doi:10.3969/j.issn.1000-436x.2014.12.024

CTCS-3 级 GSM-R 车地通信数据丢失概率及其影响的研究

张霞[1,2,3]，马连川[2,3]，曹源[2,3]，张玉琢[1,2,3]

（1. 北京交通大学 轨道交通控制与安全国家重点实验室，北京 100044；
2. 北京交通大学 轨道交通运行控制系统国家工程研究中心，北京 100044；
3. 北京交通大学 电子信息工程学院，北京 100044）

摘 要：为了解决 CTCS-3 级列控系统 GSM-R 车地数据传输接口（Euroradio）安全功能模块没有提供时间相关风险防护措施的问题，建立基于 DSPN 的数据传输过程中故障恢复模型和通信模型。结合这 2 种模型并利用 TimeNET4.0 对数据丢失概率进行仿真，发现即使只考虑数据丢失才会造成列控系统危险输出的极端情况，仍不满足相关规范对于 CTCS-3 级列控系统数据传输 SIL4 级要求。

关键词：CTCS-3 级列控系统；GSM-R；安全通信协议；确定与随机 Petri 网

中图分类号：U285; TN929 **文献标识码**：A **文章编号**：1000-436X(2014)12-0203-07

Research on data loss probability and its impact of CTCS-3 train ground communication based on GSM-R

ZHANG Xia[1,2,3], MA Lian-chuan[2,3], CAO Yuan[2,3], ZHANG Yu-zhuo[1,2,3]

(1. State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China;
2. National Engineering Research Center of Rail Transportation Operation and Control System, Beijing Jiaotong University, Beijing 100044, China;
3. Electronic and Information Engineering College, Beijing Jiaotong University, Beijing 100044, China)

Abstract: In order to solve the problem that Euroradio's safe functional module (SFM) of CTCS-3 train control system can not apply protective measures for time-related transmission risks, communication model and failure recovery model for transmission of CTCS-3 train control system are built which based on deterministic and stochastic Petri nets (DSPN). Combining the two models and using TimeNET 4.0 to simulate the result of data loss probability, a conclusion can be concluded that even considering that only data loss will cause dangerous of train control system, the result still can not meet the requirement of SIL4 based on the relevant specification for the CTCS-3.

Key words: China train control system level 3; GSM-R; safety communication protocol; deterministic and stochastic Petri net

1 引言

CTCS-3 级列控系统在我国高速铁路中得到广泛应用，其列控数据传输基于铁路综合数字移动通信系统（GSM-R, GSM for railway）实现。《CTCS-3 级列控系统无线通信功能接口规范》（对应于欧洲的 Euroradio FIS[1]，以下简称 Euroradio）中的安全功能模块（SFM, safe functional module）为数据传输过程中可能出现的风险提供安全防护措施。根据最新版本的 EN 50159 标准[2]的规定，GSM-R 属于第三类开放传输系统，应对于重复、删除、插入、乱序、损坏、延迟和伪装等所有 7 种传输风险提供

收稿日期：2014-05-07；**修回日期**：2014-09-02

基金项目：国家自然科学基金资助项目（51305021, U1334211）；国家高新技术研究发展计划（“863”计划）基金资助项目（2012AA112001）；国家重大科技专项基金资助项目（2011ZX03001-007-01）

Foundation Items: The National Natural Science Foundation of China (51305021, U1334211); The National High Technology Research and Development Program of China (863 Program)(2012AA112001); The Major National Science and Technology Projects (2011ZX03001-007-01)

强防护措施。Euroradio SFM 所提供的防护措施只有源和宿标识符、认证过程和加密过程，能够对插入、损坏和伪装等 3 种传输风险提供强防护措施，但对重复、删除、乱序、延迟等 4 种与时间相关的传输风险则没有提供相应的防护措施。因此可以认为分析 CTCS-3 级数据传输安全特性时可以排除插入、损坏和伪装等传输风险，而只考虑与时间相关的传输风险。

