Comparative analysis of the M-out-of-N structure in EN50129:2018 and IEC61508:2010

Yiwei Wang¹*, Yixuan Wang ², Lianchuan Ma ³, Jiakun Wen⁴ and Fan Zhang⁴

¹ School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, 100044, China
² School of Mathematics and Physics, University of Science & Technology Beijing, Beijing, 100083, China
³ National Engineering Research Center for Rail Transit Operation Control System, Beijing Jiaotong University, Beijing, 100044, China
⁴ Corresponding author’s e-mail: 19120254@bjtu.edu.cn

Abstract. By comparing and analysing EN50129:2018 and IEC 61508:2010, it is found that there are differences in the meaning of the M-out-of-N structure between these two standards. The reason for the differences lies in that the M-out-of-N structure definition of EN50129:2018 is based on the required functions, while the M-out-of-N structure definition of IEC 61508:2010 is based on the dangerous failures. The 2 out of 2 structure defined by EN50129:2018 is equivalent to the 1 out of 2 structure defined by IEC 61508:2010. The 2 out of 2 structure defined by IEC 61508:2010 is equivalent to the parallel redundancy or dual hot standby structure. Further, it is found that the formula given by EN50129:2018 is not as conservative as that given by IEC61508:2010.

1. Introduction

EN50129:2018[1] was approved by European Committee for Electrotechnical Standardization (CENELEC) in June 2018 and issued in November of the same year. This standard replaces EN50129:2003 and cancels CLC/TR50451:2007, CLC/TR50506-1:2007, CLC/TR50506-2:2009 and other documents. This standard emphasizes its consistency and compliance with EN61508 standard as one of the equivalent parts of railway communication, signal and processing system of EN61508 series (equivalent to IEC61508:2010). However, EN50129:2003[2] only emphasizes the consistency with EN61508-1 (equivalent to IEC61508-1:2001).

The importance of safety structure for railway signal safety related electronic system is self-evident. EN50129:2018 puts forward three ways for railway signal safety related electronic system to realize fail-safety principle: composition, reaction and inherent. Among them, composite fail-safety is the most common.

According to EN50129:2018, the realization of composite fail-safety principle is realized by M-out-of-N (MooN, N≥M,M≥2) redundancy, which means that in order to realize the composite fail-safety principle and reach the safety integrity level (SIL) SIL-4 index requirements, at least 2 out of 2 (2oo2) structure can be used. Of course, the 2 out of 2 structure here must use the composite fail-safety dual electronic structure with the fail-safety comparison or the diverse electronic structure based on the fail-safety comparison recommended in table E.4 of the appendix of this standard.

IEC61508:2010 series of standards [3, 4] does not give a complete and clear definition of
M-out-of-N (MooN) Channel architecture, but only states that it has a majority voter for detecting and shielding faults. Of course, the voter can accept external tests by itself or use self-monitoring technology. According to the calculation results given in IEC61508-6:2010, under the same conditions, the safety index parameters of 2 out of 2 structure are far lower than those of 1 out of 2 (1oo2), 2 out of 3 (2oo3) structure (about 1-2 orders of magnitude). In most cases, when the 1 out of 2 and 2 out of 3 structures meet the SIL-4 index requirements, the 2 out of 2 structures do not meet the SIL-4 index requirements.

Through the comparative analysis of EN50129:2018 and IEC61508:2010, it can be found that although they are both called 2 out of 2 structures, the meanings of the two standards are different, and the reasons behind the differences need to be given a comparative analysis. Therefore, this paper compares the definition of M-out-of-N structure in EN50129:2018 and IEC61508:2010, the calculation method of safety index and the numerical analysis of safety index to analyse the differences between the two standards on 2 out of 2 structure.

