereas the load-carrying capacity of the mobile platform itself is 170 kg. The robot is powered by a lithium-ion battery pack, which, under ideal conditions, provides up to 4 hours of autonomous operation.

*a)*

*b)*



**FIGURE 1.** (a) A mobile robot equipped with a manipulator and androgynous docking units, (b) a road train of several mobile robots connected via androgynous docking units.

The robot’s manipulator is equipped with an androgynous docking interface for connecting interchangeable tools, similar to the one described in [1]. This interface provides not only mechanical coupling but also commutation of power supply with a working current of up to 5 A, as well as an Ethernet-compatible fieldbus. The mobile platform is also fitted with an androgynous docking interface that enables several robots to be coupled into a train formation (Fig. 1b), ensuring both information and power supply interconnection between them. The platform’s docking interface is rated for currents of up to 20 A.

Let us consider how dynamic fault tolerance management of the described robots would be implemented in the case of an urgent order for the production of a small batch of various types of gas turbine engines.

During the generation of the production schedule, the MES system (Manufacturing Execution System) performs a risk assessment of potential delays in both primary and auxiliary operations. Based on this assessment, fault tolerance requirements are formulated for all equipment involved in the technological process.

For the mobile robots considered in this example, the set of possible risks to be evaluated was predefined by experts using the HAZOP procedure [2]. The evaluation of each specific risk was performed separately for every technological operation in which robot participation was planned. In the general case, such a procedure for identifying the composition of risks can be automated [3-6].



**FIGURE 2.** Calibrated risk graph.

The determination of the required fault tolerance level in the considered example was carried out in a semi-qualitative manner using one of the variants of a calibrated risk graph [7-10] (Fig. 2).

The following parameters of the graph were defined for the evaluation procedure:

Consequences of risk realization (C):

C1 – minor damage, originally accounted for in the production cost structure;

C2 – damage that significantly reduces the profit from order fulfillment;

C3 – damage leading to overall losses, including due to the disruption of the schedule for other orders;

C4 – damage affecting the financial stability of the enterprise.

**TABLE 1.** Fault Tolerance Levels Determined within the Considered Example

|  |  |  |
| --- | --- | --- |
| **Fault Tolerance Level** | **Designation** | **Acceptable probability of failure during a process operation** |
| There are no fault tolerance requirements | УО0 | — |
| Low | УО1 | No more 10-1 |
| Medium | УО2 | No more 10-2 |
| High | УО3 | No more 10-3 |
| Very high | УО4 | No more 10-4 |
| Unacceptable | УО5 | — |

In addition to the permissible failure probability (P₀) during the execution of a technological operation, each fault tolerance level is characterized by minimum requirements regarding the hardware redundancy multiplicity (Table 2). These requirements are determined, in a manner similar to [11], based on the fraction of detectable failures (F\_D – Fault Detection coverage) for the particular equipment unit.

**TABLE 2.** Requirements for the hardware redundancy ratio are defined within the framework of the example under consideration.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **The proportion of diagnosed failures *FD*** | **Minimum hardware redundancy ratio depending on the required level of fault tolerance** | | | |
| УО1 | УО2 | УО3 | УО4 |
| Less than 60% | 1 | 2 | 3 | 4 |
| From 60% to 90% | 0/1 | 1 | 2 | 3 |
| From 90% to 99% | 0/1 | 0/1 | 1 | 2 |
| More than 99% | 0/1 | 0/1 | 0/1 | 1 |

We now analyze the fault tolerance level requirements generated by the system for situations where the same risk results in different requirements when the robot executes different technological operations (Table 3).

**TABLE 3.** Results of Fault Tolerance Level Requirement Generation by the Manufacturing Execution Control System

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Technological operation** | **Risk** | **Risk parameters** | | | | **Required level of fault tolerance** |
| C | F | P | W |
| ... | | | | | | |
| Transportation of turbine blades | Impossibility of further transportation due to the failure of the power supply subsystem | C2 | F2 | P1 | W2 | Low |
| Transportation of turbine disk | Impossibility of further transportation due to the failure of the power supply subsystem | C3 | F2 | P2 | W2 | High |
| ... | | | | | | |

**CONCLUSIONS**

The previously noted difference of two levels in fault tolerance requirements is attributed to two main factors.