2009 年，单振宇[3]利用有色 Petri 网对根据系统需求所设计的 CTCS-3 级通信协议进行建模，分析验证所设计的通信协议能满足性能需求。2012 年，陈黎洁[4]选择分层赋时有色 Petri 网对安全通信协议进行研究，通过改变信道与应用层模型的参数分析所修改的安全通信协议中安全连接建立的时间特性。2014 年，全宏宇[5]利用 Matlab SimEvents 清晰地模拟了车地通信系统的信息交互流程，并统计分析了通信协议的安全连接建立时间以及不同长度无线消息传输延迟时间。上述研究成果在研究安全通信协议时，通过在现有 Euroradio 安全通信协议中添加时间戳和序列号等措施防护时间相关风险[3,6]，并对改变后的安全通信协议进行了功能或性能验证。但这些研究的不足之处在于没有阐明添加这些针对时间相关传输风险防护措施的理由。

根据 GSM-R 数据传输原理[7]，可以发现数据延迟和数据丢失是造成重复、删除、乱序、延迟等时间相关传输风险的 2 种主要原因。在实际情况中，数据丢失会造成列控车载设备由于接收不到数据而导致移动授权缩短失败等危险。根据文献[1]可知，数据帧在重传多次后仍没传输成功则视该数据帧为丢失。相对数据延迟而言，数据丢失发生的概率更低。因此，本文主要分析 CTCS-3 级列控系统数据传输中数据丢失的概率能否满足相关规范的安全要求。

2 基于 DSPN 的 CTCS-3 级无线通信模型与故障恢复模型

由于 Petri 网能够完成系统的形势描述、正确性验证、性能评价、目标实现和测试等任务，Petri 网成为了研究人员分析通信系统与通信协议的主要工具。而确定与随机 Petri 网（DSPN, deterministic and stochastic Petri nets）是一般 Petri 网的扩充，允许变迁的实施延时既可以是常数，也可以是指数分布的随机变量，这对周期性通信或数据传输的问题非常适用。所以本文选用 DSPN 作为建模工具[8]。

2.1 数据传输过程中的故障恢复模型

无线传输过程容易受外界环境的影响，导致信道故障的来源主要有无线降质、越区切换和链路中断 3 种类型[9]。而根据相关研究成果[10]可知多普勒频移对于 2G 和 3G 无线传输系统基本无影响，因此本文研究时不考虑多普勒频移的影响。

在实际建模过程中，上述 3 种故障模型单独设计，其好处在于不仅能仿真数据传输过程中数据与单一故障“碰撞”的过程，还能仿真这 3 种故障全部发生情况下的数据传输过程,这样仿真结果更加准确。数据传输过程中的故障恢复模型如图 1 所示。该模型描述的是 3 种不同的故障由未发生到发生的转变过程，3 个模型初始状态表示 3 种故障均没有发生。

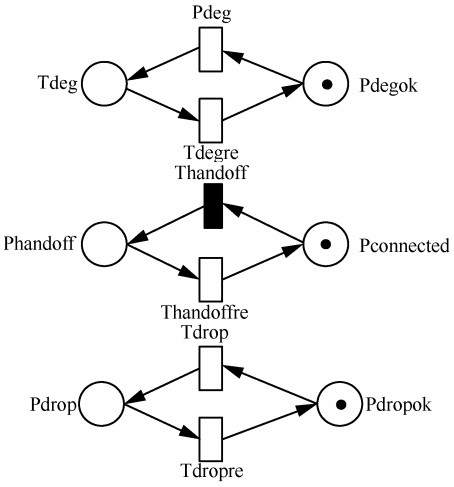

图 1 数据传输过程中的故障恢复模型

2.2 数据传输过程中的通信模型

建立 Euroradio SFM 以下部分的数据传输过程中的通信模型需要考虑以下 3 点。

1) 根据文献[1]对数据传输性能指标影响最大的是 GSM-R 物理层，其他层对于数据的处理时间相对整个数据传输过程而言可以忽略。因此在模型的初始状态，数据直接以 TDMA 帧形式准备发送。

2) 由于 CTCS-3 规范中规定每帧数据为 30 byte，而 TDMA 帧中一个时隙的长度为 156.25 bit，所以要完成这 30 byte 数据帧的传输，需要 2 个 TDMA 帧。在建立 DSPN 模型时为建模方便，将 2 个 TDMA 帧看做是一个 Petri 网标识。

