

ICS 13.200

**Stresstest der Resilienz von kritischen Infrastrukturen, die
cyber-physischen Bedrohungen ausgesetzt sind;
Text Englisch**

Stress-testing resilience of critical infrastructures exposed to cyber-physical threats;
Text in English

Tests de résistance des infrastructures critiques exposées aux menaces cyberphysiques;
Texte en anglais

Gesamtumfang 35 Seiten

Dieses Dokument wurde durch die im Vorwort genannten Verfasser erarbeitet und verabschiedet.

Contents

	Page
Foreword	4
Introduction.....	5
1 Scope	6
2 Normative references	7
3 Terms and definitions.....	7
4 Symbols and abbreviations.....	9
5 Resilience stress-testing	10
5.1 Context and definition	10
5.2 Principles.....	11
6 Resilience stress-testing framework.....	12
6.1 Integrating top-down and bottom-up approaches.....	12
6.2 Main stakeholders (“interested parties”)	12
6.3 Basic methodology.....	15
6.4 Stress-testing criteria.....	16
6.5 Level of functionality (“vertical loss”).....	16
6.6 Time (“horizontal loss”).....	17
6.7 Cumulative loss of functionality (area)	18
7 Stress-testing workflow	19
7.1 General	19
7.2 Pre-testing phase.....	19
7.3 Stress-testing phases.....	21
7.3.1 Preparation phase.....	21
7.3.2 Testing phase	21
7.3.3 Closing phase.....	21
7.4 Post-testing phase	21
8 Resilience stress-testing implementation.....	22
8.1 Implementation principles	22
8.2 Stress-testing process	22
9 Resilience indicators used in stress-testing	27
10 Stress-testing reporting	27
11 Target users of the stress-testing results	28
Annex A (informative) Application Example.....	29
A.1 Title.....	29
A.2 Introduction.....	29
A.3 Virtual testbed	29
A.4 Application of a virtual testbed	31
A.5 Application in a case study.....	31
Bibliography	33

Figures

Figure 1 — The stress-testing framework: from regulation to tools.....	12
Figure 2 — The stress-testing process stakeholders	14
Figure 3 — Generic model of the functionality level of a SIP over a scenario time: the generic functionality level (FL) is defined through functional elements generally comprising resilience elements (e.g. preparedness), security elements (e.g. security protective measures), safety elements (e.g. safety protective measures) and critical functionality elements of the infrastructure (e.g. providing energy); for each element the single indicators should be defined	15
Figure 4 — Functionality level as stress-testing limit (up) and time as stress-testing limit (down)	17
Figure 5 — Loss of functionality surface as stress-testing limit.....	18
Figure 6 — Comparing the FL curve with the stress-testing criteria.....	19
Figure 7 — Stress-testing workflow	20
Figure 8 — Functionality elements and indicators (an example)	24
Figure 9 — Example of the functionality level over scenario time: the example shows fast drop of the FL (down to 25 %) and then fast recovery to almost nominal level (to approx. 95 %, within hours) with the final recovery to almost 97 % for over a month.....	25
Figure 10 — The figure depicts an example of stress-test for a critical infrastructure [20] showing the functionality during an adverse event/scenario (the scenario time in days). The details of the overall scenario cycle (above) are shown below. The pink curve represents the stress-test acceptance limits, the other curves represent the functionality levels of the respective individual subsystems. All the curves, except the computer network one, are within the stress-test acceptance limits.	26
Figure A.1 — High-level organization of the virtual-testbed.....	31
Figure A.2 — The critical process flow of the Carmagnani Pilot.....	32
Figure A.3 — Model of the Carmagnani critical process used in the virtual-testbed	32

Tables

Table 1 — Functionality elements and indicators	16
Table 2 — Examples of threats providing possible basis for stress-testing scenarios: will the system/infrastructure withstand the threat and recover according the pre-specified criteria	23

Foreword

This DIN SPEC has been developed according to the PAS procedure. The development of a DIN SPEC according to the PAS procedure is carried out in DIN SPEC-consortiums and does not require the participation of all stakeholders.