Firstly, the production volume of turbine disks is significantly lower than that of blades. In the described manufacturing environment, this results in a complete absence of warehouse stock for disks. At the same time, the disk is a critical component essential for turbine assembly; therefore, any delay associated with its transportation directly affects the ability to meet the established production schedule. This is reflected in the fact that the consequences of the risk under consideration are assessed as C2 for the operation of transporting turbine blades and as C3 for transporting the disk.

The second factor is the weight of the workpiece. The weight of the blades does not exceed 6 kg, which allows them to be quickly transferred to a second robot using its manipulator in the event of a failure, thereby minimizing delays. In contrast, the disk weighs more than 100 kg. In the absence of an overhead crane in the workshop, automatic reloading of the disk onto a functional robot outside zones equipped with special loaders is impossible. As a result, the possibility of preventing negative consequences in the event of risk realization is evaluated as P1 for transporting turbine blades and as P2 for transporting the turbine disk.

Once the requirements have been formulated, a compliance check is performed for each robot participating in the planned operations. In the example considered, to meet the required fault tolerance level, a robot must simultaneously satisfy the minimum requirements for both the probability of failure during the execution of a technological operation and the hardware redundancy multiplicity.

The control systems of the described transport robot—and its power supply subsystem in particular—possess no hardware redundancy (redundancy multiplicity 1/1). The built-in diagnostic system is capable of detecting up to 70 % of potential failures. The overall failure probability of the power supply subsystem (due to battery capacity degradation, discharge caused by leakage currents, deterioration of battery contact conductivity, etc.) is P₀₁ = 0.0125. This corresponds to fault tolerance level FT1, which is acceptable for transporting blades but insufficient for transporting turbine disks.

**REFERENCES**

1. A. Yun *et al.*, “ModMan: An advanced reconfigurable manipulator system with genderless connector and automatic kinematic modeling algorithm,” *IEEE Robotics and Automation Letters* **5**(3), 4225–4232 (2020); <https://doi.org/10.1109/LRA.2020.2977213>.
2. B. S. Dhillon, *Robot System Reliability and Safety: A Modern Approach* (CRC Press, Boca Raton, FL, 2015).
3. S. Rahman *et al.*, “ExpHAZOP+: Knowledge-based expert system to conduct automated HAZOP analysis,” *Journal of Loss Prevention in the Process Industries* **22**(4), 373–380 (2009); <https://doi.org/10.1016/j.jlp.2009.02.006>.
4. GOST R IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety Systems* (Standartinform, Moscow, 2010).
5. N. R. Matyokubov, T. O. Rakhimov, and S. G. Boboyev, “Group control of functional linear actuation elements of mechatronic modules,” *Transactions of the Korean Institute of Electrical Engineers* **73**(6) (2024); <https://doi.org/10.5370/KIEE.2024.73.6>.
6. N. Yusupbekov, N. Matyokubov, and T. Rakhimov, “Electromagnetic mechatronic module control algorithm based on linear performance element of industrial robots,” *AIP Conference Proceedings* **3119**(1), 060012 (2024); <https://doi.org/10.1063/5.0213521>.
7. International Electrotechnical Commission (IEC), *IEC 62061: Safety of Machinery—Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems* (IEC, Geneva, 2005).
8. V. Hegde, “Reliability in the medical device industry,” in *Handbook of Performability Engineering*, ed. K. B. Misra (Springer, London, 2008), pp. 997–1009.
9. A. N. Yusupbekov and U. U. Kholmanov, “Intelligent glass production process control system,” in *Lecture Notes in Networks and Systems*, Vol. 912 (Springer, 2024), pp. 103–109; <https://doi.org/10.1007/978-3-031-53488-1_12>.
10. U. U. Kholmanov and V. H. Shamsutdinova, “Application of gas mixture detectors for automatic control systems,” *AIP Conference Proceedings* **3119**(1), 030005 (2024); <https://doi.org/10.1063/5.0214844>.
11. A. M. Romanov, A. I. Kharchenko, and E. N. Kashirskaya, *Software for Logging Fault and Emergency Monitoring Signals of Technological Equipment Operation* (Certificate of computer program registration No. 2016662149, Russian Federation, issued October 31, 2016).