2. Comparison and analysis of structure definition of M-out-of-N in EN50129:2018 and IEC61508:2010

In the EN50129:2018, M-out-of-N structure redundancy, which is defined as: in the total N items, at least M items complete the function, so as to meet the requirements. M-out-of-N system is composed of N independent main items (EN 50129:2018 B.3.2.2 is written as M-out-of-N system has M main items), each main item can have one or more "additional items" to check the main items.

The standard clearly points out that under the composite fail-safety condition, each safety related function is executed by at least two items, and the nonrestrictive behavior can only be executed when the required numbers of items are consistent. Unrestricted state output adopts "AND" logic. Each item should have an independent failure detection and negation mechanism. For item X (or Y), this mechanism can be performed by item Y (or X). The failure of two items occurring at the same time may be dangerous, which is equivalent to giving a clear definition of 2 out of 2 structure.

Although the IEC61508:2010 series standard does not directly give a complete definition of M-out-of-N structure, it gives the definitions of 1 out of 2, 2 out of 2, 2 out of 3 and other structures [3].

Among them, the 1 out of 2 structure consists of two parallel connected channels, and any channel can handle safety functions. Both channels appear dangerous failure and the safety function fails on demand. This means that only when two channels appear dangerous failure, the safety function will fail. This structure needs to consider common cause failure.

2 out of 2 structure is composed of two parallel channels, both of which require safety function before safety function occurs. This means that if one of the two channels appears dangerous failure, the safety function will fail. This structure does not need to consider common cause failure.

2 out of 3 structure is composed of three parallel channels, and its output signal has majority vote arrangements. If only one channel output is different from the other two channels output state, the final output state will not change accordingly, so the structure needs to consider common cause failure.

It can be seen that the starting point of EN50129:2018's definition of M-out-of-N structure is the required function. However, the starting point of IEC61508:2010 for the definition of M-out-of-N structure is dangerous failure.

Theoretically, the failure of any electronic system can be further divided into "safe" failure and "dangerous" failure [5], and the failure rate $\lambda = \lambda_d + \lambda_s$. After the system fails, normal system functions will not be executed any more. However, if only a "safe" failure occurs, the system is still safe; only a "dangerous" failure occurs, the system is dangerous.

Of course, if the system failure is directly regarded as a dangerous failure, it is also feasible. At this time, it is equivalent to the system failure rate $\lambda = \lambda_d$, and there is no system safe failure, that is, the system safe failure rate $\lambda_s = 0$. This interpretation is suitable for
the railway signal safety related system. Because the railway signal safety related system not only needs to continuously and directly perform all system functions including the safety critical signal control function, but also must carry out safety protection for its own failure.

For the 1 out of 2 structure given in IEC61508:2010 series standards, there is the output logic shown in table 1.

| Channel A status | Channel B status | Output | Conclusion                     |
|------------------|------------------|--------|--------------------------------|
| Safety           | Safety           | Safety | For a dangerous failure:      |
|                  |                  |        | OR logic                      |
| Safety           | Danger           | Safety |                               |
| Danger           | Safety           | Safety |                               |
| Danger           | Danger           | Danger |                               |

According to the characteristics of normal function or safety failure of safety state, Make a logical decomposition of table 1 to get table 2.

| Channel A status | Channel B status | Output |
|------------------|------------------|--------|
| Functional normality | Functional normality | Functional normality |
| Functional normality | Safe failure    | Functional failure |
| Safe failure    | Functional normality | Functional failure |
| Safe failure    | Safe failure    | Functional failure |
| Functional normality | Dangerous failure | Functional failure |
| Safe failure    | Dangerous failure | Functional failure |
| Dangerous failure | Functional normality | Functional failure |
| Dangerous failure | Safe failure    | Functional failure |
| Dangerous failure | Dangerous failure | Functional failure |

Note that both safe failure and dangerous failure belong to failure. Simplify table 2 to get table 3.

| Channel A status | Channel B status | Output | Conclusion                   |
|------------------|------------------|--------|------------------------------|
| Function         | Function         | Function | For function:           |
| Function         | Failure          | Failure  | AND logic                   |
| Failure          | Function         | Failure  |                             |
| Failure          | Failure          | Failure  |                             |

It can be concluded that the 1oo2 structure given in IEC61508:2010 series of standards adopts “OR” logic for dangerous failure and adopts "AND" logic for function. The function here shall have the same meaning as the nonrestrictive behavior of "AND" logic output in EN50129:2018.