Results incorporated in this document received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088.

This document has been developed and adopted by the initiator(s) and authors named below:

- Chairperson: Prof. Aleksandar Jovanović, Steinbeis Advanced Risk Technologies, Germany
- Bundesamt für Sicherheit in der Informationstechnik, Germany, Andreas Erdrich
- CovIQ, Germany, Jan Seitz
- Consorzio Interuniversitario Nazionale Per L'informatica, Italy, Giovanni Mazzeo
- Engineering Ingegneria Informatica S.p.A, Italy, Lorenzo Sutton
- EU-VRi, European Risk and Resilience Institute, Germany, Mai Thi Nguyen
- German Commission for Occupational Health and Safety and Standardization (KAN), represented by German committee for operating safety (ABS), Christoph Thust
- INOV INESC Inovação — Instituto de Novas Tecnologias, Portugal, Gonçalo Cadete
- Jozef Stefan Institute, Slovenia, Prof. Marko Gerbec
- Satways Ltd., Greece, Dimitris Diagourtas, Dr. Souzanna Sofou
- Steinbeis Advanced Risk Technologies, Germany, Dr. Somik Chakravarty
- Studio QSA snc, Italy, Gennaro Bacile
- United Technologies Research Centre Ireland Ltd., Dr. Piotr Sobonski

The work was done with experts, active at UNI, Italy.

At present, there are no standards covering this topic in the body of German Standards.

DIN SPECs are not part of the body of German Standards.

A draft of this DIN SPEC has not been published.

Despite great efforts to ensure the accuracy, reliability and precision of technical and non-technical information, the DIN SPEC-consortium cannot give any explicit or implicit assurance or warranty in respect of the accuracy of the document. Users of this document are hereby made aware that the consortium cannot be held liable for any damage or loss. The application of this DIN SPEC does not release users from the responsibility for their own actions and is applied at their own risk.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. DIN shall not be held responsible for identifying any or all such patent rights.

Provision of this document free of charge as a PDF via the Beuth WebShop has been financed in advance.

For current information on this document, please go to DIN's website (www.din.de) and search for the document number in question.

Introduction

The term “stress-testing” has generally been used to describe the situation in which the performance of a system was exposed to the conditions (real or assumed ones, usually combined in the form of a scenario) bringing such systems (technical system, organization, society...) to its limits: exposed to a usually extreme stress, the system would be “tested” in the sense of meeting some criteria, in the extreme case testing its capability to “survive” these extreme conditions, i.e. scenario.

In the narrower, more technical sense, the term was often used for testing the survivability under the conditions not included in the design basis: some new changing conditions, new increasing exposure to hazards and threats, previously unrecognized possible harmful events, previously ignored risks are all the cases where it became very important to know if the system/organization will be up to the challenge. Examples of banks exposed to the crises like the one of 2008 or nuclear plants exposed to disasters like the Fukushima one, have increased the need to know if a system, or even more often a class of systems will “survive” and, possibly behave and function safely in the assumed scenario.

The good intention of answering the above question by means of stress testing faced, however, the issues of validity, comparability and repeatability of the testing. With many interests involved, it became essential that the “rules of the game” get aligned and, possibly agreed. In the context of increasing complexity of organizations, infrastructures, systems, technologies and society in general, risks such as, e.g., disruptive innovation, information overflow and/or indiscriminate use of new technologies, the issue has become even more important.

This document supports the above efforts to improve and enhance the capability to better anticipate and manage the unexpected challenges of the future in particular for:

- critical infrastructure (critical entities¹) and
- cyber, cyber-physical and other new threats (emerging risks).

This document will thus contribute towards attaining consistency in risk and resilience management approaches towards emerging risks in different EU countries, across different organizations and across different types of activities and sectors.

