# Established Definitions of Super-Critical Operational Modes as Automotive System Requirements

*Dmytro Humennyi[1], Oleksandr Humennyi[2]*

[1] Kyiv National University of Construction and Architecture
Povitroflots'kyi Ave, 31, Kyiv, Ukraine, 03037,
apollo.d.g@gmail.com, orcid.org/0000-0001-6736-0543
[2] Institute of Vocational Education of the National Academy of Pedagogical Sciences of Ukraine
Maksyma Berlyns'koho St, 9, Kyiv, Ukraine, 04060
gumenniy7@gmail.com, orcid.org/0000-0001-6596-3551

*Received 30.10.2023, accepted 04.12.2023*
https://doi.org/10.32347/uwt.2023.13.1201

**Abstract.** This paper introduces and elaborates on Super-Critical Operational Modes (SCOMs) within automotive systems. In the landscape of increasingly software-centric automotive functionalities, SCOMs are pivotal for maneuvering through severe operational disruptions while ensuring vehicle safety and longevity. Distinctly diverging from the traditional focus on normal operational modes and isolated component failures, this research accentuates the imperative need for a systematic understanding and mitigation of SCOMs. A nuanced classification system is proposed for SCOMs: Type I (Mild), Type II (Moderate), and Type III (Severe) intensities, each distinguished by their respective intensity levels, impacts, and recovery complexities. Particularly for Type III SCOMs, an innovative approach rooted in automatic diagnostics, analysis, and internal system restructuring is advocated, thereby obviating the need for external intervention. This framework provides invaluable insights for practitioners, enabling the identification, analysis, and autonomous response to SCOMs, thereby fostering the development of resilient, self-sustaining, and safe automotive systems.

**Keywords:** Automotive Platform, Super-Critical Operational Modes, Adaptability, Requirement Engineering, System Specifications.

**Dmytro Humennyi**
Associate Professor of the Department,
Candidate of Technical Sciences

Oleksandr Humennyi
Head of the Department,
Candidate of Pedagogical Sciences

## INTRODUCTION

Over the past fifteen years, the automotive industry has undergone a platform transformation, transitioning from hardware-oriented to software-oriented. Most functionalities of each industrial product are now software-oriented, with hardware serving to meet the software's vehicle management needs.

Development processes for both hardware and software in vehicles are well standardized through a suite of frameworks, standards, and best practices. This suite facilitates easy integration of processes and ensures transparency and traceability from both technological and holistic viewpoints.

A crucial early stage in developing vehicle hardware and software is describing system requirements and specifications that will underpin architectural design, component development, testing, integration, documentation, and traceability of the program. These factors facilitate the transfer of artifacts from one department to another, maximizing development efficiency through transparent and accessible processes and information.

According to the A-SPICE3.1 framework, the development of system requirements and specifications outlines the product's expected behavior at the highest level of abstraction. Here, the tasks for the system to function are defined, and the actions of hardware and software components are described as the product transitions from one mode of operation to another.

The modern approach to formulating system requirements and specifications focuses exclusively on normal operating mode. This approach also includes self-diagnostic tools that can identify a list of possible faults in the system that can be easily detected through direct measurement of values.

Thus, the current methods for describing requirements, which focus on normal operation and diagnosing faults in individual components, are also based on requirements. This is done by comparing obtained values with expected ones during pre-defined test cases.

Diagnostic data can be effectively used to transition the vehicle into a safe operating mode, allowing it to be safely transported to a service center for further functionality restoration or component replacement. The policy of ensuring user safety is deemed more important than preserving the vehicle’s functional integrity and its ability to continue operating without external intervention.

During vehicle operation, preserving its ability to continue functioning effectively for a certain additional time after a critical failure or breakdown is crucial. According to the author, this plays an important role in ensuring functional safety.

While working on a new automotive platform, the authors proposed and developed a new category of requirements describing system actions to restore functionality and integrity after a critical failure or breakdown. These requirements are based on the system's residual resilience. They share some features with the functional safety requirements of ISO/IEC 26262 but apply a different approach to classification and actions related to their execution.

