DOI: 10.35598/mcfpga.2026.017

Safety Assessment of a Fault-Tolerant Microcontroller-Based Wind Turbine Control System Considering Safe States and Maintenance Strategy

1st Leonid Ozirkovskyy
ORCID 0000-0003-0012-2908
Institute of Information and Communication Technologies and Electronic Engineering (ICTE)
Lviv Polytechnic National University
Lviv, Ukraine
leonid.d.ozirkovskyi@lpnu.ua

2nd Bohdan Volochiy
ORCID 0000-0001-5230-9921
Institute of Information and Communication Technologies and Electronic Engineering (ICTE)
Lviv Polytechnic National University
Lviv, Ukraine
bohdan.y.volochiy@lpnu.ua

3rd Bohdan Husiak
ORCID 0009-0000-6041-2849
Institute of Information and Communication Technologies and Electronic Engineering (ICTE)
Lviv Polytechnic National University
Lviv, Ukraine
bohdan.husyak@lpnu.ua

***Abstract*—This paper presents a methodology for the quantitative assessment of the safety indicators of a fault-tolerant microcontroller-based wind turbine control system (WTCS) with recovery, treated as a mission-critical system. Unlike the classical case of implementing microcontroller-based control systems with a 2-out-of-3 majority structure, the present WTCS is a functionally heterogeneous structure in which a redundant main microcontroller is combined with an independent protection (safety) chain and a safe-stop actuation path (pitch-to-feather and braking). A distinctive feature of the proposed structure is that not every failure of a microprocessor module leads to an accident: a controller failure that triggers transition to a safe state is treated as a degraded-but-safe condition rather than an emergency. The paper proposes a methodology for the quantitative assessment of the WTCS safety indicators using the improved state space method. The proposed methodology is intended for the system engineering design stage and models the system behaviour with a high degree of adequacy, taking into account both failure rates (λ) and recovery rates (μ). By applying this methodology, the designer obtains the failure functions FA(t), which are analogues of minimal cut sets, and the probability of the system entering an emergency situation Q(t) over the entire operating interval. The influence of the maintenance strategy on safety is demonstrated. The results are validated by fault tree analysis.**

Keywords*—*microcontroller-based system*, *safety, safety indicators, wind turbine control system, fault-tolerant system, state space method, failure function, minimal cut sets, recovery, maintenance.

I. Introduction

Wind energy has become a critical part of modern power infrastructure, and the wind turbine control system (WTCS) belongs to the class of mission-critical systems whose failure may cause severe material damage, equipment destruction, or hazard to personnel [1]. The control system governs power regulation, blade pitch, nacelle yaw orientation, and, most importantly, the safe shutdown of the turbine in abnormal conditions such as rotor overspeed. The design of such systems is governed by standards IEC 61400-1 for wind turbine safety [2] and IEC 61508 for functional safety of electrical/electronic safety-related systems [3].

A characteristic property of a microcontroller-based WTCS that distinguishes it from systems with a symmetric 2-out-of-3 majority structure is that it is functionally heterogeneous and possesses a designed safe state. A loss of the main control function does not by itself constitute an accident: if the protection chain and the safe-stop actuation operate, the turbine is feathered and braked, i.e. it reaches a degraded-but-safe condition. An accident occurs only when the control function is lost and the path to the safe state is also unavailable, which may lead to uncontrolled overspeed and structural failure.

At the system engineering design stage, when no physical prototype exists, it is necessary to assess safety indicators by modelling. Field testing is not applicable, therefore the development of design methodologies that estimate safety indicators through analytical models is a relevant task.

II. Problem Statement and Limitations of Traditional Methods

Three interrelated indicators are used for a comprehensive safety assessment: minimal cut sets (MCS), the probability of an emergency situation Q, and the frequency of failure w(t) [4]. Minimal cut sets are a qualitative indicator that identifies the vulnerable points of the system, i.e. the minimal combination of component failures that causes the whole system to fail. The probability Q is a dimensionless value reflecting the

probability that at a given moment the system is in an emergency state.