3) 基于 GSM-R 进行数据传输时，以下 2 种情

况引起数据重传：一是由于传输过程中遇到故障而导致数据部分丢失或错误；二是由于传输超时。文献[1]中规定数据的最大重发次数为 5 次。

CTCS-3 级列控系统数据传输过程中的通信模型如图 2 所示。

表 1 给出了图 1 和图 2 的库所说明，表 2 中给出图 1 和图 2 的变迁含义及各变迁的取值，数据取自文献[1,11]。

表 1　　图 1 和图 2 的库所说明

库所	含义
Pdegok	无线链路正常
Pdeg	无线链路中断
Pconnected	没有发生越区切换
Phandoff	越区切换执行状态
Pdropok	没有发生无线降质
Pdrop	无线降质发生
Pdatabuf	数据链路层数据存储区
Psenddata	数据开始发送
Ptrans/Ptrj	数据传输过程没有任何故障
Ptradr/ Ptradrj	数据传输过程中存在无线降质
Pduan	数据传输过程中遇到故障导致通信中断
Ptci	简化部分的库所
Pwgzsucc	传输过程没有故障时，数据应答消息到达发
Psuccj	第 1/2/3/4/5 次重传成功
Pprocess/ Pproj	传输过程存在故障，重发消息到达发送方
Poni	数据发送时启动定时器
Pouti1	定时器超时，重新发送数据
Presendj	数据重新发送，等待相应的时隙到来
Plost	数据丢失

注：$0 \leqslant i \leqslant 5$，当 $i=0$ 时，数字“0”不显示；$1 \leqslant j \leqslant 5$，$1 \leqslant m \leqslant 8$，$1 \leqslant k \leqslant 3$。

在图 2 所示的通信模型中，当数据传送到达空中接口时，首先要判断是否发生故障。

1) 当数据传输过程中没有任何故障发生时，变迁 Twgz 被激发进行数据传输，经过数据的上行、下行和接收方的判断之后 Ttrade 被激发，表示发送方收到数据的应答帧，经过一定时间的应答帧分析后变迁 Twgzsucc 被激发，开始准备传输下一帧数据。

2) 当数据传输过程中发生无线降质，则变迁 Tcoll1 被激发，由于无线降质是在数据传输过程中由于信道衰落或者受到干扰而造成，对数据而言，造成的最恶劣影响就是部分数据错误，并不会引起传输延时，所以经过正常的上、下行传输和接收方的数据校验之后变迁 Tdrde 被激发，将库所 Ptradr 中的标记转入 Pprocess 中，表示发送方收到接收方传输回来的要求数据帧重传的信息，发送方对这一信息进行处理判断之后变迁 Tprocess 被激发，开始准备数据重发。

3) 当数据传输过程中遇到越区切换时，变迁 Tcoll2 被激发。由于 GSM-R 采用的是硬切换技术，所以越区切换执行时会造成一定时间的通信中断，而在该通信中断过程中正在进行的传输数据就会发生丢失，导致接收方不会接收到数据而产生相应的应答帧。所以只有在定时器 Ttimer 溢出后才能进行重发。

4) 当数据传输过程中发生链路中断的时候，变迁 Tcoll3 被激发。由于链路中断同样会造成一定时间的通信中断，数据传输及重发过程与越区切换基本一致，只是由于二者的中断时间不同，需要发送的重传的数据帧数不同而已。

5) 当数据传输过程中无线降质和链路中断同时发生、越区切换和链路中断同时发生或者 3 种故障全部发生时，由于链路中断或者越区切换而造成数据丢失，等待超时重发。

6) 关于定时器部分，变迁 Tgen 被激发，数据帧开始发送的同时启动定时器 Ttimer，即标记进入 Psenddata 的同时另一个标记同样进入 Pon。当标记到达 Pwgzsucc 或者 Pprocess 时清除 Pon 中的标记，表示当发送方收到接受方发回的应答帧时，无论是数据成功的信息还是要求数据重传的信息，都满足定时器溢出之前收到应答帧就清零定时器的要求。当定时器超时 Ttimer 被激发，标记进入 Pout1。实际数据传输过程中定时器超时立即重新发送数据，而不管已经发送的数据是否仍在传输中，但是在 DSPN 模型中，某一时刻只能保证一个标记被传输，否则会造成标记堆积而导致仿真失败。当定时器超时且数据仍在传输没有应答帧到达发送方时，即库所 Pout1 中存在标记，同时 Pduan 中存在标记，Tca3 被激发，清除 Pduan 中的标记，表明数据丢失等待定时器超时超发。当定时器超时的同时恰巧收到数据帧应答时，即 Pout1 中存在标记，Pwgzsucc 或者 Pprocess 中存在标记，激发变迁 Ttiao5 或者 Ttiao6，清除 Pwgzsucc 或者 Pprocess 中的标记来进行超时重发。

