doi: 10.7690/bgzdh.2020.03.006

基于 IEC 61784-3 的 openSAFETY 残余错误率计算

王文俊，李彦平，骆云志
（中国兵器装备集团自动化研究所有限公司特种产品事业部，四川 绵阳 621000）

摘要：针对 IEC 61784-3 残余错误率扩展计算模型参考计算公式的应用受到极大限制的问题，提出相应改进建议。以 openSAFETY 为分析对象，结合其运行机理，在深入分析扩展计算模型中参考公式的原理后，提出对残余错误率扩展计算模型中计算公式的改进建议，并根据改进公式完成 IEC 61784-3 扩展计算模型下 openSAFETY 的安全完整性等级评估。结果表明：改进后的扩展计算模型对 openSAFETY 的残余错误率计算比原模型的适用性更强，结果更准确。

关键词：IEC 61784-3；openSAFETY；残余错误率
中图分类号：TP273　**文献标志码：**A

Residual Error Rate Calculation of openSAFETY Based on IEC 61784-3

Wang Wenjun, Li Yanping, Luo Yunzhi
(*Department of Special Product*, *Automation Research Institute Co*., *Ltd*. *of China South Industries Group Corporation*, *Mianyang* 621000, *China*)

Abstract: Aiming at the problem that the application of IEC 61784-3 residual error rate extended calculation model reference calculation formula is greatly limited, the corresponding improvement suggestions are put forward. Taking openSAFETY as the object of analysis, combined with its operation mechanism, after thoroughly analyzing the principle of reference formula in extended computing model, this paper puts forward suggestions for improving the calculation formula in extended computing model of residual error rate, and completes the security integrity evaluation of openSAFETY under IEC 61784-3 extended computing model according to the improved formula. The results show that the improved extended model is more applicable and accurate than the original model in calculating the residual error rate of openSAFETY.

Keywords: IEC 61784-3; openSAFETY; residual error rate

0　引言

在对可靠性有较高需求的控制系统中，对其通信系统的安全完整性等级（safety integrity level，SIL）提出相应要求，而残余错误率的计算结果对 SIL 评定有着决定性的影响。残余错误率的准确计算对通信系统可靠性设计具有指导性意义。

本课题来源于某反应堆仪控系统自定义通信协议安全数据单元帧格式设计及其安全完整性等级验证评估部分工作，需要对残余错误率作出准确计算。

IEC 61784-3 标准第 3 版公布后，残余错误率评估模型与之前发生较大变化，传统的残余错误率计算模型已不能准确评估 SIL，而目前对于新的扩展计算模型的相关研究甚少，仅有的参考文献介绍的计算公式也因通信模型、安全措施不同而不适用于本课题计算。

笔者选取与课题通信协议模型近似且已广泛使用的 openSAFETY 为研究对象，在深入研究其运行机理的情况下，结合 IEC 61784-3 标准的具体要求，提出对残余错误率扩展计算模型计算公式的改进建议，解决扩展计算模型计算公式对 openSAFETY 适用性问题，对其他工程应用中的残余错误率计算有较高参考意义。

1　openSAFETY 的安全帧格式

IEC 61784-3 中规定的数据传输错误主要有：数据损坏、（数据）非预期重复、数据乱序、数据丢失、不可接受的延迟、消息插入、伪装和寻址错误 8 种。这些错误的有效应对措施如表 1 所示。

openSAFETY 针对这些通信失效模式采用时间戳、时间预期、连接认证、数据完整性保证、冗余交叉校验和不同的数据完整性保证系统 6 种方式来保障通信功能的安全。根据表 1 内容，这些安全保障手段可以检测全部的常见失效模式。由这些保障措施设计的 openSAFETY 安全数据帧格式如图 1[1] 所示。

收稿日期：2019-11-16；**修回日期：**2019-12-13
作者简介：王文俊（1993—），男，江西人，硕士，从事通信协议方面研究。E-mail: wwjmike@qq.com。