The goal of this publication is to describe the classification of system requirements for the supercritical operating mode of an automotive platform.

## SUPER-CRITICAL OPERATIONAL MODES IN AUTOMOTIVE FIELD

**Introduction to Super-Critical Operational Modes.**

In the realm of automotive systems, the term 'critical mode' refers to scenarios where a system is operating at the limits of its designed capabilities, or is at risk of failing to meet established safety or reliability criteria[1]. Critical modes are pivotal, but there are instances where systems encounter situations more severe than these standard critical conditions, known as 'super-critical modes'. In a super-critical mode, an automotive system faces the risk of losing its structural integrity, which can result in the irreversible loss of its main functionalities.

These super-critical operational modes (SCOMs) are noteworthy not merely due to the impending risks they pose to the system itself but also due to the unforeseen risks that may arise in such states. This notion aligns with John von Neumann's innovative concept of developing dependable systems using components that are inherently unreliable. Von Neumann’s theory suggests that certain unreliability factors can be counteracted through incorporating structural and functional redundancies.

Automotive systems, particularly those with robotic functionalities operating under highly complicated and unpredictable conditions, are susceptible to transitioning into super-critical modes. Therefore, understanding, analyzing, and devising strategies to either prevent these modes or recover from them is crucial. The study of SCOMs and strategies for mitigation is imperative for the safety and reliability of automotive systems, drawing attention from various scholars and experts in the field. Notable contributions to understanding and addressing super-critical modes have been made by experts like Lerman, Kristina[4], Na, Jing[5], Goodwin, Walter[6], Tkach, Mykhailo[7], and Lisovychenko, Oleh[8]. Moreover, John von Neumann's foundational ideas on creating reliable systems continue to be a guiding light in this area of study[9].

**Characteristics of Super-Critical Operational Modes.**

Unique Features of SCOMs

Understanding the difference between critical and super-critical states in a system is essential, and this distinction can be illustrated through a mathematical and graphical approach. Let's denote the state of a system at time $t$ as $S(t)$.

- Stable Systems: In stable conditions, $S(t)$ maintains within a predetermined acceptable range of values, symbolically represented as $S(t) \in [a, b]$.
- Critical States: In a critical state, $S(t)$ might temporarily exit the acceptable range but eventually returns within the bounds, mathematically represented by:

$$\exists t_0 \text{ such that } S(t_0) \neg\in [a, b], yet \lim_{t\to\infty}\big(S(t)\big) \in [a, b]$$

- Super-Critical States: In a super-critical state, $S(t)$ permanently goes beyond the acceptable range without reverting, expressed as:

$$\exists t_0 \text{ such that } S(t_0) \neg\in [a, b], yet \lim_{t\to\infty}\big(S(t)\big) \neg\in [a, b]$$

This mathematical framing can be applied to robotic automotive systems, where the state $S(t)$ encompasses various elements including structural integrity, parametric integrity, external pressures, and the system's restorative force, each with its respective mathematical representation and constraints.

Challenges Posed by SCOMs

Super-Critical Operational Modes pose a set of unique challenges, particularly in automotive systems:

- Structural Integrity: The critical challenge is maintaining the system's structural integrity, represented by $S(t)$, during super-critical states. When structural integrity is entirely lost ( $S(t) = 0$), the system is non-functional.
- Parametric Integrity: Ensuring parametric integrity, denoted as $C(t)$, is equally crucial. Parametric integrity is sensitive to external pressures and needs constant monitoring and control to prevent the system from entering a super-critical state.
- External Pressures: The system is often exposed to varying external pressures, $P(t)$ , which can unpredictably affect both structural and parametric integrity, pushing the system towards a super-critical state.
- Restorative Forces: Applying appropriate restorative forces, $R(t)$, is a significant challenge, as it requires precise calculation and application to prevent the system from going super-critical.
- Functional State: The overall functional state of the system, $F(t)$, is the product of its structural and parametric integrity. Monitoring and maintaining a balanced functional state is pivotal to prevent entering super-critical states.

