

# DIN EN 16590-2:2014-11 (E)

## Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 2: Concept phase (ISO 25119-2:2010 modified)

---

<b>Contents</b>		<b>Page</b>
Foreword .....		5
Introduction .....		6
1	Scope .....	8
2	Normative references .....	8
3	Terms and definitions .....	8
4	Abbreviated terms .....	8
5	Concept -- Unit of observation .....	9
5.1	Objectives .....	9
5.2	Prerequisites .....	9
5.3	Requirements .....	9
5.3.1	Unit of observation and ambient conditions .....	9
5.3.2	Limits of unit of observation and its interfaces with other units of observation .....	10
5.3.3	Sources of stress .....	10
5.3.4	Additional determinations .....	10
5.4	Work products .....	11
6	Risk analysis and method description .....	11
6.1	Objectives .....	11
6.2	Prerequisites .....	11
6.3	Requirements .....	11
6.3.1	Procedures for preparing a risk analysis .....	11
6.3.2	Tasks in risk analysis .....	11
6.3.3	Participants in risk analysis .....	11
6.3.4	Assessment and classification of a potential harm .....	11
6.3.5	Assessment of exposure in the situation observed .....	12
6.3.6	Assessment of a possible avoidance of harm .....	12
6.3.7	Selecting the required AgPLr .....	13
6.4	Work products .....	15
7	System design .....	15
7.1	Objectives .....	15
7.2	Prerequisites .....	15
7.3	Requirements .....	15
7.3.1	Assignment of AgPL .....	15
7.3.2	Achieving the required AgPLr .....	16
7.3.3	Achievement of the performance level .....	17
7.4	Work products .....	17
Annex A (normative)	Designated architectures for SRP/CS .....	18
A.1	General .....	18
A.2	Category B (basic) .....	18
A.3	Category 1 .....	19
A.4	Category 2 .....	19
A.5	Category 3 .....	20

<b>A.6</b>	<b>Category 4</b> .....	<b>22</b>
<b>Annex B (informative) Simplified method to estimate channel MTTFdC</b> .....		<b>24</b>
<b>B.1</b>	<b>General</b> .....	<b>24</b>
<b>B.2</b>	<b>Component MTTFd values</b> .....	<b>24</b>
<b>B.2.1</b>	<b>Determination of component MTTFd values</b> .....	<b>24</b>
<b>B.2.2</b>	<b>MTTFd for components from B10</b> .....	<b>25</b>
<b>B.3</b>	<b>Parts count method</b> .....	<b>25</b>
<b>B.4</b>	<b>Calculation of symmetric MTTFdC for two-channel architectures</b> .....	<b>26</b>
<b>Annex C (informative) Determination of diagnostic coverage (DC)</b> .....		<b>27</b>
<b>C.1</b>	<b>General</b> .....	<b>27</b>
<b>C.2</b>	<b>Estimation of the required DC</b> .....	<b>27</b>
<b>C.3</b>	<b>Estimation of channel DC</b> .....	<b>29</b>
<b>C.4</b>	<b>Calculation of channel DC</b> .....	<b>30</b>
<b>C.5</b>	<b>Calculation of DC</b> .....	<b>30</b>
<b>Annex D (informative) Estimates for common-cause failure (CCF)</b> .....		<b>31</b>
<b>Annex E (informative) Systematic failure</b> .....		<b>33</b>
<b>E.1</b>	<b>General</b> .....	<b>33</b>
<b>E.2</b>	<b>Procedure for the control of systematic failures</b> .....	<b>33</b>
<b>E.3</b>	<b>Procedure for the avoidance of systematic failures</b> .....	<b>33</b>
<b>Annex F (informative) Characteristics of safety functions</b> .....		<b>36</b>
<b>F.1</b>	<b>General</b> .....	<b>36</b>
<b>F.2</b>	<b>Start interlock</b> .....	<b>36</b>
<b>F.3</b>	<b>Stop function</b> .....	<b>36</b>
<b>F.4</b>	<b>Manual reset</b> .....	<b>36</b>
<b>F.5</b>	<b>Start and restart</b> .....	<b>37</b>
<b>F.6</b>	<b>Response time</b> .....	<b>37</b>
<b>F.7</b>	<b>Safety-related parameters</b> .....	<b>37</b>
<b>F.8</b>	<b>External control function</b> .....	<b>37</b>
<b>F.9</b>	<b>Muting (manual suspension of safety functions)</b> .....	<b>37</b>
<b>F.10</b>	<b>Operator warning</b> .....	<b>37</b>
<b>Annex G (informative) Example of a risk analysis</b> .....		<b>38</b>
<b>G.1</b>	<b>Workflow</b> .....	<b>38</b>
<b>G.2</b>	<b>Example risk analysis of an electro-hydraulic transmission for a self-propelled working machine (forage harvester) -- Extract from a complete risk analysis</b> .....	<b>38</b>
<b>G.2.1</b>	<b>System description</b> .....	<b>38</b>
<b>G.2.2</b>	<b>Surrounding conditions</b> .....	<b>39</b>
<b>G.2.3</b>	<b>System states and transitions</b> .....	<b>39</b>
<b>G.2.4</b>	<b>System failures</b> .....	<b>40</b>
<b>G.3</b>	<b>Assessment</b> .....	<b>41</b>
<b>G.3.1</b>	<b>System failure -- Stops unintentionally</b> .....	<b>41</b>
<b>G.3.2</b>	<b>System failure -- Does not move when commanded</b> .....	<b>42</b>
<b>G.4</b>	<b>Results</b> .....	<b>42</b>
<b>Annex ZA (informative) Relationship between this European Standard and the Essential Requirements of EU Machinery Directive 2006/42/EC</b> .....		<b>43</b>
<b>Bibliography</b> .....		<b>44</b>