表 1　各种措施对可能的错误有效性

通信错误	序列号	时间戳	时间预期	连接认证	消息反馈	数据完整性保证	冗余交叉校验	不同的数据完整性保证系统
数据损坏					×	×	仅串行总线用	
数据重复	×	×					×	
数据乱序	×	×					×	
数据丢失	×				×		×	
通信延迟		×	×					
消息插入	×	×		×	×		×	
伪装				×	×			×
寻址错误				×				

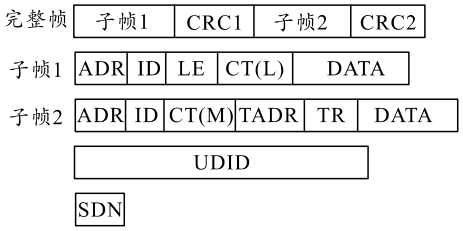

图 1　安全协议数据帧格式

其中：ADR 为地址字段，长 10 位，用于实现连接认证功能；ID 为帧识别字段，长 6 位，用于区别不同的帧类型；LE 为长度字段，长 8 位，用于描述负载数据(DATA)的字节长度；CT 为连续时间字段，长 16 位，高 8 位在子帧 2 中，低 8 位在子帧 1 中，记录网络内部时间，实现时间戳以及时间预期功能；DATA 为负载数据字段，长 0～8 字节(短帧)或 9～240 字节(长帧)，子帧 1 和子帧 2 的负载数据相互冗余，实现数据冗余交叉校验以及数据完整性保障功能；CRC 为 CRC 校验码字段，子帧 1 和子帧 2 有对应的 CRC 字段，长帧数据使用 CRC-16，短帧数据使用 CRC-8，保证数据完整性；TADR 为时间请求地址字段，长 10 位，用于回应时钟同步请求时的附加地址码；TR 为时间请求区分字段，长 6 位，用于区分不同的时间请求消息；UDID 为设备识别码，长 6 字节，用于区分是否为 openSAFETY 域设备；SDN 为安全域码，长 10 位，用于区分 openSAFETY 域内的不同安全域。

2　残余错误率计算

在 IEC 61784-3：2017(第 3.1 版)中，新的残余错误率扩展计算模型将残余错误率分为数据完整性错误、真实性错误、时效性错误和伪装错误 4 个部分[2]，计算公式如下：

$$\lambda_{SC} = RR_T + RR_A + RR_I + RR_M 。 \tag{1}$$

式中：RR_T 表示时效性的残余错误率；RR_A 表示真实性的残余错误率；RR_I 表示数据完整性的残余错误率；RR_M 表示伪装的残余错误率。分别计算以上几种残余错误率，即可求得总的残余错误率。

2.1　数据完整性错误

IEC 61784-3 将表 1 中的“数据损坏”错误归类为数据完整性错误。而“数据损坏”指的是在消息传递过程中，由于传输介质出错或者外部干扰导致的数据内容错误。工程应用中，该错误主要由电磁干扰引起传输数据的位跳变导致。

2.1.1　数据完整性残余错误率计算公式介绍

数据完整性残余错误率 RR_I 的计算公式如下：

$$RR_I = RP_I v RP_U RP_{FSCP} 。 \tag{2}$$

式中：RP_U 表示数据单元的实际取值范围占总范围大小的比值；v 表示每小时安全帧采样速率；RP_{FSCP} 表示其他功能安全通信协议安全措施的残余错误率(即其他措施对 RR_I 的影响)；RP_I 表示数据完整性残余错误概率，计算公式如下

$$RP_I \approx 2^{-r} \sum_{k=d_{min}}^{n} \binom{n}{k} \times (P_e^k (1-P_e)^{n-k})^2 。 \tag{3}$$

式中：P_e 表示位跳变概率，一般取值 0.01；r 表示 CRC 校验长度，本例采用 CRC-16 校验，取值 16；n 表示安全数据单元位长度，本例中以冗余数据长度近似，假定 DATA 为 10 字节，取值 96；d_{min} 表示最小汉明距离，本例取值 4。

