Сетевой научный журнал «Ресурсы» https://resources.today
Russian Journal of Resources

2026, Том 13, № 3 / 2026, Vol. 13, Iss. 3 https://resources.today/issue-3-2026.html

URL статьи: https://resources.today/PDF/21ECOR326.pdf

DOI: 10.15862/21ECOR326 (https://doi.org/10.15862/21ECOR326)

2.3.3. Автоматизация и управление технологическими процессами и производствами (технические науки)

Ссылка для цитирования этой статьи:
Непогода, Ф. В. Обеспечение отказоустойчивости распределенной системы управления приводами гибкого производственного участка / Ф. В. Непогода, А. В. Гончаров, А. В. Шаховской, Е. Г. Ротанов // Ресурсы. — 2026. — Т. 13. — № 3. — URL: https://resources.today/PDF/21ECOR326.pdf. DOI: 10.15862/21ECOR326.

For citation:
Nepogoda F.V., Goncharov A.V., Shakhovskoy A.V., Rotanov E.G. Ensuring fault tolerance of a distributed drive control system of a flexible manufacturing section. *Russian Journal of Resources*. 2026;13(3): 21ECOR326. Available at: https://resources.today/PDF/21ECOR326.pdf. DOI: 10.15862/21ECOR326. (In Russ., abstract in Eng.).

УДК 681.5.09

Непогода Филипп Владимирович
ФГБОУ ВО «Московский государственный университет технологий и управления имени К. Г. Разумовского», Москва, Россия
Аспирант

Гончаров Андрей Витальевич
ФГБОУ ВО «Московский государственный университет технологий и управления имени К. Г. Разумовского», Москва, Россия
Кандидат технических наук, доцент
E-mail: a.goncharov@mgutm.ru

Шаховской Андрей Владимирович
ФГБОУ ВО «Московский государственный университет технологий и управления имени К. Г. Разумовского», Москва, Россия
Кандидат технических наук, доцент
E-mail: a.shakhovskoy@mgutm.ru

Ротанов Евгений Геннадьевич
ФГБОУ ВО «Московский государственный университет технологий и управления имени К. Г. Разумовского», Москва, Россия
Кандидат технических наук, доцент
E-mail: e.rotanov@mgutm.ru

Обеспечение отказоустойчивости распределенной системы управления приводами гибкого производственного участка

Аннотация. Распределенные системы управления приводами, применяемые на гибких производственных участках, сокращают объем кабельных связей и упрощают переналадку, однако вместе с числом узлов и сетевых соединений возрастает число элементов, отказ которых останавливает станцию или весь участок. В работе обоснован подход, при котором отказоустойчивость системы управления оценивается не долей времени ее исправного состояния, а сохраняемой производительностью участка, а механизмы резервирования сопоставляются по вкладу в сокращение потерь рабочего времени. Объектом моделирования выступает участок из четырех обрабатывающих центров, робота-загрузчика и транспортно-

накопительной системы с 32 сервоприводами, шестью узлами управления станций и контроллером участка. Сопоставлены четыре архитектуры: базовая с линейными сетями; с кольцевым резервированием среды передачи; с дополнительным горячим резервом контроллера участка и переключением сети уровня приводов в пределах цикла обмена; авторская, дополненная переносом функций отказавшего узла станции на узел-партнер. Расчеты выполнены по марковским моделям и дискретно-событийной имитацией на интервале 20 тыс. лет функционирования с проверкой по аналитическому решению. Установлено, что авторская архитектура сокращает потери эквивалентного времени работы участка с 32,84 до 15,89 ч в год, то есть на 51,6 %, и почти вдвое уменьшает число полных остановов. Показано, что кольцевое резервирование сети уровня приводов дает эффект лишь при времени восстановления связи, не превышающем времени срабатывания сторожевого таймера приводов, а при восстановлении за 200 мс увеличивает число остановов станций, сокращая только их длительность. Перенос функций допустим для пар однотипных станций и пары «робот — транспортная система» по условию планируемости задач, тогда как размещение функций робота на узле обрабатывающего центра недопустимо. После введения всех механизмов 93 % остаточных потерь приходится на отказы самих сервоприводов, что задает предел отказоустойчивости, достижимый средствами системы управления. Результаты могут быть использованы при выборе архитектуры и протоколов резервирования систем управления гибких производств.

