Мишучков В.И., Обычайко Д.С., Хрисостому Г., Шихин В.А.

Поддержание работоспособности кибер-физической системы посредством введения актуализируемого показателя эксплуатационной надежности

Аннотация: Восстановление работоспособности кибер-физических систем (КФС) как фактор безопасности функционирования энергообъектов рассматривается в отношении чрезвычайно-критического и критического оборудования в составе КФС и деления полного жизненного цикла на временные срезы, соответствующие предаварийному, аварийному, восстановленному и спрогнозированному состояниям. На основе построенных графов формулируется задача определения вероятности восстановления соответствующих компонент. Вводятся дифференциальные уравнения, связывающие вероятности восстановления кибернетических и физических компонент с интенсивностями отказов и восстановлений различного типа. Решение данных обыкновенных дифференциальных уравнений допускает аналитическое решение с ясной графической интерпретацией по временной области, где отображается изменение вероятности перехода компонентов системы из одного состояния в другое. Результаты проведенных исследований пойдут в основу разработки алгоритма актуализации модели эксплуатационной надежности КФС на полном жизненном цикле.

Ключевые слова: энергобезопасность, надежность, кибер-физические системы, эксплуатационная надежность, жизненный цикл, граф состояний

Одними из основных показателей при оценке работоспособности КФС [1-3] являются показатели надёжности и безопасности [4]. КФС должны быть способны продолжать работу в непредвиденных обстоятельствах и оперативно адаптироваться к новым условиям работы, а также самовосстанавливаться в случае сбоев. Важно отметить, что использование сетевых и вычислительных устройств предоставляет возможности для организации направленных кибератак [5]. Все это повышает

необходимость и актуальность исследования факторов живучести КФС [6].

В промышленных системах принято весь состав оборудования подразделять на типы по отношению к сохранению работоспособности системы в целом: не критичное оборудование, низкий уровень критичности, средний уровень критичности, критическое, чрезвычайно критическое. Особо выделим чрезвычайно критическое (ЧК) и критическое (КР) оборудование. Рассмотрим систему, состоящую из двух типов компонентов: физических (ФК) и кибернетических (КК). Построим граф состояний указанной КФС.

Полагаем, что ФК имеют 2 варианта восстановления из аварийного состояния: автоматическое (повторное включение через определенный промежуток времени, включение резерва) и ручное (ремонтная бригада). КК имеют 3 варианта восстановления из аварийного состояния: автоматическое, ручное и восстановление по умолчанию.

Рассмотрим КФС на четырех временных срезах (рис. 1): предаварийное, аварийное, восстановленное, спрогнозированное состояние. Восстановление может происходить в ручном режиме (для ФК и КК), автоматически (для ФК и КК), по умолчанию (для КК).

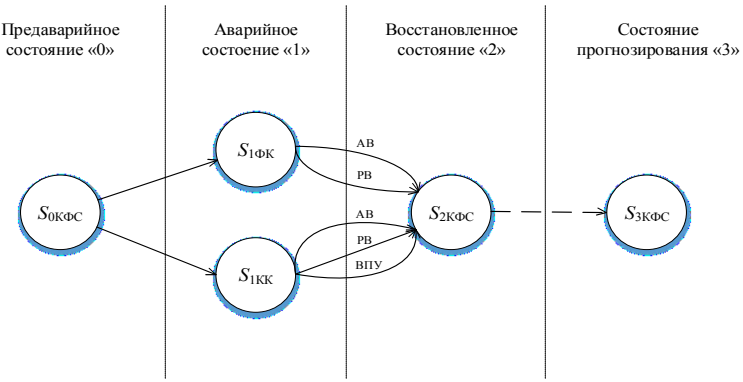

Рис. 1 – Граф состояний КФС-системы по отношению к чрезвычайно-критическому оборудованию

$S_{0КФС}$ – предаварийное состояние, компоненты системы в рабочем состоянии; $S_{1ФК}$ – аварийное состояние, вышел из строя физический компонент; $S_{1КК}$ – аварийное состояние, вышел из строя кибернетический компонент; $S_{2КФС}$ – восстановленное состояние КФС, компоненты системы в рабочем состоянии; $S_{3КФС}$ – спрогнозированное состояние КФС.