As the case with other standards and pre-standardization documents, this document is intended to be used in the respective applicable national and EU framework of regulatory documents and as such

- 1) It differentiate between the facilities that pose a risk to life, limb and the environment and critical infrastructures in conceptual terms (in fact defined as “critical entities” in the new EU CER Directive [1]);
- 2) It does not concern, affect or supersede any organizational responsibilities in the area of occupational health and safety, or other related areas, and
- 3) It assumes that the stress-testing needs sufficient involvement of the operators, authorities and testing organizations (e.g. in terms of the “colored teams”).

An application example is given in Annex A.

1 https://ec.europa.eu/home-affairs/system/files/2020-12/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf

1 Scope

This document provides a framework and guidelines for stress-testing industrial plants and sites (critical entities) against cyber-physical attacks. The background for the document is the work in the EU projects on DRS (Disaster Resilient Society), in particular the projects dealing with the resilience of critical infrastructures (entities), its assessment and stress-testing [e.g. [2] [3] and the projects members of the ECSCI cluster (European Cluster for Securing Critical Infrastructures)²].

This document defines the baseline for stress-testing the resilience of industrial plants and sites (critical entities, acc. to the new EU directive), including references, definitions and scope. It establishes/specifies principles of the stress-testing, defines the stress-testing framework (e.g. roles and responsibilities), proposes resilience assessment and stress-testing methods and indicators, as well as the process (procedure) in which these are used. The emphasis of the procedure is on the virtual-testbed based testing of the systems relevant for the security of the entities. These elements provide a de-facto guideline for the resilience stress-testing, including also guidance for the stress-testing results acceptance and reporting and communication.

This document is intended to be used by three main groups of stakeholders: the owners of critical entities (the “blue team”), the testing teams (“red team”) and the supervising bodies (the “white team”, e.g. authorities, e.g. in the case of the Seveso-entities, the “competent authorities” defined by the directive). The document is expected to be used also by the stress-testing service providers (including the IT-security and resilience analysis specialist) as the cornerstone reference, similarly to the TIBER-EU [4] guideline applied in the financial sector.

One of the main objectives of this document is to support ensuring security in the case of critical entities in terms of:

- enhanced cyber resilience;
- harmonized way of how entities will perform stress-tests;
- thereby improve the process of stress-testing in entities and fostering mutual recognition of stress-testing across the EU.

The main elements of this document will be:

- the organizational aspects (e.g. creation of teams) and
- the procedural aspects.

This document may be of a particular relevance for the areas such as security, risk and resilience analysis, health and environmental protection, management systems, especially in combination with extended use of information technology, digitalization, smart systems, AI and similar technologies (e.g. with smart manufacturing).

This document does not apply and is not intended to be used as a replacement for any applicable security related regulations and standards. It provides additional information and transparency. This document does not apply to machinery. This document does not define occupational safety and health.

2 <https://www.cyberwatching.eu/projects/2159/infrastress/news-events/european-cluster-securing%C2%A0critical-infrastructure%C2%A0ecsci-workshop>

It is confirmed that, despite the need of clarity many of the important issues around the stress-testing – e.g. in the field of regulations, for instance related to who would be issuing the request for test-testing, it is important to start working on the topic of stress-testing of resilience of critical infrastructures exposed to cyber-physical threats. However, when doing so, this document

- a) should be understood as one of the initial steps (only!) in the proactive discussions about the stress-testing among all the interested parties,
- b) should be clearly understood as a document which will “be developed further” as full consensus based standard, and
- c) should evolve as a document developed under the clear premise of respecting and supporting current regulation and established practices.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Security and resilience — Vocabulary*

ISO 31073³, *Risk management — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 31073 and ISO 22300 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

DIN and DKE maintain terminological databases for use in standardization at the following addresses:

- DIN-TERMinologieportal: available at <https://www.din.de/go/din-term>
- DKE-IEV: available at <http://www.dke.de/DKE-IEV>

3.1

emerging risk

highly uncertain risk which is developing with potential for serious consequences/impacts

Note 1 to entry: Risk is as defined in ISO 31000.