The principal method for the qualitative search of minimal cut sets is fault tree analysis (FTA) [4]. It also allows the average values of Q and w(t) to be calculated, but considers them statically, i.e. at fixed points in time, which does not reflect the dynamics of safety indicators in the presence of repair. For a repairable WTCS, safety depends not only on the mean time to failure (MTTF) but also on the mean time to repair (MTTR), and consequently on the chosen maintenance strategy [8]. These factors are not captured by static methods, and dynamic fault trees lack a universal procedure for quantitative assessment.

To overcome these limitations, the improved state space method based on state transition diagrams is used [5], [6]. It models the system as a set of discrete states with failure intensities λ and recovery intensities μ, and yields the failure functions FA(t) as time-dependent analogues of minimal cut sets over the entire operating interval.

A further shortcoming of the classical approach is that it implicitly treats every combination of two or more component failures as an accident. For a wind turbine this assumption is overly conservative: many failure combinations are intercepted by the protection chain and resolved by transition to a safe state, so they should not be counted in the probability of an emergency situation. A method that does not distinguish safe states from accident states therefore overestimates the risk and may lead to an unjustified increase of redundancy. The improved state space method removes this drawback because each module is represented by a separate component of the state vector [5], which preserves complete information about the operability of every subsystem at any moment and allows the safe and accident subspaces to be separated explicitly.

III. Architecture of the Wind Turbine Control System

The object of study is a microcontroller-based WTCS organised as a heterogeneous fault-tolerant structure consisting of three functionally distinct subsystems [7]:

the redundant main microcontroller (C), which performs power and pitch regulation and is built as a voting structure; *the independent protection chain (P)*, which monitors overspeed and vibration and initiates emergency shutdown; and *the safe-stop actuation path (B)*, which feathers the blades (pitch-to-feather) and applies aerodynamic and mechanical braking.

To describe each state of the WTCS, a state vector with three components (C, P, B) is used. If a subsystem is operational, the corresponding component equals 1; if it is faulty, the component equals 0. The initial state, when all subsystems are operational, is (1,1,1). A failure of the controller leads to (0,1,1), a failure of the protection chain to (1,0,1), and a failure of the safe-stop path to (1,1,0).

Transitions characterised by the failure rate λ reflect the loss of a subsystem; transitions characterised by the recovery rate μ reflect its repair and are directed from a state with fewer operational components to a state with more. Because the WTCS is repairable, the non-operational states are not absorbing.

The reliability behaviour of the WTCS is described as follows. From the fully operational state (1,1,1) three failure transitions are possible, corresponding to the loss of operability of the microcontroller, the protection chain, or the safe-stop path. From a state in which the microcontroller has failed, a subsequent failure of the protection chain or of the safe-stop path leads to a condition in which a safe shutdown can no longer be guaranteed. By contrast, a failure of the microcontroller alone is compensated by an operational protection chain and safe-stop path, so the corresponding state is degraded but safe. The repair of any subsystem returns the system towards states with a higher number of operational components, which models continuous maintenance during operation.

IV. Failure Condition with Account of the Safe State

The key feature of the proposed model is the classification of non-operational states into two subspaces: safe (degraded) states and accident states. An accident requires the simultaneous loss of the control function and the safe-stop path. Hence the logical failure (accident) condition is formulated as:

$$(C = 0 \wedge B = 0) \vee (C = 0 \wedge P = 0) \vee (P = 0 \wedge B = 0) \quad (1)$$

After minimisation according to the rules of Boolean algebra, the condition is obtained in disjunctive normal form as a disjunction of elementary conjunctions, which are also called masks of failure situations:

$$M1\colon (C = 0 \wedge B = 0);\ M2\colon (C = 0 \wedge P = 0);\ M3\colon (P = 0 \wedge B = 0) \quad (2)$$

The masks are used to select, from the subspace of non-operational states, those states that correspond to an accident, while states in which the loss of control is compensated by an operational safe-stop path are assigned to the safe subspace. This step extends the previously published six-stage methodology [6] with an explicit separation of safe and accident states.