2.1.2　数据完整性残余错误率计算公式分析

RR_I 计算公式主要分为 RP_I、v 和 RP_U 3 部分，具体分析如下：

1) RP_I 描述的是相应安全措施失效的概率，工程中常用 CRC 校验和数据冗余 2 种措施，在图 2 的数据冗余模型下，标准给出式(3)进行计算；

2) 由于每次安全数据帧的传输都可能发生电磁干扰引起的数据损坏，故用 v 描述事件发生频率；

3) 某些情况下，虽然发生损坏的数据无法被 CRC 和冗余手段检测出来，但是数据超出合理范围，因此，数据取值范围 RP_U 也能进一步降低残余错误率。

综上所述，式(2)和(3)主要针对的是在 CRC 校验

和图 2 所示模型数据冗余 2 种安全措施下，以 v 速率传输取值范围占比为 RP_U 数据时的残余错误率。

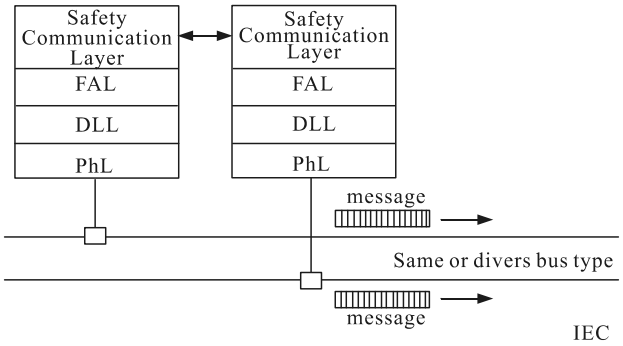

图 2 通信模型

2.1.3 数据完整性残余错误率计算公式改进

参考图 1 的 openSAFETY 安全数据帧格式，容易发现其与标准中提供模型的区别：

1) 冗余模型不同：不同于图 2 模型的完全相同信息通过不同渠道独立发送，openSAFETY 将冗余数据包含在同一帧中，因此，冗余位长度不能采用原来的全帧位长度。

2) CRC 校验不同：由于子帧 1 和子帧 2 的信息不同，CRC 校验结果不能相互比对，其残余错误概率的计算也应相应变化[3]。

3) 存在可预期的信息：openSAFETY 存在一些可预期的信息，其错误检出概率比判断取值范围 RP_U 的更高。如 LE 字段，当数据内容发生跳变时，不改变数据长度，此时 LE 字段的错误必然检出。

综上所述，IEC 61784-3 标准中的数据完整性残余错误率计算公式已不适用于 openSAFETY：RP_I 的计算需要进行很大调整，RP_U 也已经不适用。结合 openSAFETY 具体特点，可以用下列公式计算 openSAFETY 的数据完整性错误残余率：

假设在子帧 1 中发生 e 个位跳变，此事件发生概率为：

$$R_1(e)=\binom{N_1}{e}\cdot P_e^e(1-P_e)^{(N_1-e)}。\tag{4}$$

式中：N_1 表示子帧 1 的位长度(含 CRC)，本例取值 128；e 表示发生跳变的总位数。

同理有子帧 2 发生 e 个位跳变概率：

$$R_2(e)=\binom{N_2}{e}\cdot P_e^e(1-P_e)^{(N_2-e)}。\tag{5}$$

式中 N_2 表示子帧 2 的位长度，本例取值 136。

在子帧 1 和子帧 2 中，不同字段使用不同的安全措施，如：ADR、ID、DATA 字段在子帧 1 和 2 中具有冗余措施，意味着只有当子帧 1 和 2 中对应字段的对应数据位发生相同跳变时，该错误无法检测。而 LE 字段是可预期的，当 LE 字段发生错误，此错误仍可以通过计算 DATA 长度进行检测纠正。此外，绝大部分字段都使用了 CRC 校验。需要对使用这几种措施的数据字段进行区分考虑，字段安全措施使用如表 2 所示。可预期性涉及内部机制[4]，在此不详细说明其原理。

表 2 字段安全措施

字段	长度/bit	CRC 校验	冗余	可预期
ADR	10	√	√	
ID	2	√	√	
ID	4	√	√	√
LE	6	√		√
CT(L)	8	√		
CT(M)	8	√		√
TADR	10	√		√
TR	6	√		√
CRC	8/16			
DATA	(0-240)*8	√	√	

