Механика Транспорт Комуникации

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 13, брой 3/3, 2015 г.

Научно списание http://www.mtc-aj.com **статия № 1257**

МОДЕЛИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ МИКРОПРОЦЕССОРНЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ, ТЕЛЕМЕХАНИКИ И СВЯЗИ

Мащенко Павел Евгеньевич
maschich@mail.ru

Кафедра «Автоматика, телемеханика и связь на железнодорожном транспорте» Московского государственного университета путей сообщения (МГУПС (МИИТ)), РОССИЯ

***Ключевые слова**: безопасность, техническое обслуживание, квалификация обслуживающего персонала.*

***Резюме**: В последнее время для описания работы технических систем стал применяться вероятностный подход. Самым оптимальным математическим аппаратом для данных целей является теория вероятностей для марковских и полумарковских случайных процессов. В статье рассмотрены две модели функциональной безопасности микропроцессорных систем железнодорожной автоматики, телемеханики и связи, а именно:*

- модель безопасности одноканального устройства с одноуровневым контролем и n-стадиями разрегулировки;

- модель безопасности одноканального устройства, учитывающая надёжность аппаратуры диагностики и квалификацию обслуживающего персонала.

В последнее время для описания работы технических систем стал применяться вероятностный подход. Самым оптимальным математическим аппаратом для данных целей является теория вероятностей для марковских и полумарковских случайных процессов. Рассмотрим модель безопасности одноканального устройства с одноуровневым контролем и n-стадиями разрегулировки (рис. 1).

На рис. 1 вершиной «0» показано состояние исправности основного и контрольного оборудования устройства. В него система может попасть после ремонта неисправных средств контроля (вершина «1») или из состояния восстановления (вершина «2»).

Вершиной «1» показано состояние отказа контролирующего оборудования, которое не влияет на работу основного устройства. В него система может перейти из вершины «0».

Состояние «2» – состояние восстановления, которое наступает либо после обнаружения явного отказа основного оборудования (из вершины «5»), либо по истечении некоторого (обычно большого) времени существования скрытого отказа основного оборудования, когда факт этого отказа каким–то образом проявился (из вершины «3»).

Вершиной «3» показано состояние скрытого отказа устройства. В данное состояние устройство попадает либо по причине отказа средств контроля и последующего отказа основного оборудования (из вершины «0»), либо по причине пропуска отказа

средствами контроля (из вершины «1»), либо из состояния разрегулировки (из вершин «4_1», «4_2» и «4_n»). Во втором случае принято, что нецелесообразно учитывать надежность средств контроля, поскольку они уже не выполнили свою функцию обнаружения отказа.

Вершинами «4_1», «4_2» и «4_n» показаны разные стадии разрегулировки системы. В построении последующих графов будем предполагать несколько стадий разрегулировки [2,3], причём условимся, что, чем больше индекс вершины, описывающей разрегулировку, тем больше в системе разрегулировка по параметру. Вообще, выделяют несколько стадий разрегулировки, например, можно считать, что в данном графе значение параметра находится в допусковой зоне; следующая стадия – нахождение параметра в области, обеспечивающей работоспособность системы; следующая – нахождение параметра в области устойчивого функционирования, выход за пределы которой приводит в состояние отказа; следующая – отказ системы, не приводящий к опасным последствиям и т.д. Возможно и другое назначение и стадий разрегулировки. К примеру, можно рассматривать две стадии разрегулировки: первая – когда величина параметра не равна номинальному значению, но это ещё не приводит к перемежающимся отказам; вторая – когда разрегулировка становится причиной перемежающихся отказов в аппаратуре.

Вершиной «5» показано состояние устройства, соответствующее явному отказу устройства. В него система может перейти из состояния исправности основного и контрольного оборудования (из вершины «0»), либо из состояния скрытого отказа (из вершины «3»), либо из состояния разрегулировки (из вершин «4_1», «4_2» и «4_n»).