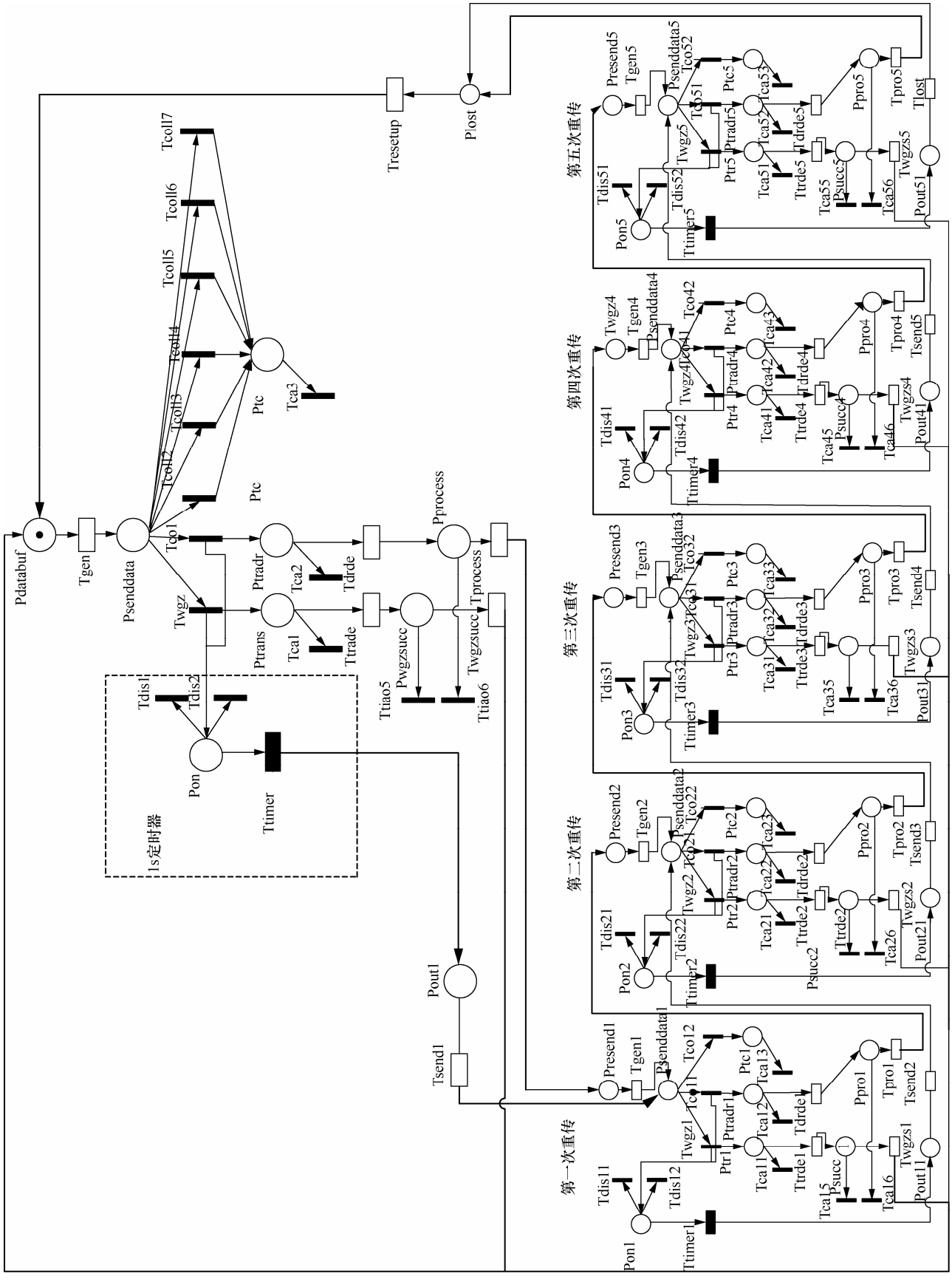

图 2　CTCS-3 级列控系统数据传输过程中的通信模型

表 2　　图 1 和图 2 的变迁说明

变迁	含义	激发速率
Tdeg	链路中断	视网络覆盖情况而定
Tdegre	链路中断恢复	0.352 4
Thandoff	越区切换发生	视网络覆盖情况而定
Thandoffre	越区切换恢复	10
Tdrop	无线降质	视网络覆盖情况而定
Tdropre	无线降质恢复	4.608
Tgeni	数据发送延时	86.655
Twgzi	数据传输过程中没有发生任何故障	瞬时变迁
Tcoi1	数据传输过程中发生无线降质	瞬时变迁
Tcollp	数据传输过程中故障两两发生或全部发生	瞬时变迁
Tcoj2/Tcolli2n	简化后的变迁	瞬时变迁
Ttradei	数据传输过程中没有任何故障的传输延时	4.476
Tdrdei	数据传输过程中存在无线降质的传输延时	4.476
Tprocess/Tproj	数据在接受方判断数据需要重传的处理延时	149.79
Tsendj	数据超时重发	86.655
Twgzsucc/Twgzsj	数据在接受方判断数据正确的处理延时	149.79
Tdisi1	定时器还没有超时且数据成功传输	瞬时变迁
Tdisi2	定时器还没有超时且关于数据的应答帧到达接收方	瞬时变迁
Ttimeri	数据发送的时候启动定时器	1
Tcaik Tca3/Tca13/Tca23/Tca33/Tca43/Tca53 Tca4/Tca14/Tca24/Tca34/Tca44/Tca54	清除库所中的 token	瞬时变迁
Ttiaoi5/Ttiaoi6 Ttiao6/Ttiao16/Ttiao26/Ttiao36/Ttiao46/Ttiao56	数据帧到达发送方的同时定时器超时	瞬时变迁
Tlost	数据在第五次重传时启动的定时器超时，数据丢失	29.958