当 e 个错误中有 i 个发生在冗余字段时，子帧 1 中该事件发生概率为：

$$Ba_1(e,i)=\frac{\binom{D}{i}\binom{N_1-D}{e-i}}{\binom{N_1}{e}}。\tag{6}$$

式中：D 表示冗余字段总位数，本例取值 96；i 表示跳变发生在冗余字段的位数。同理，发生在子帧 2 的概率为

$$Ba_2(e,i)=\frac{\binom{D}{i}\binom{N_2-D}{e-i}}{\binom{N_2}{e}}。\tag{7}$$

子帧 1 和子帧 2 的冗余字段对应数据位发生相同跳变的概率为：

$$B_b(i)=\binom{D}{i}^{-1}。\tag{8}$$

选择合适的 CRC 生成多项式，CRC 校验残余错误概率为：

$$Bc(e)=2^{-r}。\tag{9}$$

上文已分析可预期字段可进一步减少残余错误率。错误残余率减少的数学期望为：

$$Bd_1(e)=\frac{\binom{N_1-M_1}{e}}{\binom{N_1}{e}}\cdot\left(1-\frac{\binom{r}{e}}{\binom{N_1-M_1}{e}}\right)。\tag{10}$$

式中 M_1 表示子帧 1 的可预期信息长度，本例取值 12。同理，对于子帧 2 有：

$$Bd_2(e)=\frac{\binom{N_2-M_2}{e}}{\binom{N_2}{e}}\bullet\left(1-\frac{\binom{r}{e}}{\binom{N_2-M_2}{e}}\right)。\tag{11}$$

式中 M_2 表示子帧 2 的可预期信息长度，本例取 28。

综上所述，可以计算残余错误概率为：

$$RP_I=\sum_{i=1}^{d+6}\left(\sum_{e_1=\max(i,d)}^{d+6}R_1(e_1)\bullet Ba_1(e_1)\bullet B_c\bullet Bd_1(e_1)\right)\bullet$$
$$\left(\sum_{e_2=\max(i,d)}^{d+6}R_2(e_2)\bullet Ba_2(e_2)\bullet B_c\bullet Bd_2(e_2)\right)Bb(i)。\tag{12}$$

最后，残余错误概率乘以每小时采样率 v 得到最终的数据完整性残余错误率：

$$RR_{\mathrm{I}}=RP_{\mathrm{I}}\bullet v。\tag{13}$$

2.2　真实性错误

IEC 61784-3 将表 1 中的“消息插入”和“寻址错误”归类为真实性错误。其中“消息插入”主要是指接收到非预期或者未知来源的信息；而“寻址错误”主要是指信息被传递给错误的对象，主要发生在信息转送的模块中。

2.2.1　真实性残余错误率计算公式介绍

真实性残余错误率 RR_{A} 的计算公式如下：

$$RR_{\mathrm{A}}=RP_{\mathrm{I}}\times 2^{-LA}\times R_{\mathrm{A}}\bullet RP_{\mathrm{FSCP}}。\tag{14}$$

式中：LA 表示连接认证字段长度，即地址字段长度，本例取值 10；R_{A} 表示传输方向错误发生率，一般取值 10^{-3}。

2.2.2　真实性残余错误率计算公式分析

真实性错误残余错误率计算主要分为 RP_{I}、2^{-LA} 和 R_{A} 3 部分，具体分析如下：

1) 由于地址字段信息一般会经过 CRC 校验，因此，地址字段发生错误时，必然先会引起数据完整性错误发生，此处用 RP_{I} 描述相应残余错误概率。

2) 2^{-LA} 描述的是地址字段均匀发生错误概率。实际上，可以借助 RP_{U} 来理解这个概念，当地址字段数据在传输过程中无错误地传输到目的设备处时，连接认证工作是由目的设备将预期值与传输值比对完成。此时，由于认证 ID 的唯一性，传输值的取值范围只有唯一值，即 $RP_{\mathrm{U}}=2^{-LA}$。