Ключевые слова: отказоустойчивость; распределенная система управления; сервопривод; гибкий производственный участок; резервирование; промышленная сеть реального времени; функциональная реконфигурация; производительность с учетом деградации; коэффициент готовности

Введение

Гибкое автоматизированное производство в современных условиях становится важнейшим инструментом обеспечения технологической независимости машиностроения, поскольку позволяет выпускать широкую номенклатуру изделий малыми партиями без длительной переналадки оборудования. Ядром такого производства выступает *гибкий производственный участок*[1], объединяющий обрабатывающие центры, промышленных роботов и транспортно-накопительные системы под управлением единой вычислительной среды. Особое место в его структуре занимает *система управления приводами*: именно через нее управляющие решения превращаются в перемещения рабочих органов, и именно ее отказ немедленно прерывает выпуск продукции.

Переход от централизованных систем числового программного управления к *распределенным* системам, в которых приводы, узлы управления станций и контроллер участка связаны промышленными сетями реального времени, существенно сократил объем кабельных связей, упростил наращивание состава оборудования и открыл возможность программной переконфигурации участка. Вместе с тем распределенность имеет и обратную сторону: возрастает число вычислительных узлов, разъемных соединений и программных компонентов, каждый из которых способен стать источником отказа. В связи с этим возрастающее значение

[1] Термин «гибкий производственный участок» используется в работе в значении понятия «гибкий автоматизированный участок», определяемого ГОСТ 26228-90 как «участок цеха, технологическое оборудование которого состоит преимущественно из гибких производственных систем, ячеек и модулей». См.: ГОСТ 26228-90. Системы производственные гибкие. Термины и определения, номенклатура показателей: государственный стандарт Союза ССР: введен 01.01.1991. — Приложение 1.

приобретает *отказоустойчивость*[2] системы управления приводами, то есть ее способность продолжать выполнение необходимых функций при отказах отдельных элементов. Острота проблемы определяется масштабами потерь от незапланированных простоев. По оценке компании Siemens, в 2024 г. крупное промышленное предприятие теряло из-за таких простоев в среднем 27 ч в месяц, а совокупные потери пятисот крупнейших компаний мира достигли 11 % их выручки, или около 1,4 трлн долл. в год.[3]

Отметим, что проблема построения надежных систем из ненадежных элементов была поставлена задолго до появления гибких производств. Еще в 1956 г. Дж. фон Нейман показал, что надежность вычислительной структуры может быть повышена сколь угодно введением избыточности и мажоритарного голосования, даже если отдельные элементы отказывают с заметной вероятностью [1]. В том же году Э. Мур и К. Шеннон доказали аналогичный результат для релейных схем [2]. Сам термин «отказоустойчивые вычисления» (fault-tolerant computing) ввел в научный оборот А. Авиженис в 1967 г. [3], а спустя почти четыре десятилетия он вместе с Ж.-К. Лапри, Б. Рэнделлом и К. Лэндвером систематизировал понятийный аппарат направления [4]. Нам импонирует предложенная этими авторами трактовка: надежность в широком смысле (dependability) понимается ими как «способность предоставлять услугу, которой можно обоснованно доверять», а отказоустойчивость — как средство «избегать отказов обслуживания при наличии неисправностей» (перевод наш) [4]. Для нас эта трактовка принципиальна, поскольку переносит акцент с исправности элементов на сохранение *услуги*, которую система оказывает объекту управления.

В современной научной литературе сложились три направления, непосредственно связанные с обеспечением отказоустойчивости распределенных систем управления приводами.

Первое направление образуют работы по отказоустойчивому управлению динамическими объектами. М. Бланке, М. Киннэр, Я. Лунце и М. Старошвецки обобщили методы диагностирования и аккомодации отказов, при которых закон управления перестраивается после обнаружения дефекта [5]. Ю. Чжан и Дж. Цзян систематизировали подходы к реконфигурируемому отказоустойчивому управлению и разделили их на пассивные, рассчитанные на заранее известный перечень отказов, и активные, опирающиеся на диагностирование и перестройку системы [6]. Р. Изерман связал диагностирование неисправностей с последующим обеспечением отказоустойчивости [7]. В отечественной литературе основы функционального диагностирования динамических систем заложены Л. А. Мироновским [8], а современное развитие этого подхода представлено, в частности, в работе А. Н. Жирабока, В. Ф. Филаретова, А. В. Зуева и А. Е. Шумского, предложивших метод обеспечения отказоустойчивости систем управления с полной или частичной развязкой от дефектов [9].