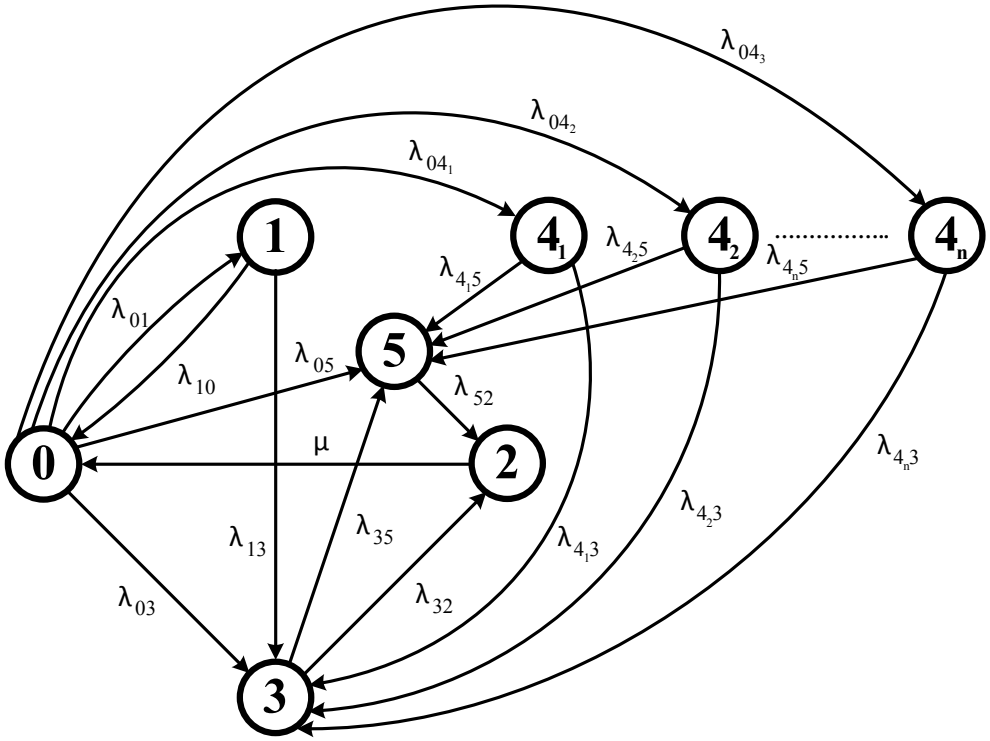

Рис. 1. Модель безопасности одноканального устройства с одноуровневым контролем и n-стадиями разрегулировки.

В данной задаче множество работоспособных состояний S_p=(0, 1); множество неработоспособных состояний $\overline{S}_p$ =(2, 3, 4_1, 4_2,...4_n, 5).

Для марковских случайных процессов с дискретными состояниями и дискретным временем матрица переходных вероятностей для данного графа приведена ниже [1].

$$\begin{vmatrix} P_{00} & P_{01} & 0 & P_{03} & P_{04_1} & P_{04_2} & \dots & P_{04_n} & P_{05} \\ P_{10} & P_{11} & 0 & P_{13} & 0 & 0 & \dots & 0 & 0 \\ P_{20} & 0 & P_{22} & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & P_{32} & P_{33} & 0 & 0 & \dots & 0 & P_{35} \\ 0 & 0 & 0 & P_{4_13} & P_{4_14_1} & 0 & \dots & 0 & P_{4_15} \\ 0 & 0 & 0 & P_{4_23} & P_{4_24_2} & 0 & \dots & 0 & P_{4_25} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & P_{4_33} & P_{4_34_3} & 0 & \dots & 0 & P_{4_35} \\ 0 & 0 & P_{52} & 0 & 0 & 0 & \dots & 0 & P_{55} \end{vmatrix}.$$

В случае непрерывной цепи Маркова, используя дифференциальные уравнения Колмогорова для данного графа, перейдём при $t \to \infty$ к система алгебраических уравнений [1]:

$$\left.\begin{aligned} &\lambda_{10} \cdot p_1(t) + \mu \cdot p_2(t) = (\lambda_{01} + \lambda_{03} + \lambda_{04_1} + \lambda_{04_2} \dots \lambda_{04_n} + \lambda_{05}) \cdot p_0(t) \\ &\lambda_{01} \cdot p_0(t) = (\lambda_{10} + \lambda_{13}) \cdot p_1(t) \\ &\lambda_{32} \cdot p_3(t) + \lambda_{52} \cdot p_5(t) = \mu \cdot p_2(t) \\ &\lambda_{03} \cdot p_0(t) + \lambda_{13} \cdot p_1(t) + \lambda_{4_13} \cdot p_{4_1}(t) + \lambda_{4_23} \cdot p_{4_2}(t) + \dots + \lambda_{4_n3} \cdot p_{4_n}(t) = (\lambda_{32} + \lambda_{35}) \cdot p_3(t) \\ &\lambda_{04_1} \cdot p_0(t) = (\lambda_{4_13} + \lambda_{4_15}) \cdot p_{4_1}(t) \\ &\lambda_{04_2} \cdot p_0(t) = (\lambda_{4_23} + \lambda_{4_25}) \cdot p_{4_2}(t) \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ &\lambda_{04_n} \cdot p_0(t) = (\lambda_{4_n3} + \lambda_{4_n5}) \cdot p_{4_n}(t) \\ &\lambda_{05} \cdot p_0(t) + \lambda_{35} \cdot p_3(t) + \lambda_{4_15} \cdot p_{4_1}(t) + \lambda_{4_25} \cdot p_{4_2}(t) \dots + \lambda_{4_n5} \cdot p_{4_n}(t) = \lambda_{52} \cdot p_5(t) \end{aligned}\right\}.$$

Таким образом, получена система линейных однородных алгебраических уравнений со следующими неизвестными: $p_0(t)$, $p_1(t)$, $p_2(t)$, $p_3(t)$, $p_{4_1}(t)$, $p_{4_2}(t), \dots,$ $p_{4_n}(t)$, $p_5(t)$. Одно из уравнений можно заменить на:

$$p_0(t) + p_1(t) + p_2(t) + p_3(t) + p_{4_1}(t) + p_{4_2}(t) \dots + p_{4_n}(t) + p_5(t) = 1.$$

Данную систему уравнений решить известными алгебраическими методами достаточно сложно, поэтому предлагается воспользоваться численным методом.

Рассмотренный граф не учитывает возможные изменения системы при техническом обслуживании (ТО). Далее рассмотрим модель безопасности одноканального устройства, учитывающая надёжность аппаратуры диагностики и квалификацию обслуживающего персонала, в которой этот аспект учтён, причём время технического обслуживания намного меньше времени между окончанием предыдущего и началом следующего цикла ТО.

Анализируя рассмотренный граф, можно сделать вывод, что повышение адекватности моделей возможно за счёт учёта в графах специфических свойств процесса технического обслуживания систем. Практически все свойства процесса эксплуатации устройств зависят от профессиональной квалификации обслуживающего персонала.

Соответственно от неё напрямую зависит длительность технического обслуживания системы, вероятности переходов системы из одной стадии разрегулировки в другую и т.д.

На рис. 2 вершиной «0» показано состояние исправности основного и контрольного оборудования устройства. В него система может попасть после ТО средств контроля (вершина «ТОК») или планового ТО основного оборудования (вершина «ТОО») или из состояния восстановления (вершина «2»).

Вершиной «1» показано состояние отказа первого комплекта контролирующего оборудования, которое не влияет на работу основного устройства. В него система может перейти из вершины «0» или «1'».

В предыдущих графах рассматривался одноуровневый контроль, при котором отказ средств контроля не вызывает отказ основного устройства. В данном графе используется двухуровневый контроль, подразумевающий введение в состав устройства средств контроля основного и, отдельно, контрольного оборудования с вероятностями правильного обнаружения, например, α_1 и α_2 соответственно [4]. Это означает, что объем контрольного оборудования увеличен и составит: $W_{\hat{e}_2} = W_{\hat{e}_1} + W_{\hat{e}\hat{i}}$, где $W_{\hat{e}\hat{i}} = f(\alpha_1)$, а $W_{\hat{e}_1} = f(\alpha_2)$.

При двухуровневом контроле отказ средств контроля обнаруживается с вероятностью α_2, восстанавливается и при последующем отказе основной аппаратуры отказ может не возникнуть. Если же откажет аппаратура контроля второго уровня объемом $W_{\hat{e}_1}$, то это приведет к переходу от двухуровневого к одноуровневому контролю.