**Necessity of SCOMs in Automotive Systems. Relationship Between SCOMs and System Requirements.**

As is well-known, the ISO 26262 standard comprehensively addresses the issues of functional safety in the automotive sector. At the core of the standard is the ASIL (Automotive Safety Integrity Level) classifier of functional hazard, which is defined within the range of ASIL A, B, C, and D, as well as systems that are not safety-related and are characterized as quality management (QM). Primarily, the determination of the ASIL level is based on the risk of human injury in the event of system failure under evaluation. In contrast, SCOMs do not consider this risk as a unit of measurement. Instead, they take into account the functional integrity of the vehicle and its ability to continue operating.

From the perspective of requirements, SCOMs (Super-Critical Operational Modes) requirements are on the system level. They must be decomposed into software and hardware requirements for further development and testing. Additionally, they contribute to the collective documentation regarding the system behavior in super-critical modes. This documentation forms a section of the product's architectural description.

Requirements for SCOMs are characterized by the automation of decision-making regarding system management, system reconfiguration, and access to diagnostic interfaces. From a hardware standpoint, SCOMs have requirements for additional equipment, such as backup systems, communication devices, and the like. These specifications ensure that the vehicle can efficiently and effectively respond to and operate in super-critical situations, minimizing risks and maximizing the potential for system recovery and continuity of operation.

## PROPOSED CLASSIFICATION OF SUPER-CRITICAL OPERATIONAL MODES

### Classification Criteria.

Super-Critical Operational Modes can be classified using several criteria, reflecting their intensity, impact, and the complexity of the recovery process. The proposed classification includes:

- Intensity Level: This criterion measures how far the system deviates from its standard operational parameters. Intensity is categorized into mild, moderate, and severe, based on the extent of deviation and the potential risk involved[10].
- Impact Scale: It quantifies the degree of damage or disruption the SCOM can cause to the system and its environment. The impact scale can be minimal, substantial, or critical[11].
- Recovery Complexity: This categorizes SCOMs based on the difficulty and resources required to bring the system back to normal operation, ranging from low to high complexity.

### SCOM Classification Types.

Based on the criteria above, SCOMs can be divided into three primary types:

1. Type I – Mild Intensity:
   - Intensity Level: Mild
   - Impact Scale: Minimal
   - Recovery Complexity: Low
   - Description: Type I SCOMs are minor operational anomalies, recoverable through automated internal solutions without external intervention.
2. Type II – Moderate Intensity:
   - Intensity Level: Moderate
   - Impact Scale: Substantial
   - Recovery Complexity: Medium
   - Description: Type II SCOMs involve significant system deviations leading to partial failures. Recovery necessitates advanced, fully automated internal procedures, activating specialized response mechanisms for a seamless transition back to normal operation without external guidance or intervention.
3. Type III – Severe Intensity:
   - Intensity Level: Severe
   - Impact Scale: Critical
   - Recovery Complexity: High
   - Description: Type III SCOMs entail drastic deviations with the approach emphasizing automatic diagnostics, analysis, and internal system restructurization. The system autonomously engages in self-diagnosis, internal analysis, and initiates restructuring processes to restore functionality, minimizing reliance on external intervention.

### Application in Automotive Systems.

In automotive systems, these classifications can be mapped to real-world operational challenges. For instance:

- Type I SCOMs: Issues like software glitches or sensor malfunctions are rectifiable through system reboots or automated self-correction mechanisms.
- Type II SCOMs: Challenges such as partial system failures or major software bugs are addressed through advanced automated internal recovery procedures, eliminating the need for external involvement.
- Type III SCOMs: Catastrophic failures initiate a sequence of self-diagnosis, comprehensive internal analysis, and automatic restructuring to recover functionality autonomously without external interventions.