Второе направление посвящено сетевым системам управления и промышленным коммуникациям. Дж. Эспанья, П. Нагштабризи и Ю. Сюй обобщили результаты анализа систем управления, замкнутых через канал связи с задержками и потерями пакетов [10]. М. Фельзер проанализировал промышленные сети Ethernet реального времени [11], а Х. Кирманн, М. Ханссон и П. Мюри обосновали протокол параллельного резервирования, обеспечивающий восстановление без прерывания обмена [12].

---

[2] Термин «отказоустойчивость» употребляется в значении понятия «устойчивость к отказам» по пункту 3.6.3 ГОСТ Р МЭК 61508-4-2012 как «способность функционального блока продолжать выполнять необходимую функцию при наличии сбоев или ошибок». См.: ГОСТ Р МЭК 61508-4-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения: национальный стандарт Российской Федерации: введен 01.08.2013. — URL: https://meganorm.ru/mega_doc/norm/gost-r_gosudarstvennyj-standart/18/gost_r_mek_61508-4-2012_natsionalnyy_standart_rossiyskoy.html (дата обращения: 23.10.2026).

[3] The True Cost of Downtime 2024 / Siemens AG. — 2024. — URL: https://assets.new.siemens.com/siemens/assets/api/uuid:1b43afb5-2d07-47f7-9eb7-893fe7d0bc59/TCOD-2024_original.pdf (дата обращения: 23.10.2026).

Третье направление связано с реконфигурируемыми производственными системами и архитектурой их программного обеспечения. Ё. Корен и соавторы сформулировали концепцию реконфигурируемых производственных систем, способных изменять структуру в ответ на изменение производственных условий [13].

В. Вяткин показал, что распределенные функциональные блоки стандарта IEC 61499 позволяют перемещать функции управления между вычислительными узлами [14], а Г. М. Мартинов и соавторы развили методы декомпозиции и синтеза специализированных систем числового программного управления [15].

Перечисленные направления развиваются во многом обособленно. Отказоустойчивость систем управления оценивается, как правило, по вероятности безотказной работы или коэффициенту готовности самой системы, тогда как для гибкого участка значима не исправность системы управления сама по себе, а *сохраняемая производительность*. Вопрос о том, какой вклад в производительность участка вносит каждый механизм отказоустойчивости и при каких условиях резервирование действительно маскирует отказ, остается открытым.

Объектом исследования выступает распределенная система управления приводами гибкого производственного участка механической обработки.

Предметом исследования являются механизмы обеспечения отказоустойчивости этой системы и их влияние на производительность участка.

Цель исследования состоит в обосновании состава механизмов отказоустойчивости, обеспечивающего наибольшее сокращение потерь производительности гибкого производственного участка, и в определении условий, при которых эти механизмы сохраняют эффективность.

1. Материалы и методы

Опираясь на положения теории надежности и отказоустойчивого управления, уточним используемый понятийный аппарат. *Распределенной системой управления приводами* в работе названа совокупность контроллера участка, узлов управления станций, сервоприводов и связывающих их сетей реального времени, в которой функции управления движением распределены по нескольким вычислительным узлам.

Под *механизмом отказоустойчивости* понимается аппаратное, сетевое или программное средство, которое при отказе элемента сохраняет выполнение функции полностью либо с допустимым снижением качества. Считаем принципиально важным, что для гибкого участка мерой отказоустойчивости должна служить *сохраняемая производительность*: отказ одного обрабатывающего центра снижает выпуск лишь частично, а отказ робота-загрузчика или контроллера участка останавливает участок полностью.

Эмпирической базой послужила расчетная модель участка механической обработки, состав которого типичен для гибких производств машиностроения. Участок включает четыре взаимозаменяемых обрабатывающих центра (ОЦ1–ОЦ4) с пятью сервоприводами каждый, робот-загрузчик на линейной оси с семью приводами и транспортно-накопительную систему (ТНС) с пятью приводами штабелера и конвейера паллет, всего 32 сервопривода.