При n-уровневом контроле объем контрольного оборудования увеличивается до:
$W_{\hat{e}_n} = W_{\hat{e}_{(n-1)}} + ... + W_{\hat{e}_1} + W_{\hat{e}_o}$, где $W_{\hat{e}_{(n-1)}} = f(\alpha_n),\ ..., W_{\hat{e}_1} = f(\alpha_2),\ W_{\hat{e}\hat{i}} = f(\alpha_1)$.

Вершиной «1'» показано состояние отказа второго комплекта контролирующего оборудования, при этом система переходит к одноуровневому контролю. В вершину «1'» система может перейти из вершины «0».

Состояние «2» – состояние восстановления, которое наступает либо после обнаружения явного отказа основного оборудования (из вершины «5»), либо по истечении некоторого (обычно большого) времени существования скрытого отказа основного оборудования, когда факт этого отказа каким-то образом проявился (из вершины «3»).

Вершиной «3» показано состояние скрытого отказа устройства. В данное состояние устройство попадает либо по причине отказа средств контроля и последующего отказа основного оборудования (из вершины «0»), либо по причине пропуска отказа средствами контроля (из вершины «1»), либо из вершин «3'» или «4'». Во втором случае принято, что нецелесообразно учитывать надежность средств контроля, поскольку они уже не выполнили свою функцию обнаружения отказа.

Вершина «3'» – работа в состоянии скрытого отказа. В данном случае после планового технического обслуживания (ПТО) разрегулировка не обнаружена. ПТО осуществляется с целью предотвращения внезапных переходов в отказ на совокупность функциональных блоков, узлов и элементов аппаратуры. Предполагается, что через время Т будет производиться ПТО. В вершину «3'» система может попасть только из вершины «3».

Вершина «ТОО» соответствует состоянию ПТО системы. Из данной вершины через определённое время с вероятностью 1 аппаратура переходит в состояние «0». Переход в данную вершину осуществляется только из вершины «0».

Вершина «ТОК» соответствует состоянию ремонта аппаратуры контроля первого уровня (ПТО не является). Переход в данную вершину осуществляется только из вершины «1».

Вершиной «4» показано состояние устройства, соответствующее проверке параметров при наличии разрегулировки системы. В него система может перейти из состояния исправности основного и контрольного оборудования (вершина «0»).

Вершина «4'» описывает состояние работы при разрегулировке системы (предполагается, что после ПТО разрегулировка не обнаружена), которое является промежуточным между состоянием исправности основного и контрольного оборудования (вершина «0») и скрытым (вершина «3») или явным (вершина «5») отказами. В данном случае разрегулировка рассматривается только по одному основному параметру. В вершину «4'» система может попасть только из вершины «4».

Вершиной «5» показано состояние устройства, соответствующее явному отказу устройства. В него система может перейти из состояния исправности основного и контрольного оборудования (из вершины «0»), либо из состояния скрытого отказа (из вершины «3»), либо из состояния разрегулировки (из вершины «4»).

В данной задаче множество работоспособных состояний S_p=(0, 1, 1', ТОК); множество неработоспособных состояний $\overline{S}_p$ =(2, 3, 3', 4, 4', 5,ТОО). На графе отмечены интенсивности потока событий.