Note 2 to entry: The term “developing” refers to changes in the risk understanding related to risk sources, events, effects/consequences, likelihood and/or background knowledge.

[SOURCE: ISO/WD 31050, 3.1]

3 Currently under development.

3.2

organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO 14001:2015, 3.1.4]

3.3

resilience

ability to absorb and adapt in a changing environment

Note 1 to entry: In the context of urban resilience the ability to absorb and adapt to a changing environment is determined by the collective capacity to anticipate, prepare and respond to threats and opportunities by each individual component of an urban system.

[SOURCE: ISO 22300:2021, 3.1.206]

3.4

resilience attribute

features or characteristics of an organizations ability to absorb and adapt in a changing environment

[SOURCE: ISO/WD 31050, 3.7]

3.5

resilience indicator

measurable variable, quantitative or qualitative, that can be used to describe the ability of an entity to absorb and adapt in a changing environment

Note 1 to entry: In the context of critical infrastructures the resilience indicators are able to represent the capacity of an infrastructure to anticipate, prepare and respond to threats and opportunities it is susceptible to.

Note 2 to entry: In the context of stress testing activities for critical infrastructures specific resilience indicators are used to describe the capacity of an infrastructure to anticipate, prepare and respond to cyber-physical threats it is exposed to.

3.6

risk

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

[SOURCE: ISO 31000:2018, 3.1]

3.7

system

combination of interacting elements organized to achieve one or more stated purposes

Note 1 to entry: A system is sometimes considered as a product or as the services it provides.

Note 2 to entry: In practice, the interpretation of its meaning is frequently clarified by use of an associative noun, e.g. aircraft system. Alternatively, the word “system” is substituted simply by a context-dependent syndrome, e.g. aircraft, though this potentially obscures a system principles perspective.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.46, modified — Note 3 to entry has been removed.]

4 Symbols and abbreviations

AI	Artificial intelligence
BI	Business intelligence
BT	Blue team
C/P	Cyber/Physical
CI	Critical Infrastructure
CPS	Cyber-Physical Systems
DCL	Dynamic checklist
EC	European Commission
ERRA	European risk and resilience assessment and rating initiative
EU	European Union
FE	Functionality elements
FI	Functionality indicator
GUI	Graphical User Interface
ICS	Industrial Control System
IT	Information Technology
MTU	Master Terminal Unit
OT	Operational Technology
PDCA	“Plan-do-check-act” cycle
RT	Red team
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SIPS	Sensitive Industrial Plants and Sites
SWOT	Strength-weakness-opportunity-threat
WT	White team

5 Resilience stress-testing

5.1 Context and definition

The main idea for stress-testing in the area of critical infrastructures comes from the nuclear industry (see the ENSREG Declaration [5]), where the politics required that European nuclear power plants be subjected to “stress tests” [6]. In the time after the Fukushima accident, the scenarios analyzed as the “beyond-compliance” ones were:

- earthquake;
- flood;
- station blackout;
- loss of offsite power;
- loss of service water supply;
- precautionary measures;
- accident management measures;
- aircraft crash;
- release of explosive and toxic gases in the vicinity of plants;
- effects of an accident in one power plant unit on the neighboring unit.

The term “stress-testing” is often defined as a re-assessment, done in order to see if the critical infrastructure will be able to meet the safety and/or other criteria setup for a given adverse event scenario, leaning on the definition of the stress-testing in the ENSREG Declaration [5].

The definition of the resilience stress-testing of a critical infrastructure/entity:

A dedicated and targeted re-assessment of the system/SIPS resilience based on real, realistic or assumed scenarios initiated by the selected adverse event(s)/threat(s), with the goal to check and verify if the critical infrastructure will be able to meet the safety, security and/or other criteria setup for that scenario and measured in terms of the resilience (preferably macro) indicators.

