

А. А. БАЙБУЛАТОВ, В. Г. ПРОМЫСЛОВ  
ИПУ РАН, Москва

## О МЕТРИКЕ ДОСТУПНОСТИ ДЛЯ ПРОМЫШЛЕННЫХ СИСТЕМ УПРАВЛЕНИЯ

*Для современных систем управления на промышленных объектах свойство доступности является наиболее важным среди других компонентов, составляющих триаду информационной безопасности. Однако в политиках и программах безопасности обычно более широко освещаются свойства конфиденциальности и целостности, а свойству доступности уделяется сравнительно мало внимания. Более того, для оценки и поддержания безопасности используется целый ряд моделей, но ни одна из них непосредственно не связана со свойством доступности. Стараясь восполнить указанный пробел, в докладе рассматривается свойство доступности в контексте промышленных систем управления. Для идейной характеристики доступности предлагается использовать определение доступности по МЭК 62443, а в качестве количественной меры доступности – задержку передачи сигнала от источника до приемника. Для исследования свойства доступности предложена референтная модель. На основе задержки как меры выведена метрика доступности. Для расчета метрики предложено использовать системный анализ.*

**Введение.** При исследовании информационной безопасности промышленных систем управления обычно используется классическая модель, объединяющая три свойства: конфиденциальность, целостность и доступность, каждое из которых обладает своей степенью ценности. Известно, что для систем управления наиболее важным является свойство доступности. В частности, отсутствие доступности компонентов систем управления промышленных объектов важных для безопасности в результате кибератак увеличивает вероятность серьезных нарушений и угрожает безопасности самих объектов и окружающей среды в целом.

При оценке доступности функций промышленных систем управления возникает целый ряд задач. Одна из первых заключается в правильном выборе идейной интерпретации доступности, поскольку разные нормативные документы дают несколько различные определения понятию доступности. Другая проблема – как используя выбранную трактовку подобрать количественный показатель или меру доступности. Следующая проблема – как показатель или целый ряд показателей свести в одну количественную метрику. Одна из заключительных задач – разработать математический метод для расчета метрики.

Предлагаемый доклад посвящен исследованию свойства доступности для промышленных систем управления. Поясняется выбор определения доступности, предложена мера доступности и выведена метрика. Предложена референтная модель доступности и изложена идея для расчета метрики.

**Идея метрики доступности. Понятие доступности в международных стандартах.** При исследовании доступности и выборе определения, подходящего для систем управления промышленных объектов важных для безопасности, следует руководствоваться специализированными стандартами ИСО, МЭК, МАГАТЭ. При этом наиболее важными характеристиками, которые следует рассматривать при разработке метрики доступности, являются количественная измеримость и совместимость с системами важными для безопасности. В таблице представлены результаты анализа определений доступности в некоторых стандартах ИСО, МЭК, МАГАТЭ.

Т а б л и ц а

Анализ определений доступности

Стандарт	Количественная измеримость	Совместимость с системами важными для безопасности
ИСО/МЭК 27000 [1]	-	+
МАГАТЭ № NP-T-1.13 [2]	+	-
МАГАТЭ № SSG-39 [3]	-	+
МЭК 62645 [4]	-	+
МЭК 62443 [5]	+	+

Из проведенного анализа определений [6] следует, что наиболее подходящим является определение доступности согласно МЭК 62443 [5]: «свойство, гарантирующее своевременный и надежный доступ к информации и функциям, относящимся к системе управления, и их использование».

**Мера доступности.** Следуя определению МЭК 62443 в качестве объективного измеряемого показателя, или, другими словами, меры доступности удобно выбрать время передачи сигнала от источника до приемника или задержку. Важное преимущество задержки – количественная измеримость этого показателя: в условиях нормальной эксплуатации задержка является диагностической функцией и измеряется специальным программным обеспечением [7].

**Референтная модель доступности.** На основе задержки как меры доступности можно вывести универсальную метрику для количественной оценки доступности управления. Для этого необходимо построить модель, имея в виду, что доступность для промышленного объекта может быть представлена состоящей из 5-ти уровней [8]: физическое оборудование, организационный персонал, программно-технические средства + вычислительная сеть, организационный процесс, информация. В предлагаемом докладе рассмотрен только уровень программного обеспечения.

Для решения задач, связанных со свойством доступности в контексте промышленных систем управления, в частности, для количественной оценки доступности удобно использовать референтную модель [6] (рисунок). Концепции (домены), которые составляют модель, означают следующее. Метрика доступности – это абстрактная величина, основанная на соответствующих мерах доступности, которая служит для количественной оценки доступности. Функция – это одна из функций, для реализации которой служит рассматриваемая система управления. Под системой понимается архитектура системы. Платформа – это набор объектов, которые нуждаются в защите. Задержка – это измеряемая или оцениваемая величина времени прохождения сигнала с учетом архитектуры системы. Временные параметры – это параметры, для которых измеряется задержка.

Доступность	Метрика доступности
	Функция
	Система
	Платформа
	Задержка
	Временные параметры

Рисунок. Референтная модель доступности

**Метрика доступности.** При описании доступности системы управления и создании метрики в соответствии с референтной моделью, в первую очередь, необходимо рассмотреть домен Функция. Для простоты расчетов можно выбрать только одну функцию, например, функцию мониторинга. В соответствии с моделью доступность может быть выражена как следующая композиция:

$$\text{Доступность} = A \circ F \circ S \circ a \circ d(t),$$

где  $A$  – метрика доступности,  $F$  – выбранная функция,  $S$  – архитектура системы,  $a$  – платформа,  $d$  – задержка,  $t$  – временной вектор.