3) 不同于数据完整性主要受传输过程中电磁干扰产生错误，真实性错误主要由硬件错误导致，因此 R_{A} 取值明显小于 v。

由于 openSAFETY 针对真实性错误的安全措施与标准一致，此部分公式无需改进。

2.3　时效性错误

时效性错误主要包含表 1 中的“数据重复”“数据丢失”“通信延迟”和“数据乱序”4 种错误。“数据重复”是指接收到的数据在时效性上满足要求，但是已经收到过完全一致的数据信息。“数据丢失”是指预期接收到的数据没有收到彻底消失。“通信延迟”是指接收到的信息比规定的时效范围延迟过多。“数据乱序”是指接收到的信息完全偏离预期时间范围，甚至比预期值提前。

2.3.1　时效性错误残余错误率计算公式介绍

时效性的残余错误率 RR_{T} 的计算公式如下：

$$RR_{\mathrm{T}}=2^{-LT}\times w\bullet R_{\mathrm{T}}\bullet RP_{\mathrm{FSCP}}。\tag{15}$$

式中：LT 表示 CT 字段长度，本例取值 16；w 表示 CT 可取值的范围(时间窗)，本例取值 1；R_{T} 表示 CT 字段错误发生率，一般取值 10^{-3}。

2.3.2　时效性错误残余错误率计算公式分析

时效性错误包含的具体错误类型最多，导致其发生的原因也很复杂，可能是通信负荷过重网络拥堵、内部存储单元空间不足(数据被覆盖丢失)、通信中断等。时效性错误检测核心要求是时效性字段代码的准确传输和比对，因此，RR_{T} 计算公式主要分为 $2^{-LT}w$ 和 R_{T} 2 部分：

1) $2^{-LT}w$ 与 2^{-LA} 情况类似，唯一不同的是，时效性判断一般是某几个值均有效，而不像 ID 具有唯一性，因此，多了 w 部分。

2) R_{T} 与 R_{A} 情况一致，取值相同。

值得注意的是：RR_{T} 和 RR_{A} 相比，计算上缺少 RP_{I} 项。这主要是因为时效性字段代码不一定参与 CRC 校验，从最坏的角度考虑时，计算不含 RP_{I} 一项。

2.3.3　时效性错误残余错误率计算公式改进

根据 openSAFETY 帧格式设计，显然时效性字段即 CT 字段是参与 CRC 校验的，因此，类比 RR_{A} 计算公式，RR_{T} 计算公式可改进为：

$$RR_{\mathrm{T}}=RP_{\mathrm{I}}\times 2^{-LT}\times w\bullet R_{\mathrm{T}}\bullet RP_{\mathrm{FSCP}}。\tag{16}$$

2.4　伪装错误

伪装错误主要包含表 1 中的“伪装”类型。“伪装”主要是指非安全帧错误地发送给了安全帧接收

对象。由于安全数据和非安全数据 CRC 生成多项式、地址码、通信时段等信息一般不同，因此，伪装类型错误最容易检测出来。

2.4.1 伪装错误残余错误率计算公式介绍

伪码的残余错误率 RR_M 的计算公式如下：

$$RR_{\mathrm{M}} = 2^{-LA} \times 2^{-LT} \times w \times 2^{-r} \times RP_{\mathrm{U}} \times 2^{-LR} \times R_{\mathrm{M}}。 \quad (17)$$

式中：R_{M} 表示伪码错误发生率，一般取值 10^{-3}；LR 表示安全数据重复冗余部分长度，本例取值 96。

2.4.2 伪装错误残余错误率计算公式分析

伪装错误将从数据完整性、真实性和时效性 3 个方面进行检测，与此对应可以将其残余错误率计算公式分为 2^{-LA}、$2^{-LT} \times w$、$2^{-r} \times RP_{\mathrm{U}} \times 2^{-LR}$ 和 R_{M} 4 部分，具体分析如下：