**SCOM Classification Calculation.**

The Criteria Definition and Criteria Quantification for SCOM are defined in Table 1 and Table 2, respectively.

**Table 1.** Criteria Definition

| Criteria Name | Criteria Description |
|---|---|
| Intensity Level (IL) | Degree of deviation from normal operational parameters |
| Impact Scale (IS) | Degree of potential damage or disruption caused to the system or its environment |
| Recovery Complexity (RC) | Resources and effort needed for system recovery |

**Table 2.** Criteria Quantification

| Criteria | Min.Value | Med.Value | Max.Value |
|---|---|---|---|
| Intensity Level (IL) | Mild: 1-3 | Moderate: 4-6 | Severe: 7-10 |
| Impact Scale (IS) | Minimal: 1-3 | Substantial: 4-6 | Critical: 7-10 |
| Recovery Complexity (RC) | Low: 1-3 | Medium: 4-6 | High: 7-N/A |
| Occurrence Probability | Events that are highly unlikely to happen or happen very infrequently. Example: Once in every 100,000,000 runs. | Events that are not common but have been known to happen occasionally. Example: Once in every 10,000,000 runs. | Events that happen more frequently and are somewhat expected to occur during the system's lifecycle. Example: Once in every 1,000,000 runs. |

SCOM Classification Formula: $SCI = w_1 \cdot IL + w_2 \cdot IS + w_3 \cdot RC$, where $w_1, w_2, w_3$ are the weights assigned to each criterion reflecting their importance. Ensure that $w_1 + w_2 + w_3 = 1$.

Classification Thresholds:

Define threshold values for each type:

- Type I: $SCI \leq T1$
- Type II: $T1 < SCI \leq T2$
- Type III: $SCI > T2$

## CONCLUSION

Through this significant research, we have unveiled and elaborated on the concept of Super-Critical Operational Modes in automotive systems. This is crucial as the industry continues to move towards software-centric functionalities.

We've introduced SCOMs as vital for navigating severe operational anomalies while ensuring vehicle safety and longevity. A nuanced classification system for SCOMs has been proposed, dividing them into Type I (Mild), Type II (Moderate), and Type III (Severe) intensities. Each type of SCOM is defined by its intensity level, impact scale, and recovery complexity.

For Type III SCOMs, we advocate for an innovative approach focused on automatic diagnostics, analysis, and internal system restructuring. This method reduces the need for external intervention, promoting the development of resilient, autonomous, and safe automotive systems. We have also developed a mathematical framework for the quantitative classification of SCOMs. This framework integrates criteria like intensity level, impact scale, and recovery complexity, each with defined value ranges, and considers the probability of occurrence to provide a comprehensive perspective on each SCOM's risk and severity.

This research significantly enhances practitioners' understanding and offers systematic mitigation strategies for operational anomalies in automotive systems. The adoption of the proposed classification and approach enables engineers and developers to proactively identify, analyze, and respond to SCOMs. This proactive approach leads to the creation of robust and self-reliant automotive systems and aids in the decision-making process during both the development and operational phases, ensuring efficient resource allocation and effective response strategies.

Future research should focus on developing and validating recovery strategies for each SCOM type, integrating these insights into standard procedures within the industry. Further refinement and expansion of the SCOM classification model are necessary to accommodate technological advancements and emerging operational challenges in automotive systems. Empirical studies should also be conducted to validate and refine the proposed SCOM classification model and the associated recovery strategies, ensuring their efficacy and reliability in real-world automotive operational contexts.

We would like to express our gratitude to all contributors and experts whose foundational work and insightful comments have significantly enriched this research. Special thanks are also extended to our peers for their invaluable feedback and constructive critiques during the development of this paper.

This paper profoundly contributes to literature and practice in the field of automotive system development by exploring and establishing the definitions and classifications of SCOMs. The insights and framework provided guide current practitioners and lay a solid foundation for future research and development initiatives aimed at enhancing the safety, resilience, and efficiency of automotive systems in facing super-critical operational scenarios.