Tresetup	重启	11 764.71

注：$0 \leqslant i \leqslant 5$，当 $i=0$ 时，数字“0”不显示；$1 \leqslant j \leqslant 5$，$1 \leqslant m \leqslant 8$，$1 \leqslant k \leqslant 3$，$2 \leqslant p \leqslant 7$，$L$ 代表小区间平均距离，v 表示列车运行速度 50 ~500 km/h。

考虑到 GSM-R 网络主要存在 2 种覆盖方式：单层覆盖和冗余覆盖。冗余覆盖较单层覆盖能提高数据传输的可靠性，从而链路中断和无线降质发生概率降低，但冗余覆盖会造成越区切换更加频繁。

根据文献[11]，单层覆盖下无线降质出现周期大于 7 s 的概率为 99%，降质持续时间小于 1 s 的概率为 99%。考虑极端情况假定列车时速为 500 km/h，无线小区之间的距离 L 为 7 km，则越区切换发生的时间间隔为 50 s，切换导致的通信中断时间最长为 300 ms。链路中断故障每小时发生的概率为 10^{-2}，GSM-R 设备检查到中断后重新建立链接。链接中断后 5 s 内重新建立链接的概率为 95%[11]。而冗余覆盖下越区切换发生的时间间隔为单层覆盖的 1/2，无线降质出现周期为大于 70 s 的概率为 99%，降质持续时间小于 1 s 的概率为 99%，链路中断故障每小时发生的概率为 10^{-3}，链接中断后 5 s 内重新建立链接的概率为 95%。因此，单层覆盖及冗余覆盖下故障恢复模型参数选择如表 3 所示。

表 3　　单层覆盖及冗余覆盖下故障恢复模型参数选择

覆盖方式	Tdeg（每小时）	Thandoff	Tdrop（每秒）
单层	10^{-2}	L/v	0.001 436
双层	10^{-3}	$L/2v$	0.000 143 6