*NOTE In practical terms, it examines how (critical) infrastructures/entities react or would react to the scenario-based threats and measures resilience indicators, to check and verify if the critical infrastructure will be able to meet the safety and/or other criteria (e.g. the ability to continue baseline operations) defined for such a scenario. The resilience indicators are interpreted based on a dedicated/customized resilience scale and resilience phase model. The result of the stress-testing should be defined on the “successfully passed <-> failed” scale and supported by the recommendations on the **SWOT** matrix [7], **PDCA** cycle [8] [9], and classified (e.g. according to the 5 phases of the resilience cycle [3]).*

Stress-testing helps to provide the end-users with an instrument to check how their critical infrastructures will or would react to a threat scenario based on assumed, “known” or “unknown” threats.

Especially the “unknown” threats can make the SIPS exposed to new risks, which can emerge from long-standing issues, due to thresholds suddenly being crossed. This means that the number of hazards leading to a risk may be growing, or that the exposure to the hazard leading to the risk is increasing, or that the effects/impacts of the hazards getting worse (e.g. seriousness of effects and/or the number of people affected) beyond what is or was considered acceptable. Risks can also emerge through a difference in estimation, e.g. due to a change in social or public perceptions or due to new scientific knowledge.

These new, previously unknown or not considered, emerging risks can pose considerable challenges to resilience, safety, security and operational and business continuity. These “new and/or increasing” risks can be related to different areas of activities, such as new processes, new technologies, new types of workplace, or social or organizational change.

The emerging risks can also come from the side of long-standing issues, now newly considered as a risk due to a change in social or public perceptions or due to new scientific knowledge. This can mean for these risks e.g., that the number of hazards leading to the risk may be growing, or that the exposure to the hazard leading to the risk is increasing, or that the effects/impacts of the hazards are getting worse (e.g. seriousness of effects and/or the number of people affected).

The emerging risks may interrelate with the processes like globalization, digitalization, innovation, cross-boundary operations and they can, directly or indirectly, influence each other, being interconnected, systemic and/or interdependent. In this context, the world can be considered as one complex system, as a de-facto global “infrastructure-of-infrastructures”.

New possibilities to deal with emerging risks (e.g. use of social media and/or crowd sensing), may improve the resilience of a system, but might also interact with emerging risks in unexpected ways and become part of them. They can, at the same time, both increase and decrease the level of trust in process of managing the “unknown futures”. New technologies and solutions will help only if they are well accepted by society and perceived as fair, transparent and well-being oriented. Mistrust or lack of confidence, lack of fairness and/or transparency of innovation can damage or even stop the innovation in a particular field.

5.2 Principles

The approach proposed in this document suggests the following main principles of resilience stress-testing:

- 1) Ensuring alignment and compliance with existing and latest EU and national regulations (e.g. EU Directive [10] [11] [12] [13], ISO 22300, ISO 22301, ISO 22316, ISO 22328-1, ISO 31000 and ISO/WD 31050, and/or TIBER-EU [4]).
- 2) Considering extreme uncertainties and emerging risks in stress-testing of resilience.
- 3) providing proof that the CI is able to withstand the conditions imposed by the stress-testing conditions as the main goal. The success and the proof of success should be defined upfront.
- 4) The testing process (8.2) should be suitable for use by both small and large organizations (see 3.2, including SMEs), and shall use appropriate and agreed indicators (Clause 9).
- 5) The approach should use accepted methods and tools (Clause 8) in the stress-testing process (8.2); the methods and tools should be leveraged to conduct an accurate stress testing phase that can simulate the real event/alarming condition. It should be aligned and possibly compatible with other recognized principles used in the area, such as application of precautionary principles, ALARP⁴.
- 6) The approach foresees the use of resilience indicators (Clause 9) for the definition of the success criteria of the stress-testing. The indicators should be agreed and aligned.
- 7) Reporting (Clause 10) should be accepted by all interested parties (Clause 11). The stress-testing results should be comparable, transparent and possibly usable for benchmarking.

4 <https://www.hse.gov.uk/managing/theory/alarpglance.htm>