Для описания вероятности возврата системы из аварийного состояния в рабочее (из $S_{1ФК}$ в $S_{2КФС}$, из $S_{1КК}$ в $S_{2КФС}$) предлагается использовать дифференциальные уравнения:

(1)

$$\begin{cases} P_{12}^{ФК} = \alpha_{АВ}^{ЧК} \cdot \frac{dP_{12}^{ФК}}{dt} + \alpha_{РВ}^{ЧК} \cdot \frac{dP_{12}^{ФК}}{dt} - \beta_{АВ}^{ЧК} \cdot \frac{dP_{12}^{ФК}}{dt} - \beta_{РВ}^{ЧК} \cdot \frac{dP_{12}^{ФК}}{dt} + \gamma_1 \cdot P_{ЗАМ}^{ФК} + \gamma_2 \cdot P_{РЕМ}^{ФК} \\ P_{12}^{КК} = \alpha_{АВ}^{ЧК} \cdot \frac{dP_{12}^{КК}}{dt} + \alpha_{РВ}^{ЧК} \cdot \frac{dP_{12}^{КК}}{dt} + \alpha_{ВПУ}^{ЧК} \cdot \frac{dP_{12}^{КК}}{dt} - \beta_{АВ}^{ЧК} \cdot \frac{dP_{12}^{КК}}{dt} - \beta_{РВ}^{ЧК} \cdot \frac{dP_{12}^{КК}}{dt} - \beta_{ВПУ}^{ЧК} \cdot \frac{dP_{12}^{КК}}{dt} + \gamma_1 \cdot P_{ЗАМ}^{КК} + \gamma_2 \cdot P_{РЕМ}^{КК} \end{cases}$$

приведем уравнение (1) к следующему виду:

$$\begin{cases} P_{12}^{ФК} = (\alpha_{\_,} + \alpha_{\_,} - \beta_{\_;} - \beta_{\_;}) \cdot \frac{dP_{12}^{ФК}}{dt} + \gamma_{\_} \cdot P_{ЗАМ}^{ФК} + \gamma_{\_} \cdot P_{РЕМ}^{ФК} \\ P_{12}^{КК} = (\alpha_{\ ;} + \alpha_{\ ;} + \alpha_{\ ЛУ} - \beta_{\ ;} - \beta_{\ ;} - \beta_{\ ЛУ}) \cdot \frac{dP_{12}^{КК}}{dt} + \gamma_{\ } \cdot P_{ЗАМ}^{КК} + \gamma_{\ } \cdot P_{РЕМ}^{КК} \end{cases} \quad (2)$$

где $P_{12}^{ФК}$ – вероятность возврата системы в рабочее состояние (переход системы из состояния $S_{1ФК}$ в $S_{2КФС}$); $P_{12}^{КК}$ – вероятность возврата системы в рабочее состояние (переход системы из состояния $S_{1КК}$ в $S_{2КФС}$) $\alpha^{ЧК}_{АВ}$ – интенсивность автоматического восстановления ЧК-оборудования; $\alpha^{ЧК}_{РВ}$ – интенсивность ручного восстановления; $\alpha^{ЧК}_{ВПУ}$ – интенсивность восстановления по умолчанию; $\beta^{ЧК}_{АВ}$ – интенсивность отказа автоматического восстановления; $\beta^{ЧК}_{РВ}$ – интенсивность отказа ручного восстановления; $\beta^{ЧК}_{ВПУ}$ – интенсивность отказа восстановления по умолчанию; $P^{КК}_{ЗАМ}$, $P^{ФК}_{ЗАМ}$ – вероятность восстановления с помощью замены компонента; $P^{КК}_{РЕМ}$, $P^{ФК}_{РЕМ}$ – вероятность восстановления с помощью ремонта компонента; γ_1 – интенсивность замены компонента; γ_2 – интенсивность ремонта компонента.

Учет наличия ЗИП на объекте, времени доставки необходимых запчастей или нового изделия и приезд ремонтной бригады приводит к задержке. Это математически формализовано и выражается наличием эффекта запаздывания.

Уравнения в системе (2) связаны с введением дополнительного ограничения на значения интенсивностей восстановлений и отказов:

$$\alpha^{чк}_{АВ} \le 1,\ \alpha^{чк}_{РВ} \le 1,\ \alpha^{чк}_{ВПУ} \le 1,\ \beta^{чк}_{АВ} \le 1,\ \beta^{чк}_{РВ} \le 1,\ \beta^{чк}_{ВПУ} \le 1 \qquad (3)$$

При рассмотрении случая критического восстановление может происходить в ручном режиме (для ФК и КК) и по умолчанию (для КК). Описание вероятности возврата системы из аварийного состояния в рабочее в случае критического оборудования:

$$\begin{cases} P_{12}^{ФК} = \alpha_{РВ}^{р} \cdot \dfrac{dP_{12}^{ФК}}{dt} - \beta_{РВ}^{ур} \cdot \dfrac{dP_{12}^{ФК}}{dt} + \gamma_{1} \cdot P_{ЗАМ}^{ФК} + \gamma_{2} \cdot P_{РЕМ}^{ФК} \\ P_{12}^{КК} = \alpha_{РВ}^{р} \cdot \dfrac{dP_{12}^{КК}}{dt} + \alpha_{ВПУ}^{р} \cdot \dfrac{dP_{12}^{КК}}{dt} - \beta_{РВ}^{ур} \cdot \dfrac{dP_{12}^{КК}}{dt} - \beta_{ВПУ}^{ур} \cdot \dfrac{dP_{12}^{КК}}{dt} + \gamma_{1} \cdot P_{ЗАМ}^{КК} + \gamma_{2} \cdot P_{РЕМ}^{КК} \end{cases} \qquad (4)$$