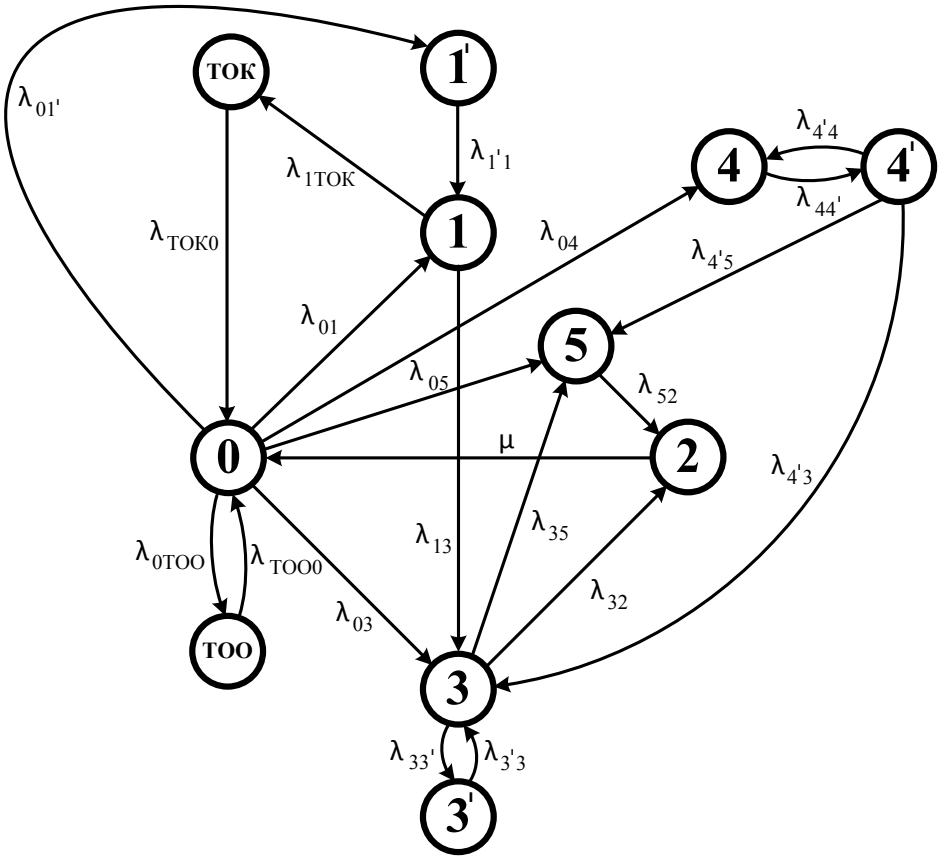

Рис. 2. Модель безопасности одноканального устройства, учитывающая надёжность аппаратуры диагностики и квалификацию обслуживающего персонала.

Для марковских случайных процессов с дискретными состояниями и дискретным временем матрица переходных вероятностей для данного графа приведена ниже.

$$\begin{vmatrix}
P_{00} & P_{01} & 0 & 0 & P_{03} & 0 & P_{04} & 0 & P_{05} & P_{0TOO} & 0 \\
0 & P_{11} & 0 & 0 & P_{13} & 0 & 0 & 0 & 0 & 0 & P_{1TOK} \\
0 & P_{1'1} & P_{1'1'} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
P_{20} & 0 & 0 & P_{22} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & P_{32} & P_{33} & 0 & 0 & 0 & P_{35} & 0 & 0 \\
0 & 0 & 0 & 0 & P_{3'3} & P_{3'3'} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & P_{44} & P_{44'} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & P_{4'3} & 0 & P_{4'4} & P_{4'4'} & P_{4'5} & 0 & 0 \\
0 & 0 & 0 & P_{52} & 0 & 0 & 0 & 0 & 0 & P_{55} & 0 \\
P_{TOO0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{TOOTOO} & 0 \\
P_{TOK0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{TOKTOK}
\end{vmatrix}.$$

В случае непрерывной цепи Маркова, используя дифференциальные уравнения Колмогорова для данного графа, перейдём при $t \to \infty$ к система алгебраических уравнений:

$$\left.\begin{aligned}
&\lambda_{TOK0} \cdot p_{TOK} + \mu \cdot p_2 + \lambda_{TOO0} \cdot p_{TOO} = (\lambda_{01} + \lambda_{03} + \lambda_{04} + \lambda_{05} + \lambda_{0TOO} + \lambda_{01'}) \cdot p_0 \\
&\lambda_{1'1} \cdot p_{1'} + \lambda_{01} \cdot p_0 = (\lambda_{1TOK} + \lambda_{13}) \cdot p_1 \\
&\lambda_{01'} \cdot p_0 = \lambda_{1'1} \cdot p_{1'} \\
&\lambda_{32} \cdot p_3 + \lambda_{52} \cdot p_5 = \mu \cdot p_2 \\
&\lambda_{03} \cdot p_0 + \lambda_{13} \cdot p_1 + \lambda_{4'3} \cdot p_{4'} + \lambda_{3'3} \cdot p_{3'} = (\lambda_{32} + \lambda_{35} + \lambda_{33'}) \cdot p_3 \\
&\lambda_{33'} \cdot p_3 = \lambda_{3'3} \cdot p_{3'} \\
&\lambda_{04} \cdot p_0 + \lambda_{4'4} \cdot p_{4'} = \lambda_{44'} \cdot p_4 \\
&\lambda_{44'} \cdot p_4 = (\lambda_{4'3} + \lambda_{4'4} + \lambda_{4'5}) \cdot p_{4'} \\
&\lambda_{05} \cdot p_0 + \lambda_{35} \cdot p_3 + \lambda_{4'5} \cdot p_{4'} = \lambda_{52} \cdot p_5 \\
&\lambda_{0TOO} \cdot p_0 = \lambda_{TOO0} \cdot p_{TOO} \\
&\lambda_{1TOK} \cdot p_1 = \lambda_{TOK0} \cdot p_{TOK}
\end{aligned}\right\}.$$