V. State Graph and Analytical Model as a System of Kolmogorov–Chapman Equations

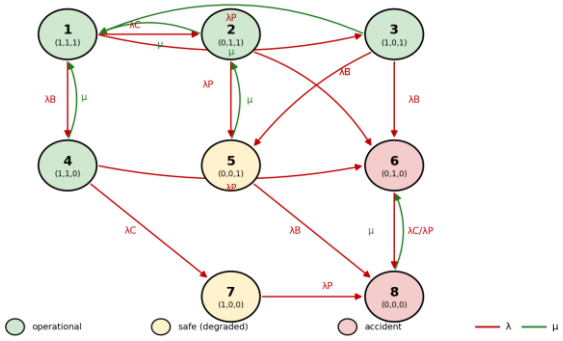

Fig. 1. State and transition graph of the fault-tolerant wind turbine control system with safe states and constant recovery.

On the basis of the state and transition graph (Fig. 1), a system of linear Kolmogorov–Chapman differential equations with constant coefficients is formed [8], which constitutes the analytical model of the system. The number of equations equals the number of states:

$$d\boldsymbol{P}(t)/dt \;=\; A \cdot \boldsymbol{P}(t) \qquad (3)$$

where P(t) is the column vector of probabilities of being in each state and A is the transition intensity matrix. Each diagonal element of A equals the negative sum of the intensities of all transitions leaving the corresponding state, while each off-diagonal element equals the intensity of the transition into that state from another state. The system was solved by the Runge–Kutta–Merson numerical method with an adaptive step, yielding the probability distribution of the system over the states $P_1(t)…P_8(t)$. The initial condition corresponds to a fully operational system, i.e. $P_1(0) = 1$ and all other probabilities equal to zero.

The failure functions are then formed as sums of the probabilities of the accident states selected by the masks, and the probability of an emergency situation is computed as the union of the failure functions treated as independent events:

$$FA_i(t) \;=\; \Sigma\, P_k(t),\; k \in Mi \qquad (4)$$

$$Q(t) \;=\; 1 - \prod (1 - FA_i(t)) \qquad (5)$$

VI. Results

Figure 2 shows the time dependence of the failure functions and of the probability of an emergency situation. Owing to recovery, the curves rise from zero and reach a steady-state plateau, in contrast to the monotonically increasing curves of a non-repairable system. The explicit account of the safe state reduces the steady-state value of Q in comparison with a naive 2-out-of-3 model that would treat any double failure as an accident, because controller failures compensated by the safe-stop path do not contribute to Q.

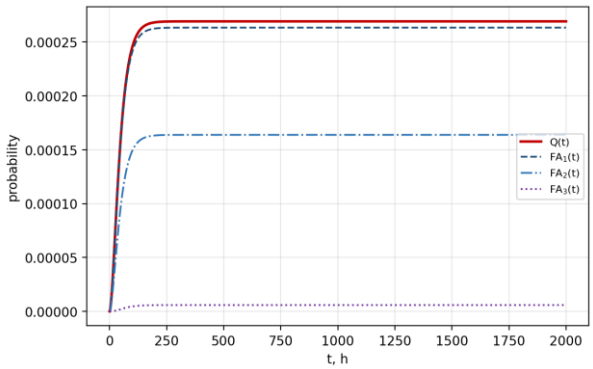

Fig. 2. Failure functions FA1(t), FA2(t), FA3(t) and probability of an emergency situation Q(t) of the wind turbine control system with constant recovery.

The influence of the maintenance strategy is illustrated in Table I, which lists the steady-state probability of an emergency situation for several values of MTTR. A faster repair (smaller MTTR, larger μ) substantially lowers Q, which quantifies the safety benefit of a more responsive maintenance policy.

It is important to note that for a repairable system the probability of an emergency situation does not grow without bound but stabilises at a steady-state value determined by the ratio of the failure and recovery intensities. This steady-state value is the quantity most relevant for long-life wind turbines, since it characterises the long-term availability of the safe-shutdown function. The failure functions FA1(t), FA2(t) and FA3(t) reach their plateaus at different levels, which reflects the different reliability of the three failure paths and indicates which combination of subsystems is the dominant contributor to risk. This information allows the designer to direct redundancy and maintenance resources to the most critical path rather than uniformly across all subsystems.