1) 2^{-LA} 和 $2^{-LT} \times w$ 分别表示的是真实性错误和时效性错误的残余错误概率；

2) $2^{-r} \times RP_{\mathrm{U}} \times 2^{-LR}$ 表示的是在 CRC 校验和数据冗余 2 种措施下的数据完整性残余错误概率，相比 RP_{I} 的计算过程，这里只是一个根据数据格式的粗略计算；

3) R_{M} 与 R_{A}、R_{T} 情况一致，取值相同。

2.4.3 伪装错误残余错误率计算公式改进

在粗略估计下，式(17)也能使用，但是使用 RP_I 替代 $2^{-r} \times RP_{\mathrm{U}} \times 2^{-LR}$ 计算更加准确，因此，可以将计算公式改进为：

$$RR_{\mathrm{M}} = 2^{-LA} \times 2^{-LT} \times w \bullet RP_{\mathrm{I}} \bullet R_{\mathrm{M}}。 \quad (18)$$

3 计算结果分析讨论

3.1 计算结果及 SIL 评估

根据第 2 节提供的计算公式以及参数，可以得到计算结果如表 3 所示。

表 3 重要参数计算结果

参数	改进前	改进后
RR_{I}	1.44×10^{-10}	1.22×10^{-12}
RR_{A}	7.80×10^{-22}	6.61×10^{-24}
RR_{T}	1.53×10^{-8}	1.03×10^{-25}
RR_{M}	2.87×10^{-45}	1.01×10^{-28}
λ_{SC}	1.54×10^{-8}	1.22×10^{-12}

根据表 4 提供的残余错误率与 SIL 对应关系，可以很容易地完成 SIL 评估：根据改进后公式计算的残余错误率，在传输 10 字节数据时，openSAFETY 满足 SIL3 要求。

表 4 残余错误率与 SIL 关系对应 h^{-1}

SIL	平均安全功能危险失效频率(PFH)	单一逻辑连接最大允许残余错误率 λSC
4	$<10^{-8}$	$<10^{-10}$
3	$<10^{-7}$	$<10^{-9}$
2	$<10^{-6}$	$<10^{-8}$
1	$<10^{-5}$	$<10^{-7}$

3.2 进一步降低残余错误率的方法讨论

对表 3 所列计算结果进行分析可以得到结论：

1) 对比改进前公式计算的 RR_{A} 和 RR_{T} 可知：连接认证(地址)字段和时效性(CT)字段经过 CRC 校验后，可大大降低其残余错误率，故在设计安全帧时，有必要将全部信息进行 CRC 校验；

2) 在 2 组计算结果中，RR_{M} 的值均最小，与其校验要求最严格是相符的，同时意味着，在设计安全帧时，可以主要考虑保障数据完整性、真实性以及时效性，当这三者满足要求时，RR_{M} 自然满足。

由此 2 点可以进一步推论：数据完整性残余错误率的降低有利于整体残余错误率降低。降低残余错误率，可以从保障数据完整性的措施入手。

3.2.1 适当的 CRC 生成多项式选取

选取适当的 CRC 生成多项式显然比增加数据冗余倍数及 CRC 校验长度对提升数据完整性更廉价且易于实现。

对于不同长度和特征的数据，生成多项式的适用性(检错能力)有所不同，评估 CRC 生成多项式检错能力可以从最小汉明距离和奇偶校验特性 2 个方面考虑。

对于阶次较高的生成多项式，其最小汉明距离已经难以通过理论精确分析计算，且理论值也与实际效果存在偏差。文献[5-6]给出了一些生成多项式的汉明距离测试结果，并提供了一些生成多项式选择的参考方法。

对于奇偶校验特性，文献[7]分析了具备此特性的生成多项式的因式分解特征，即：具备 $x+1$ 因子的多项式具备奇偶校验特性，反之，不具备。

openSAFETY 的 CRC-16 选择的生成多项式为 0xBBAD，在伽罗华域中对应多项式为：

$$g(x) = x^{16} + x^{14} + x^{13} + x^{12} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + x + 1。 \quad (19)$$

