

DIN EN ISO 19014-4:2021-01 (E)

Earth-moving machinery - Functional safety - Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system (ISO 19014-4:2020)

Contents		Page
European foreword		3
Foreword		4
Introduction		5
1	Scope	6
2	Normative references	6
3	Terms and definitions	6
4	Software development	9
4.1	General	9
4.2	Planning	10
4.3	Artifacts	11
4.4	Software safety requirements specification	12
4.5	Software architecture design	13
4.6	Software module design and coding	13
4.7	Language and tool selection	14
4.8	Software module testing	15
4.9	Software module integration and testing	16
4.10	Software validation	17
5	Software-based parameterization	17
5.1	General	17
5.2	Data integrity	18
5.3	Software-based parameterization verification	18
6	Transmission protection of safety-related messages on bus systems	18
7	Independence by software partitioning	19
7.1	General	19
7.2	Several partitions within a single microcontroller	20
7.3	Several partitions within the scope of an ECU network	21
8	Information for use	22
8.1	General	22
8.2	Instruction handbook	22
Annex A (informative) Description of software methods/measures		23
Annex B (normative) Software validation test environments		36
Annex C (informative) Data integrity assurance calculation		39
Annex D (informative) Methods and measures for transmission protection		41
Annex E (informative) Methods and measures for data protection internal to microcontroller		43
Bibliography		45