3　模型分析

结合上述数据传输过程中的通信模型和故障恢复模型，利用 TimeNET4.0 进行仿真，可以分别得到单层覆盖和冗余覆盖下数据丢失的稳态概率

P_{lost}，如图 3 和图 4 所示。

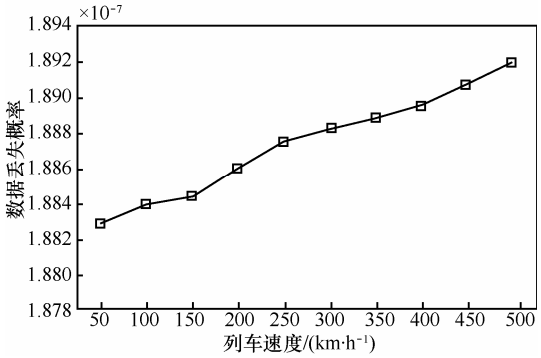

图 3 单层覆盖下列车速度对于数据丢失概率的影响

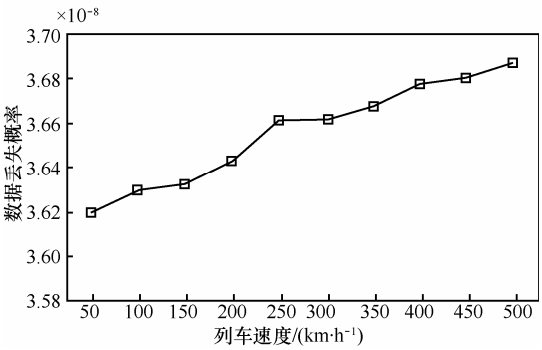

图 4 冗余覆盖下列车速度对于数据丢失概率的影响

由图 3 和图 4 可得出，单层或冗余覆盖下，随着列车速度的提高，数据丢失概率都会微升。但对于相同列车速度而言，冗余覆盖下数据丢失概率一直低于单层覆盖下的数据丢失概率，说明无线降质和链路中断对于数据丢失起主要作用，列车速度的变化对于通信的影响较小。

在实际情况中，数据丢失会使列车由于接收不到数据，而出现文献[7]中所描述的由于移动授权缩短失败所造成的危险。根据文献[7]，分配给 CTCS-3 级列控系统车地 GSM-R 传输系统危险失效率为 1.0×10^{-11}，结合前文“分析 CTCS-3 级数据传输安全特性时只考虑与时间相关的传输风险”的假设，可以认为时间相关的危险失效率就是 1.0×10^{-11}。为了说明问题，将单层覆盖和冗余覆盖下数据丢失概率及上述时间相关的危险失效率同时绘制于图 5 中。

图 5 中“标准”代表文献[7]规定的时间相关风险的危险失效率，当数据丢失概率在“标准”代表的图线下方时才满足 SIL4 级要求。但从图 5 中可以看出，不论是单层覆盖还是冗余覆盖，数据丢失概率都远在“标准”图线之上。这说明即使在只有数据丢失才会造成列控系统危险输出这一极端情况下，也不能满足相关规范对于数据传输的 SIL4 级要求，如果再考虑数据传输延时所造成的影响，就更不会满足相关规范的要求。

因此，现有 Euroradio 安全协议没有提供时间相关风险防护措施，不能满足相关规范对于数据传输的 SIL4 级要求，为了保证 CTCS-3 级列控系统 GSM-R 车地数据传输满足数据传输安全要求必须在其 SFM 上添加相应的时间相关风险防护措施。例如，可使用《RSSP-II 铁路信号安全通信协议》的安全应用中间子层协议。

4 结束语

本文从分析 CTCS-3 级列控系统 Euroradio 的 SFM 对于时间相关风险防护能力出发，基于 DSPN 建立了 CTCS-3 级列控系统数据传输过程中的通信