该多项式不含 $x+1$ 因子，故不具有奇偶校验特性，这将大大削弱其检错能力。

为进一步增强检测能力，笔者从增加奇偶校验

特性的角度出发，选取 0xC86C 作为 CRC-16 的生成多项式，其多项式分解如下：

$$g(x)=x^{16}+x^{15}+x^{12}+x^{7}+^{6}+x^{4}+x^{3}+1= (x+1)(x^{15}+x^{11}+x^{10}+x^{9}+x^{8}+ x^{7}+^{5}+x^{4}+x^{2}+x+1)。 \quad (20)$$

由上式可知：0xC86C 多项式包含 x+1 因子，具备奇偶校验特性，检错能力更强。

3.2.2　增加可预期信息长度

传输过程中，通过其他运行机制使得某些字段的内容可以预期。openSAFETY 的可预期字段具体如表 3 所示。由于这种可预期性，残余错误率得以进一步降低。在数据完整性残余错误概率计算中就用到了这个特点。

过度添加可预期信息会加重网络传输负荷，因此对可预期信息占全信息比例与残余错误降低效果的相关性分析十分必要。利用式(10)进一步分析的结果如图 3 所示。

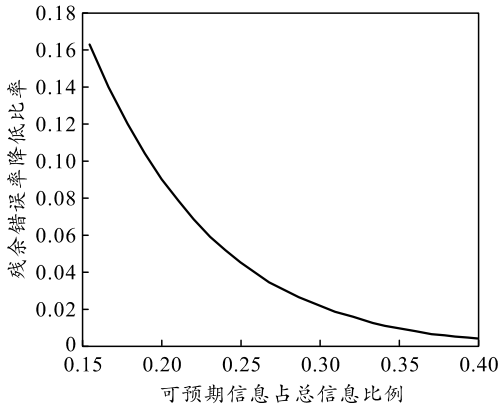

图 3　预期信息降低残余错误率效果

从图中可以看出：当预期信息占总信息 20%以下时，预期信息的增加可以显著降低残余错误率，其后，随着占比增加，残余错误率继续降低，但降低效果逐渐下降。通常，负载数据长度在一帧信息中占比较大，此时，适当设计预期信息的传输可以有效降低残余错误率，提高通信的可靠性。

4　结论

笔者基于项目应用需求，以 openSAFETY 为分析对象，在详细介绍分析 IEC61784-3 标准中参考计算公式列写原理后，结合 openSAFETY 自身特点，提出残余错误率计算公式改进意见，并完成 SIL 评估。结果表明：在 10 字节数据传输条件下，openSAFETY 满足 SIL3 要求。此外，还提出了进一步降低残余错误率的改进措施：1) 选取适当 CRC 生成多项式；2) 适当增加可预期信息的传输。该研究对其他工程项目中通信协议的残余错误率计算，以及通信协议安全数据帧设计有较高的参考价值。

参考文献：

[1] 魏昊旻, 王文海. 基于 EPL 的 openSAFETY 平台构架设计[J]. 计算机测量与控制, 2015, 23(3): 889-892.

[2] The International Electrotechnical Commission. Functional safety fieldbuses general rules and profile definitions: IEC 61784-3[S]. Geneva: IEC, 2017.

[3] 丁龙, 王宏. 安全仪表系统通信功能的可靠性评估[J]. 仪表技术与传感器, 2016(5): 84-88.

[4] Ethernet POWERLINK Standardisation Group. openSAFETY Safety Profile Specification EPSG Draft Standard 304 V1.5.0 [EB/OL]. [2017-05-15]. https://www.ethernet-powerlink.org/fileadmin/user_upload/Dokumente/Downloads/TECHNICAL_DOCUMENTS/EPSG_DS_304_V-1-5-0.pdf.

[5] PHILIP K, TRIDIB C. Cyclic Redundancy Code (CRC) Polynomial Selection for Embedded Networks[P]. Dependable Systems and Networks, 2004 International Conference on, 2004.

[6] PHILIP K. 32-Bit Cyclic Redundancy Codes for Internet Applications[P]. Dependable Systems and Networks, 2002. DSN 2002. Proceedings. International Conference on, 2002.

[7] 张平安. 16 位循环冗余校验码(CRC)的原理和性能分析[J]. 山西科技, 2005(5): 123-125.