In the same analysis process, another conclusion can be drawn: the 2oo2 structure given in IEC61508:2010 series of standards adopts "AND" logic for dangerous failure and adopts “OR” logic for function.

In conclusion, according to the definition of the 2oo2 structure given in EN50129:2018, it can be found that the 2oo2 structure defined in EN50129:2018 is equivalent to the 1oo2 structure defined in IEC61508:2010 series standard. Further promotion, the NooN structure defined in EN50129:2018 is equivalent to the 1ooN structure defined in IEC61508:2010 series standards.
The 2oo2 structure defined in IEC61508:2010 series of standards is equivalent to the parallel redundancy or dual machine hot standby in Chinese context. Further promotion, the NooN structure defined in IEC61508:2010 series of standards is equivalent to parallel N-Modular redundancy or N-Modular hot standby.

3. Calculation method of hardware safety integrity in EN50129:2018 and IEC61508:2010

IEC61508:2010 defines low demand, high demand or a continuous mode [6], and EN50129:2018 clearly states the use of high demand or a continuous mode. For IEC61508:2010, the SIL quantitative index in high demand or a continuous mode is "the average frequency of a dangerous failure of the safety function \([h^{-1}]\)".

The calculation formula of PFH value of 1oo2 structure defined in IEC61508:2010 series standard is shown in equation (1):

$$PFH_G = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DD} \cdot tce + \beta \cdot \lambda_{DU})$$  \hspace{1cm} (1)

Among them, \(\beta\) is the fraction of undetected failures that have a common cause, \(\beta_D\) is the fraction of detected failures by the diagnostic tests that have a common cause \(\beta = 2\beta_D\).

\(\lambda_{DD}\) is the detected dangerous failure rate (per hour) of a channel in a subsystem, \(\lambda_{DU}\) is the undetected dangerous failure rate (per hour) of a channel in a subsystem, and the sum of them is the dangerous failure probability \(\lambda_D\) (per hour) of a channel in a subsystem, the total failure rate (per hour) of a channel in a subsystem \(\lambda = 2\lambda_D\).

$$\lambda_D = \lambda_{DD} + \lambda_{DU}$$  \hspace{1cm} (2)

\(\lambda_{DD}, \lambda_{DU}\) and \(\lambda_D\) satisfy the relationship shown in equation (3).

$$\begin{cases} \lambda_{DU} = \lambda_D(1 - DC) \\ \lambda_{DD} = \lambda_D \cdot DC \end{cases}$$  \hspace{1cm} (3)

\(tce\) is the channel equivalent mean down time (hour) in 1oo2 structure, as shown in equation (4):

$$tce = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{T_2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTR = (1 - DC)\left(\frac{T_1}{2} + MRT\right) + DC \cdot MTR$$  \hspace{1cm} (4)

Among them, \(T_1\) is the proof test interval (hour), \(MTR\) is the mean time to restoration (hour), and \(MRT\) is the mean repair time (hour).

EN50129:2018 defines the following basic formula for the asymptotic hazardous functional failure rate (FFR):

$$FFR \approx \frac{FR_A}{SDR_A} \times \frac{FR_A}{SDR_A} \times (SDR_A + SDR_B)$$  \hspace{1cm} (5)

It can be reduced to, when A and B are identical:

$$FFR \approx \frac{2FR^2}{SDR} = 2FR^2 \times SDT$$  \hspace{1cm} (6)

In equation (6), SDT refers to the safe down time (hour), which is equal to the reciprocal of SDR.