Каждая станция имеет собственный узел управления, а координацию маршрутов деталей, загрузки и транспортировки выполняет контроллер участка. Приводы станции соединены с ее узлом последовательной сетью реального времени с циклом обмена 1 мс, узлы станций и контроллер участка — магистральной сетью, допустимое время прерывания обмена в которой принято равным 0,5 с. Характеристика элементов и принятые значения показателей их безотказности и ремонтопригодности приведены в таблице 1.

Таблица 1

Характеристика элементов распределенной системы управления приводами гибкого производственного участка и исходные данные для расчета

Элемент	Число элементов в архитектуре A1	Число элементов в архитектурах A2–A4	Средняя наработка на отказ, ч	Среднее время восстановления, ч	Последствие отказа в архитектуре A1
Сервопривод (усилитель, двигатель, датчик положения)	32	32	80 000	8,0	останов станции
Кабельный сегмент сети уровня приводов	32	38	40 000	2,0	останов станции
Узел управления станции, аппаратный отказ	6	6	60 000	12,0	останов станции
Узел управления станции, программный сбой	6	6	6 000	0,5	останов станции
Контроллер участка, аппаратный отказ	1	1–2	60 000	12,0	останов участка
Контроллер участка, программный сбой	1	1–2	6 000	0,5	останов участка
Сегмент магистральной сети участка	6	7	150 000	3,0	отключение станций за местом обрыва

Значения наработки и времени восстановления приняты расчетными; время восстановления включает ожидание запасных частей и повторный пуск. В архитектуре A2 контроллер участка один, в архитектурах A3 и A4 — два. Составлено авторами

Данные таблицы 1 свидетельствуют о том, что наиболее часто в системе отказывают не аппаратные средства вычислительных узлов, а их программное обеспечение и кабельные соединения уровня приводов. На участке ежегодно следует ожидать в среднем около десяти программных сбоев узлов и контроллера участка и семи-восьми отказов кабельных сегментов, тогда как аппаратные отказы вычислительных узлов происходят примерно один раз в год. Сервоприводы отказывают в среднем 3,5 раза в год, и их отказы сопряжены с наибольшим временем восстановления; средствами системы управления они не маскируются, поскольку станция утрачивает движение одной из осей.

Сопоставлены четыре архитектуры распределенной системы управления, последовательно наращивающие состав механизмов отказоустойчивости:

- *архитектура A1* (базовая) — линейные сети на уровне приводов и участка, один контроллер участка, функции каждого узла жестко закреплены за ним;
- *архитектура A2* — кольцевые топологии сетей обоих уровней с протоколом резервирования среды класса 200 мс[4];
- *архитектура A3* — архитектура A2, дополненная горячим резервом контроллера участка и переключением сети уровня приводов в пределах одного цикла обмена;

[4] Стандарт IEC 62439-2 устанавливает для протокола резервирования среды MRP классы гарантированного времени восстановления 500, 200, 30 и 10 мс.

Протоколы PRP и HSR по IEC 62439-3 обеспечивают переключение без прерывания обмена, а механизм резервирования кабеля сети EtherCAT, по данным EtherCAT Technology Group, восстанавливает связь менее чем за 15 мкс. См.: IEC 62439-2:2021. Industrial communication networks — High availability automation networks — Part 2: Media Redundancy Protocol (MRP).

IEC 62439-3:2021. Industrial communication networks — High availability automation networks — Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR). — URL: https://webstore.iec.ch/publication/64423 (дата обращения: 23.10.2026).

EtherCAT Technology / EtherCAT Technology Group. — URL: https://www.ethercat.org/en/technology.html (дата обращения: 23.10.2026).

- *архитектура А4* (авторская) — архитектура А3, дополненная функциональной реконфигурацией, при которой функции отказавшего узла управления станции переносятся на заранее назначенный узел-партнер.

