DIN SPEC 91461:2021-12 (E)

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

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