## REFERENCES

1. **Bekey, G. A.** (2017). Autonomous Robots: From Biological Inspiration to Implementation and Control. Cambridge, MA: MIT Press, Intelligent Robotics and Autonomous Agents series.
2. **Humennyi, D., Kozlovskyi, V., Nimchenko, T., & Shestak, Y.** (2022). Cumulative Coverage of the Simulink-based MIL Unit Testing for Application Layer of Automotive. In Y. Khlaponin, E. Corrigan, & M. Karpinski (Eds.), CEUR Workshop Proceedings, 3149 (pp. 163-168). CEUR-WS.
3. ISO 26262: Road vehicles – Functional safety (2nd ed., pp. page numbers). Geneva, Switzerland: ISO
4. **Lerman, Kristina**, et al. "Analysis of dynamic task allocation in multi-robot systems." The International Journal of Robotics Research 25 .3 (2006): 225-241.
5. **Na, Jing**, et al. "Robust adaptive finite□time parameter estimation and control for robotic systems." International Journal of Robust and Nonlinear Control 25.16 (2015): 3045-3071.
6. **Goodwin, Walter**, et al. "Semantically grounded object matching for robust robotic scene rearrangement." 2022 International Conference on Robotics and Automation (ICRA). IEEE, 2022.
7. **Tkach M.** "Return from Falling and Stabilization of Antropomorphiv Walking Robot nearby Stability Boundary." (2015).
8. **Ostapchenko, K., O. Lisovychenko, and V. Evdokimov.** "Functional organization of system of support of decision-making of organizational management." (2020).
9. **Von Neumann, John.** "Probabilistic logics and the synthesis of reliable organisms from unreliable components." Automata studies 34 (1956): 43-98.
10. Certification of Safety-Critical Systems By **Nancy G. Leveson, John P. Thomas** Communications of the ACM, October 2023, Vol. 66 No. 10, Pages 22-26 10.1145/3615860.
11. **Abdelgawad, M., Ray, I., Vasquez, T.** (2023). Workflow Resilience for Mission Critical Systems. In: Dolev, S., Schieber, B. (eds) Stabilization, Safety, and Security of Distributed Systems. SSS 2023. Lecture Notes in Computer Science, vol 14310. Springer, Cham. https://doi.org/10.1007/978-3-031-44274-2_37.

## Встановлені визначення надкритичних режимів роботи як вимог до автомобільної системи

*Дмитро Гуменний, Олександр Гуменний*

**Анотація**. Ця робота детально вивчає Супер-Критичні Операційні Режими (СКОР) у автомобільних системах, які стали ключовими у сучасній автомобільній індустрії, орієнтованій на програмне забезпечення. Вона досліджує концепцію СКОР, їх класифікацію та необхідність інтеграції в системні вимоги. Протягом останніх п'ятнадцяти років індустрія пережила зміну орієнтації з апаратного забезпечення на програмне. Ранні етапи розробки включають детальний опис системних вимог, що є важливим для визначення архітектурного дизайну, розробки компонентів, тестування та процесів документації. СКОР в автомобільних системах означають екстремальні умови експлуатації, що перевищують стандартні критичні сценарії, та мають велике значення для безпеки та надійності. СКОР відрізняються від стабільних та критичних станів за допомогою математичних та графічних представлень, вони впливають на структурну та параметричну цілісність системи. СКОР відрізняються від вимог до функціональної безпеки, вони зосереджуються на функціональній цілісності та оперативній безперервності транспортного засобу. Класифікація СКОР базується на інтенсивності, впливі та складності відновлення. Вона відповідає реальним операційним викликам, що варіюються від невеликих збоїв програмного забезпечення до катастрофічних системних збоїв. Висновок: вивчення СКОР у автомобільних системах є важливим для просування безпеки та функціональності транспортних засобів.

**Ключові слова:** Автомобільна Платформа, Супер-Критичні Операційні Режими, Адаптивність, Інженерія Вимог, Системні Специфікації