4. Comparative analysis of safety index values of 2oo2 structure in EN50129:2018 and 1oo2 structure in IEC61508:2010

For SIL quantitative indicators of the same level, the definitions of IEC61508:2010 and EN50129:2018 are the same. For example, SIL-4, quantitative indicators are \([10^{-9}, 10^{-8})\). Therefore,
PFH specified in IEC61508:2010 can be regarded as a part of FFR and basic parameter indicators specified in EN50129:2018.

Formula B.1 of functional failure rate (FFR) for its 2 out of 2 structure in Appendix B2.2.2 of EN50129:2018 is as shown in equation 5.

It can be seen that the standard implicitly treats the system failure as a dangerous failure, which indicates that it will be more conservative.

IEC61508:2010 series standards not only distinguish the dangerous failure rate $\lambda_D$ and safe failure rate $\lambda_S$, but also further distinguish the dangerous failure rate $\lambda_D$ into the detectable dangerous failure rate $\lambda_{DD}$ and the undetectable dangerous failure rate $\lambda_{DU}$.

The influence of common cause failure factor $\beta$ should be considered. The PFH value calculation formula of 1oo2 structure defined in IEC61508:2010 series standard is shown in equation (1).

When calculating the PFH value, $T_1$ in IEC6108-6:2010 is taken as 1 month, 3 months, 6 months and 12 months. Considering that the standard EN50129:2018 requires that SDT cannot be too long, $T_1$ is taken as 1 month, MTTR = MRT = 8h. $\lambda$ is $0.1 \times 10^{-6}, 0.5 \times 10^{-6}, 1 \times 10^{-6}, 5 \times 10^{-6}, 10 \times 10^{-6}$ and $50 \times 10^{-6}$ respectively. $\beta = 2 \times \beta_D$, since these formulas in EN50129:2018 do not consider common cause failure, only the minimum $\beta_D = \beta / 2 = 1\%$ is selected here. The diagnostic coverage (DC) is 0%, 60%, 90%, 99%. $\lambda_{DU} = \lambda_D(1-DC), \lambda_{DD} = \lambda_D \times DC, \lambda_D = \lambda / 2$.

When calculating the FFR value, $FR = \lambda$. Due to the difference between the two standards in the definition of the above time parameters, the process of obtaining SDT value is designed as follows: first, $t_{CE}$ is calculated according to the value of IEC61508-6:2010, then $SDT = t_{CE}$, and then the rationality is checked according to the SDT maximum value (shown in equation (5) or (6) obtained by formula B.6 in Appendix B3.3.2 of EN50129:2018. If $t_{CE}$ > maximum SDT value, $t_{CE}$ is replaced by the corresponding maximum SDT value.

\[
SDT \leq \frac{k}{1000(FR_D + FR_D)}
\]  

$k = 1$ for a 2 out of 2 system. The calculation results are shown in table 4.

| $\lambda = FR$ | DC | $t_{CE}$ (h) | $t_{CE}$ calculated according to the value of IEC61508:2010 | 2oo2 structure FFR value according to EN50129:2018 (SDT = $t_{CE}$) | maximum SDT value (h) according to formula B.6 in Appendix B3.3.2 of EN50129:2018 | Calculated value of FFR of 2oo2 structure in EN50129:2018 (corrected SDT + $\beta \times FR$) |
|----------------|----|--------------|-------------------------------------------------|------------------------------------------------|---------------------------------|-----------------------------------------------------------------|
| $0.1 \times 10^{-6}$ | 0% | 373          | 2.2E-06                                         | 7.46E-12                                           | 5000                           | 1E-10                                                            |
| $0.1 \times 10^{-6}$ | 60% | 154          | 8.8E-07                                         | 3.08E-12                                           | 5000                           | 1E-10                                                            |