TABLE I. Steady-state Q for different maintenance strategies

MTTR, h	Q (steady state)
12	$6.7\cdot10^{-5}$
24	$2.7\cdot10^{-4}$
72	$2.4\cdot10^{-3}$

VII. Validation of the Results

The simulation results obtained were validated by comparing the results obtained for the present WTCS using fault tree analysis with the TopEvent FTA software [9]. For this purpose, a fault tree was constructed and the probabilities of the minimal cut sets, together with the probability of an emergency situation, were calculated at several fixed time points. The values obtained by the FTA method coincide with the failure functions and with Q(t) of the state space method within the permissible deviation,

which is explained by the use of numerical calculation methods in both cases. The validation results confirm the reliability of the results obtained by means of the proposed methodology.

VIII. CONCLUSIONS

This paper has assessed the safety indicators of a fault-tolerant microcontroller-based wind turbine control system. The proposed methodology, based on the improved state space method, made it possible to obtain quantitative values of the safety indicators — the failure functions and the probability of entering an emergency situation. The methodology enables the designer, already at the system engineering design stage, to account for the influence on functional safety not only of component reliability but also of the recovery parameters. Introducing an explicit separation of non-operational states into safe (degraded) and accident states yields a more realistic probability of an emergency situation Q(t) than a symmetric 2-out-of-3 model. The failure functions FA(t) provide the time dynamics of the minimal cut sets over the entire operating interval, taking into account both component reliability (MTBF) and repair procedures (MTTR). The proposed methodology is a practical tool for justifying redundancy and maintenance decisions at the system engineering design stage. Validation by fault tree analysis confirmed the reliability of the obtained results. Future work will address limited recovery resources and imperfect fault coverage of the protection chain.

REFERENCES

[1] K. Fowler (Ed.), Mission-critical and safety-critical systems handbook: Design and development for embedded applications. Butterworth-Heinemann/Elsevier, 2010, doi: 10.1016/C2009-0-18238-7.

[2] IEC 61400-1:2019, Wind energy generation systems – Part 1: Design requirements. International Electrotechnical Commission, Geneva, 2019.

[3] IEC 61508:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission, Geneva, 2010.

[4] A. Maurya and D. Kumar, “Reliability of safety-critical systems: A state-of-the-art review,” Quality and Reliability Engineering International, vol. 36, no. 7, pp. 2547–2568, 2020, doi: 10.1002/qre.2715.

[5] L. Ozirkovskyy, B. Volochiy, O. Shkiliuk, M. Zmysnyi, and P. Kazan, “Functional safety analysis of safety-critical system using state transition diagram,” Radioelectronic and Computer Systems, no. 2, pp. 140–150, 2022, doi: 10.32620/reks.2022.2.12.

[6] B. Volochiy and L. Ozirkovskyy, “Method of developing unified model for estimating safety and reliability of complex systems for critical application,” 14th Int. Conf. TCSET, Lviv-Slavske, Ukraine, 2018, pp. 801–804, doi: 10.1109/TCSET.2018.8336319.

[7] E. Ruchkov, V. Kharchenko, A. Kovalenko, I. Babeshko, and A. Poroshenko, “Reliability assessment of 2oo3 and 1oo2 redundant structures,” Advanced Information Systems, vol. 4, no. 4, pp. 77–83, 2020, doi: 10.20998/2522-9052.2020.4.11.

[8] A. D. Yadav, S. C. Malik, S. Malik, and N. Nandal, “Reliability-availability-maintainability of a repairable system using Markov approach,” OPSEARCH, vol. 60, no. 4, pp. 1731–1756, 2023, doi: 10.1007/s12597-023-00684-7.

[9] TopEvent FTA – Fault Tree Analysis Software. [Online]. Available: https://www.fault-tree-analysis.com/