Метрика доступности может быть определена следующим образом [6]:

$$A = \begin{cases} 1 - \frac{d}{d_{max}}, & d < d_{max} \\ 0, & d \geq d_{max} \end{cases}, \quad (1)$$

где  $d$  – измеряемое или оцениваемое значение задержки для рассматриваемых временных параметров,  $d_{max}$  – заданное максимальное значение задержки, например, в соответствии с техническим заданием.

Для того чтобы обобщить метрику (1) и сделать ее более точной, необходимо рассмотреть домен Система, имея в виду, что в реальности задержка зависит от архитектуры системы, т. е. является составной величиной, включающей несколько временных интервалов.

Следуя системному подходу [9], можно применить понятие зависимости к домену Система. Для этого представим систему управления состоящей из совокупности  $n$  программных компонентов, т.е. рассмотрим передачу сигналов мониторинга по системе, состоящей из  $n$  компонентов.

Для задания показателя зависимости между программными компонентами рассмотрим матрицу зависимости [10]:

$$\begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{pmatrix}, \quad (2)$$

где  $c_{ij}=1$ , если компонент  $i$  зависит от компонента  $j$ , и  $c_{ij}=0$  в противном случае.

Тогда показатель зависимости системы управления в целом может быть выражен следующим образом:

$$\sum_{i=1}^n \sum_{j=1}^n c_{ij}. \quad (3)$$

Величина (3) особенно важна на этапах проектирования и пуско-наладки, когда проводятся плановые и внеплановые модификации системы.

С использованием показателя зависимости (3) задержка в системе управления может быть рассчитана следующим образом:

$$d = \sum_{i=1}^n \sum_{j=1}^n c_{ij} d_{ij}, \quad (4)$$

где  $d_{ij}$  означает время передачи сигнала от компонента  $i$  до компонента  $j$ , если  $i \neq j$ , и время выполнения компонента  $i$ , если  $i = j$ .

Из (1) и (4) метрика доступности может быть выражена:

$$A = \begin{cases} 1 - \frac{\sum_{i=1}^n \sum_{j=1}^n c_{ij} d_{ij}}{d_{max}}, & \sum_{i=1}^n \sum_{j=1}^n c_{ij} d_{ij} < d_{max} \\ 0, & \sum_{i=1}^n \sum_{j=1}^n c_{ij} d_{ij} \geq d_{max} \end{cases}. \quad (5)$$

Выражение (5) позволяет вычислять метрику доступности на основе знания структуры системы с использованием измеряемых временных интервалов прохождения сигналов и заданного максимального значения задержки.

**Заключение.** Выведенная в докладе метрика будет полезной для количественной оценки доступности на всех этапах жизненного цикла промышленных систем управления, поскольку задержка как мера измеряется в штатном режиме на этапе эксплуатации, а величина показателя зависимости может корректироваться на этапах проектирования и пуско-наладки.

#### ЛИТЕРАТУРА

1. ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO. 2018, 32 p.
2. IAEA Nuclear Energy Series No. NP-T-1.13 «Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants». IAEA, Vienna. 2015, 68+iv+viii p.
3. IAEA Safety Standards Series № SSG-39 «Design of Instrumentation and Control Systems for Nuclear Power Plants». IAEA, Vienna. 2016, 166+xvi p.
4. IEC 62645 Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems. IEC, Geneva. 2014, 93 p.
5. IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. IEC, Geneva. 2013, 170 p.
6. **Baybulatov A.A., Promyslov V.G.** "Industrial Control System Availability Assessment with a Metric Based on Delay and Dependency," IFAC-PapersOnLine. Elsevier, Amsterdam, vol. 54, issue 13, pp. 472-476, 2021.
7. **Promyslov V.G., Masolkin S.I.** "NPP APCS diagnostics implementation as a routine task of APCS," *IFAC Proceedings Volumes*, vol. 42, no. 2, pp. 221-225, 2009.

8. **Qadir S., Quadri S.M.K.** "Information Availability: An Insight into the Most Important Attribute of Information Security," *Journal of Information Security*, vol. 7, pp. 185-194, 2016.
9. **Avizienis A., Laprie J., Randell B.** "Fundamental Concepts of Dependability," *Proceedings of the 3rd IEEE Information Survivability Workshop (ISW-2000)*, pp. 7-12, 2000.
10. **Qadir S.M., Quadri S.M.K.** "Metric for Evaluating Availability of an Information System: A Quantitative Approach Based on Component Dependency," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 9, no. 2, pp. 1-11, 2017.

A.A.Baybulatov, V.G.Promyslov (RAS ICS, Moscow)

### **On availability metric for industrial control systems**

For modern control systems at industrial facilities, the availability property is the most important among other components comprising the information security triad. However, in security policies and programs, usually, the properties of confidentiality and integrity are described in detail, while the availability property is not paid much attention. Moreover, for the safety and security assessment and maintaining, a number of models are utilized, but none of them is related directly to availability. Trying to fill this gap, the article considers the availability property in the industrial control systems context. For characterizing availability, the IEC 62443 definition is suggested to use, and for the quantitative measure of availability, the delay of transmitting a signal from the source to the receiver is advocated. For the availability investigation, a reference model is proposed. On the basis of the delay as a measure, an availability metric is derived. For the metric calculation, dependability theory is suggested to utilize.