Коэффициент готовности отдельного элемента рассчитывается по классической формуле (1) в записи Б. В. Гнеденко, Ю. К. Беляева и А. Д. Соловьева [16], где K_i — коэффициент готовности, T_i — средняя наработка на отказ, $T_{\text{в},i}$ — среднее время восстановления i-го элемента.

$$K_i = \frac{T_i}{T_i + T_{\text{в},i}}. \tag{1}$$

Состояние участка описывается вектором состояний элементов $x(t)$, компоненты которого равны единице для работоспособного и нулю для неработоспособного элемента. Авторская модель связывает это состояние с мгновенной относительной производительностью участка $r(t)$ формулой (2), где φ_0 — структурная функция «ядра» участка, равная единице при работоспособности контроллера участка, робота-загрузчика, ТНС и сетевых связей с ними, φ_j — структурная функция j-го обрабатывающего центра с учетом его приводов, сетевых связей и узла управления. Модель отражает технологическую особенность участка: обрабатывающие центры взаимозаменяемы, и при отказе одного из них маршруты деталей перераспределяются между остальными, тогда как робот и ТНС обслуживают все станции и резерва не имеют.

$$r(t) = \varphi_0\big(x(t)\big) \cdot \frac{1}{4}\sum_{j=1}^{4} \varphi_j\big(x(t)\big). \tag{2}$$

Интегральной мерой отказоустойчивости служит производительность с учетом деградации (от англ. performability), введенная Дж. Мейером для систем, сохраняющих работоспособность с пониженной эффективностью [17]. В стационарном режиме она определяется формулой (3), где P — средняя относительная производительность, r_i — относительная производительность в i-м состоянии, π_i — стационарная вероятность этого состояния. Для наглядности величина (3) пересчитана в потери эквивалентного времени работы участка L по формуле (4), где Φ = 8760 ч — годовой фонд времени при непрерывной работе.

$$P = \lim_{T\to\infty} \frac{1}{T}\int_0^T r(t)\mathrm{d}t = \sum_i r_i \pi_i. \tag{3}$$

$$L = \Phi(1 - P). \tag{4}$$

Ключевым параметром резервированных структур выступает *покрытие* (от англ. coverage), то есть условная вероятность того, что отказ будет обнаружен и отработан без нарушения функционирования. Влияние покрытия на готовность восстанавливаемой системы исследовал Т. Арнольд [18], показавший, что даже небольшая доля неотработанных отказов существенно снижает выигрыш от резервирования. Для дублированного контроллера участка построена марковская модель, учитывающая аппаратные отказы и программные сбои каждого комплекта, неотработанное переключение с последующим ручным переводом на резерв и одновременную неработоспособность обоих комплектов. Стационарные вероятности ее состояний находятся из системы (5) в общепринятой записи К. Триведи и А. Боббио [19], где π — вектор стационарных вероятностей, Q — матрица интенсивностей переходов. В расчетах принято покрытие c = 0,95 и среднее время ручного переключения 0,25 ч.

$$\pi Q = 0, \sum_i \pi_i = 1. \tag{5}$$

Особого внимания заслуживает резервирование сети уровня приводов. Сервопривод контролирует поступление управляющих телеграмм сторожевым таймером и при пропуске нескольких циклов обмена переводит ось в безопасный останов. Следовательно, кольцевая топология маскирует отказ кабельного сегмента лишь тогда, когда время восстановления связи не превышает времени срабатывания таймера. Авторская запись этого условия представлена формулой (6), где $c_{\text{эф}}$ — эффективное покрытие резервирования сети, $\mathbf{1}(\cdot)$ — индикаторная функция, $t_{\text{в}}$ — гарантированное время восстановления связи, n_w — допустимое число пропущенных циклов, $T_{\text{ц}}$ — период цикла обмена. В расчетах принято $n_w = 3$. Если условие не выполняется, отказ сегмента приводит к срабатыванию таймера и станция останавливается на время повторного пуска, принятое равным 0,25 ч, однако ремонта кабеля не ожидает, поскольку кольцо уже восстановило связь.

$$c_{\text{эф}} = c \cdot \mathbf{1}\left(t_{\text{в}} \le n_w T_{\text{ц}}\right). \tag{6}$$