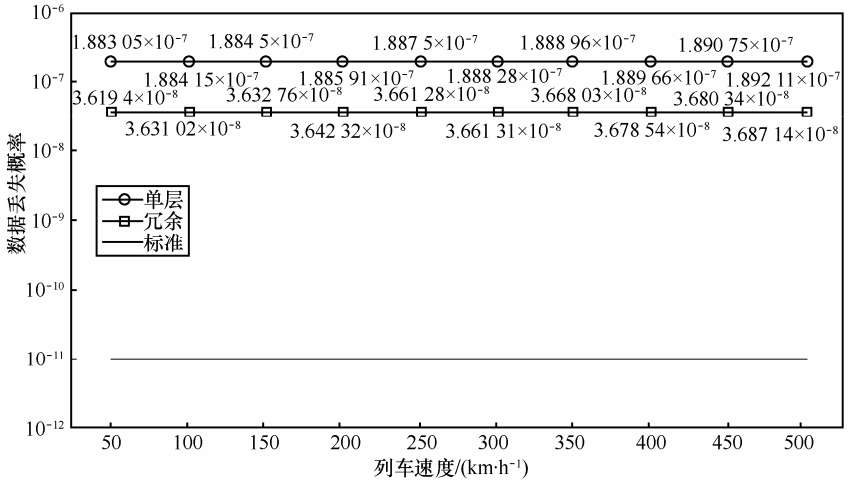

图 5 单层、冗余覆盖下数据丢失概率及时间相关的危险失效率对比

模型和故障恢复模型。将 2 种模型相结合，利用 TimeNET4.0 进行仿真，得出以下结论。

1) 单层覆盖或者冗余覆盖下，列车速度对于数据丢失的概率影响较小。

2) 相同列车速度下，冗余覆盖下数据丢失概率一直低于单层覆盖下的数据丢失概率。

3) 单层覆盖或者冗余覆盖下，即使只考虑数据丢失才会造成列控系统危险输出，也不能满足相关规范对于 CTCS-3 级列控系统数据传输的 SIL4 级要求。

因此，现有 Euroradio 安全协议没有提供时间相关风险防护措施，不能满足相关规范对于数据传输的 SIL4 级要求，为了保证 CTCS-3 级列控系统 GSM-R 车地数据传输满足数据传输安全要求，必须在其 SFM 上添加相应的时间相关风险防护措施。

参考文献：

[1] ETRMS/ETCS . Euroradio FIS[S]. 2005.

[2] ERTMS. EN50159-2010 Railway Applications—Communication, Signalling and Processing Systems—Safety-Related Communication in Transmission Systems[S]. 2010.

[3] 单振宇. CTCS-3 级车地通信协议设计与验证[D]. 北京: 北京交通大学, 2009.
SHAN Z Y. Design and Verification of CTCS-3 Train Ground Communication Protocol[D]. Beijing: Beijing Jiaotong University, 2009.

[4] 陈黎洁,单振宇,唐涛. 列车运行控制系统中安全通信协议的形式化分析[J]. 铁道学报, 2012,34(7):70-76.
CHEN L J, SHAN Z Y, TANG T. Formal analysis on safety communication protocol in train control system[J]. Journal of the China Railway Society, 2012, 34(7):70-76.

[5] 全宏宇. CTCS-3 级列控系统地车安全信息传输子系统的建模与分析[D]. 北京: 北京交通大学, 2014.
QUAN H Y. Modeling and Analysis of Safety Information Transmission Subsystem Between Train and Ground for CTCS-3 Train Control System[D]. Beijing: Beijing Jiaotong University, 2014.

[6] 陈黎洁. 列车运行控制系统安全通信协议验证方法的研究[D]. 北京: 北京交通大学, 2013.
CHEN L J. Research of Authentication Methods on Safety Communication Protocol in Train Control System[J]. Beijing: Beijing Jiaotong University, 2013.

[7] ETRMS/ETCS. ETCS Application Levels 1 & 2 - Safety Analysis[S].

[8] 林闯. 随机 Petri 网和系统性能评价[M]. 北京: 清华大学出版社, 2009.
LIN C. Stochastic Petri Nets and System Performance Evaluation[M]. Beijing: Tsinghua University Press, 2009.

[9] ZIMMERMANN A. Modeling and evaluation of stochastic Petri nets with TimeNET 4.1[A].Performance Evaluation Methodologies and Tools (VALUETOOLS), 2012 6th International Conference on[C]. 2012.54-63.

[10] 苏华鸿. 移动通信多普勒频移与高铁覆盖技术[J]. 邮电设计技术, 2009, (12):1-4.
SU H H. Mobile communication doppler frequency shift and high-speed railway coverage technology[J]. Designing Techniques of Posts and Telecommunications, 2009,(12):1-4.

[11] GSM-R QoS Working Group. ERTMS/GSM-R Quality of Service Test Specification[S]. 2006.

作者简介：

张霞（1988-），女，河北沧州人，北京交通大学硕士生，主要研究方向为基于通信的列车控制技术。

马连川（1970-），男，河北唐山人，北京交通大学副教授，主要研究方向为基于通信的列车控制技术。

曹源（1982-），男，回族，河南开封人，博士，北京交通大学讲师，主要研究方向为基于通信的列车控制技术。

张玉琢（1990-），男，河南信阳人，北京交通大学博士生，主要研究方向为列控系统形式化建模。