

# DIN EN ISO 11073-40101:2022-07 (E)

## Health informatics - Device interoperability - Part 40101: Foundational - Cybersecurity - Processes for vulnerability assessment (ISO/IEEE 11073-40101:2022); English version EN ISO/IEEE 11073-40101:2022

---

### Contents

	Page
1. Overview .....	11
1.1 General .....	11
1.2 Scope .....	12
1.3 Purpose .....	12
1.4 Word usage .....	12
2. Definitions, acronyms, and abbreviations .....	13
2.1 Definitions .....	13
2.2 Acronyms and abbreviations .....	13
3. Risk management .....	13
4. Software of unknown provenance .....	14
5. Multi-component system vulnerability assessment .....	14
6. Threat modeling.....	14
6.1 General .....	14
6.2 Data flow diagram .....	15
6.3 STRIDE classification scheme .....	15
7. Scoring system .....	15
7.1 General .....	15
7.2 CVSS .....	15
7.3 eCVSS .....	16
8. Process for vulnerability assessment .....	17
8.1 Iterative vulnerability assessment .....	17
8.2 System context.....	17
8.3 System decomposition .....	20
8.4 Scoring .....	22
8.5 Mitigation .....	24
8.6 Iteration.....	24
Annex A (informative) Bibliography .....	25
Annex B (informative) STRIDE.....	26
Annex C (informative) embedded Common Vulnerability Scoring System .....	30
C.1 Overview.....	30
C.2 Scoring equations in pseudo code .....	35
C.3 Test vectors .....	36
Annex D (informative) Microsoft TMT2Excel Macro.....	37
Annex E (informative) Example insulin delivery device vulnerability assessment.....	40
E.1 General .....	40
E.2 System context .....	40
E.3 Threat model .....	41
E.4 Pre- and post-mitigation vulnerability assessment scores .....	42