Таким образом, получена система из 11-ти линейных однородных алгебраических уравнений со следующими неизвестными: p_0, p_1, $p_{1'}$, p_2, p_3, $p_{3'}$, p_4, $p_{4'}$, p_5, p_{TOO}, p_{TOK}. Одно из уравнений можно заменить на:

$$p_0 + p_1 + p_{1'} + p_2 + p_3 + p_{3'} + p_4 + p_{4'} + p_5 + p_{TOO} + p_{TOK} = 1.$$

Рассмотренный граф составлен в предположении, что время обслуживания системы много меньше времени, проходящего между ПТО, то есть $t_{TO} << T$. При таком предположении не рассматривается вероятность появления отказа во время самого процесса технического обслуживания. В реальных условиях эксплуатации сложных систем (к таковым относятся и любые устройства обеспечения безопасности движения на железнодорожном транспорте) время их обслуживания бывает ненамного меньше времени между окончанием обслуживания в предыдущем цикле и началом его в последующем ($T_Ц$). Если время t_{TO} увеличивается, то возрастает вероятность перехода системы из состояния ТО в состояние отказа (скрытого или явного). Хорошо известны случаи, что после проведения профилактическим мер, исправная аппаратура вдруг оказывалась

неисправной. Поэтому предлагается в следующих моделях учесть данную особенность эксплуатации систем.

ЛИТЕРАТУРА:

[1] Вентцель Е.С. Исследование операций: задачи, принципы, методология. – 2-ое изд., стер. – М.: Наука.. Гл. ред. физ.-мат. лит., 1988. – 208 с. – (Пробл. науки и техн. прогресса). – ISBN 5-02-013900-9.

[2] Держо Г.Г. Количественная оценка вклада систем связи в безопасность технологических процессов на железнодорожном транспорте: Монография. – М.: ГОУ «Учебно–методический центр по образованию на железнодорожном транспорте», 2007. – 130 с.

[3] Михайлов А.В. Эксплуатационные допуски и надёжность радиоэлектронной аппаратуры. – М.: Сов. Радио, 1970. – 216 с.

[4] Розенберг Е.Н. Многоуровневая система управления и обеспечения безопасности движения поездов: дис. … д–ра техн. Наук / Е.Н. Розенберг; Всероссийский научно–исследовательский и конструкторско–технологический институт подвижного состава (ВНИКТИ МПС России). – Москва, 2004. – 317 с.

MODELS OF FUNCTIONAL SAFETY MICROPROCESSOR SYSTEMS OF RAILWAY AUTOMATION, REMOTE CONTROL AND COMMUNICATION

Mashchenko Pavel
maschich@mail.ru

Department of Automation, Remote Control and Communication on railway transport
Moscow State University of Railway Engineering (MGUPS (MIIT)), Moscow,
RUSSIA

Key words*: safety, maintenance, qualified staff.*

Abstract*: In recent years, to describe the operation of technical systems has been applied probabilistic approach. The most appropriate mathematical apparatus for this purpose is a probability theory for Markov and semi-Markov random processes. In article describes two models of functional safety microprocessor-weed systems of railway automation, remote control and communication, namely:*

- Security model single-channel devices with single-level control and the n-stages of misalignment;

- A single-channel device security model that takes into account the reliability of diagnostic equipment and qualified staff.