Table 4. EN50129: 2018 2oo2 structure and IEC61508: 2010 1oo2 structure safety index value.
It can be found that $t_{CE} >$ maximum SDT value does exist (the value with gray fill in column 3 of table 4). Thus, its corresponding FFR value in column 5 of table 4 should also be replaced by the corresponding value in the column 7 of table 4, but the final FFR value is far less than the PFH calculation value (about 3-6 orders of magnitude). The main reason is that common cause failure is not considered in Formula B.1 of EN50129:2018, but in fact, figure A.5 of EN50129:2018 has given an example of the method of considering common cause failure. Even if the correction value of common cause failure $\beta \times FR$ is considered, it is still less than the calculated value of PFH given in IEC61508-6:2010 (about 1-3 orders of magnitude). The graphical results corresponding to table 4 are shown in figure 1.
5. Conclusion
In this paper, through the comparison and analysis of EN50129:2018 and IEC61508:2010 on the definition of M-out-of-N structure, safety integrity calculation method and numerical value, the following conclusions are drawn:

- The definition starting point of EN50129:2018 is the required function, while the definition starting point of IEC61508:2010 is the dangerous failure.
- The NooN structure defined in EN50129:2018 (i.e. N-out-of-N structure in Chinese context) is equivalent to the 1ooN structure defined in IEC61508:2010 series standards, while the NooN structure defined in IEC61508:2010 series standards is equivalent to parallel N-Modular redundancy or N-Modular hot standby in Chinese context.
- It is not appropriate for EN50129:2018 Formula B.1 not to consider common cause failure [7]. However, even if the common cause failure is considered, the FFR value is not conservative enough compared with the PFH calculated in IEC61508-6:2010 under the same conditions. It is recommended to use the methods of IEC61508:2010 series standards, or derivative methods such as PDS method [8-11], to calculate the safety index parameters.

- In order to distinguish whether the N out of M structure is for dangerous failure or for the required function, it is recommended to distinguish it in the subscript mode: the subscript DF represents for dangerous failure, that is, N is MDF, and the subscript F or SF represents for function or safety function, that is, N is MF or n is MSF.

Acknowledgments
This work is supported by National Key R&D Program of China under Grant (No.2016YFB1200602) and Beijing Laboratory of Urban Rail Transit.
References

[1] CENELEC. Railway applications-Communication, signaling and processing systems-Safety related electronic systems for signaling. EN 50129:2018[S].2018.

[2] CENELEC. Railway applications - Communication, signaling and processing systems-Safety related electronic systems for signaling. EN 50129:2003[S].2003.

[3] IEC. Functional safety of electrical/electronic/programmable electronic safety-related systems. IEC61508:2010 [S].2010.

[4] Hamid Jahanian. (2015).Generalizing PFD formulas of IEC61508 for KooN configurations. ISA Transactions.55:168-174.

[5] Lianchuan MA. (2017).Safety Design Technology of Train Control System. China Railway Publishing House, Beijing.

[6] Jianghong JIN. (2010).Assessment method for failure of a safety function for safety instrumented system. China University of Mining & Technology, 12: 23-72.

[7] Li HE, Jie CHEN, et al.(2014).Effect of Calculation Average Probability Failure on Common Cause Failure. Nuclear Power Engineering, 35(6):158-160.

[8] Per Hokstad, Solfrid Håbrekke, et al. (2009). Use of the PDS method for railway applications. Norway: SINTEF Technology and Society.

[9] Ying GAO. (2019). Research on Hardware Safety Integrity Level Verification Method of Train Control System. China Academy of Railway Sciences: 32-34, 61-64.

[10] Stein Hauge, Solfrid Håbrekke, et al.(2010).Reliability Prediction Method for Safety Instrumented Systems - PDS Example collection,2010 Edition. Norway: SINTEF Technology and Society.

[11] Hongyang ZHANG, Wu DUAN, et al. (2020). Computing Method of Probability Of a dangerous failure of Redundancy Structures of Railway Signal Based on PDS.Railway Standard Design, 64(4):1-8.