приведем уравнение (4) к следующему виду:

$$\begin{cases} P_{12}^{ФК} = (\alpha_{1} - \beta_{1}) \cdot \dfrac{dP_{12}^{ФК}}{dt} + \gamma_{1} \cdot P_{ЗАМ}^{ФК} + \gamma_{2} \cdot P_{РЕМ}^{ФК} \\ P_{12}^{КК} = (\alpha_{1} + \alpha_{ВПУ} - \beta_{1} - \beta_{ВПУ}) \cdot \dfrac{dP_{12}^{КК}}{dt} + \gamma_{1} \cdot P_{ЗАМ}^{КК} + \gamma_{2} \cdot P_{РЕМ}^{КК} \end{cases} \qquad (5)$$

где по сравнению с системой уравнений (2) изменены способы восстановления, поскольку исключено автоматическое восстановление. Уравнения в системе (5) связаны с введением дополнительного ограничения на значения интенсивностей восстановлений и отказов:

$$\alpha^{кр}_{РВ} \le 1\ \alpha^{кр}_{ВПУ} \le 1,\ \beta^{кр}_{РВ} \le 1,\ \beta^{кр}_{ВПУ} \le 1 \qquad (6)$$

Физический смысл предложенной системы дифференциальных уравнений (2) состоит в том, чтобы отобразить зависимость вероятностей перехода ФК $P_{12}^{ФК}$ и КК $P_{12}^{КК}$ из одного состояния в другое с учетом реально изменяющейся интенсивности каждого возможного типа восстановления и изменяющихся потоков отказов восстановления. При известных начальных условиях вероятностей $P_{12}^{ФК}$, КК $P_{12}^{КК}$ и известных постоянных коэффициентах в правой части уравнений (определяются расчетным путем и/или на основе экспертных знаний) предложенная система обыкновенных линейных дифференциальных уравнений (2) и (5) имеет единственное решение, которое, в частности, допускает ясное графическое отображение во временной области. Это позволяет представить изменение вероятностей перехода компонентов

системы, как ФК, так и КК, из одного состояния в другое по временным срезам жизненного цикла исследуемой системы.

Граф состояний КФС на четырех временных срезах в соответствии с жизненным циклом системы позволяет в ясной форме представить особенности процесса восстановления системы относительно кибернетических компонент и физических компонент. На основе построенного графа предложена математическая формулировка и решение задачи по определению вероятности возврата работоспособности для физических и кибернетических компонент, основанное на введении дифференциальных уравнений, результат решения которых во многом определяется точностью определения констант, связанных с интенсивностями отказов и восстановлений различного типа. При известных начальных условиях вероятностей соответствующих состояний ФК и КК, а также при известных коэффициентах дифференциальных уравнений получаемое графическое отображение решения во временной области позволяет представить изменение вероятностей перехода компонентов системы из одного состояния в другое по временным срезам жизненного цикла исследуемой системы.

Литература:

1. *Antsaklis P.* Goals and challenges in cyber-physical system research // IEEE Transactions on Automatic Control. – 2014. – Vol. 59. – № 12. – P. 2017–2019.

2. *Fei Hu, Yu Lu, A. V. Vasilakos, et al.* Robust Cyber-Physical Systems: Concept, models, and implementation // Future generation computer systems. – 2016. – Vol. 56. – P. 449–475.

3. *Jay Lee, Behrad Bagheri, Hung-AnKao* Cyber-Physical Systems architecture for Industry 4.0 – based manufacturing systems // Manufacturing Letters. – 2015. – Vol. 3. – P. 18–23.

4. *Шихин В. А., Косинский М. Ю.* Исследование возможностей нечётких моделей для оценивания эксплуатационной надёжности автоматизированных систем // Мехатроника, автоматизация, управление. – 2009. – № 8. – С. 35–42.

5. *Yilin Mo, Bruno Sinopoli* On the Performance Degradation of Cyber-Physical Systems Under Stealthy Integrity Attacks // IEEE Transactions on Automatic Control. – 2016. – V. 61, № 9. – P. 2618-2624.

6. *Черкесов Г. Н.* Методы и модели оценки живучести сложных систем. / М.: Знание, 1987. – 32 с.