Функциональная реконфигурация в архитектуре А4 состоит в том, что при обнаружении отказа узла управления станции его задачи активируются на узле-партнере, где они заранее размещены в резервном режиме. Станция при этом выполняет управляемый останов и возобновляет работу через 0,05 ч уже под управлением узла-партнера, не ожидая ремонта. Перенос допустим, если объединенный набор задач остается планируемым. Достаточное условие планируемости при назначении приоритетов по частоте задач получено К. Лю и Дж. Лейлендом и записывается формулой (7) [20], где U — суммарная загрузка процессора, C_i и T_i — время выполнения и период i-й задачи, n — число задач. Поскольку условие (7) является лишь достаточным, допустимость переноса проверялась также точным анализом времени отклика по формуле (8), предложенной М. Джозефом и П. Пандья [21], где R_i — время отклика i-й задачи, $hp(i)$ — множество задач с более высоким приоритетом, D_i — допустимый срок выполнения, равный периоду. Набор задач каждого узла включает позиционное управление осями с периодом 1 мс (для ТНС — 2 мс), логику станции с периодом 10 мс, обмен с контроллером участка и диагностирование с периодом 20 мс и задачи человеко-машинного интерфейса с периодом 100 мс; при переносе добавляется задача удаленного обмена с приводами отказавшей станции.

$$U = \sum_{i=1}^{n} \frac{C_i}{T_i} \le n\left(2^{\frac{1}{n}} - 1\right). \tag{7}$$

$$R_i = C_i + \sum_{j \in hp(i)} \left\lceil \frac{R_i}{T_j} \right\rceil C_j \le D_i. \tag{8}$$

Вклад отдельных групп элементов в потери оценивался мерой значимости, восходящей к работе З. Бирнбаума [22], в которой значимость элемента определяется приростом показателя системы при переходе элемента из неработоспособного состояния в работоспособное. Авторская модификация состоит в том, что вместо вероятности работоспособности используется производительность с учетом деградации, а значимость группы элементов k измеряется потенциалом сокращения потерь по формуле (9), где $L(\lambda)$ — потери при исходных интенсивностях отказов, $L(\lambda \mid \lambda_k = 0)$ — потери при условно безотказных элементах группы k.

$$\Delta L_k = L(\lambda) - L(\lambda \mid \lambda_k = 0). \tag{9}$$

Показатели архитектур рассчитаны дискретно-событийной имитацией. Динамические деревья отказов Дж. Дуган, С. Бавузо и М. Бойда [23] для данной задачи оказались недостаточны, поскольку исход отказа зависит от текущей конфигурации системы: занятости узла-партнера, числа уже отказавших сегментов кольца, состояния резервного комплекта

контроллера. Для каждого элемента моделировалось чередование интервалов работоспособности и восстановления с экспоненциальными распределениями, параметры которых приведены в таблице 1, а исход каждого отказа (отработан, не отработан, перенесен) определялся с учетом покрытия и текущего состояния остальных элементов. Каждый элемент имел собственный поток случайных чисел, благодаря чему архитектуры сопоставлялись на одних и тех же реализациях отказов. Для оценки показателей выполнено 20 независимых прогонов продолжительностью 1000 лет функционирования каждый, доверительные интервалы построены по формуле (10), где $\overline{P}$ — среднее по прогонам, s — выборочное стандартное отклонение, $N = 20$ — число прогонов, $t_{0,975;N-1}$ — квантиль распределения Стьюдента. Потенциал (9) и чувствительность к покрытию рассчитаны на прогонах продолжительностью 20 тыс. и 8 тыс. лет соответственно. Логика исследования представлена на рисунке 1.

$$\overline{P} \pm t_{0,975;N-1} \cdot \frac{s}{\sqrt{N}} \tag{10}$$



Рисунок 1. *Схема обеспечения и оценки отказоустойчивости распределенной системы управления приводами гибкого производственного участка (составлено авторами)*

2. Результаты и обсуждение

Рассмотрим прежде всего достоверность имитационной модели. Для архитектуры A1, все элементы которой соединены последовательно в пределах «ядра» участка и каждой станции, производительность (3) допускает точный аналитический расчет через коэффициенты

готовности (1). Аналитическая оценка потерь составила 32,99 ч в год, имитационная — 32,84 ±0,27 ч; расхождение в 0,44 % находится в пределах доверительного интервала. Для дублированного контроллера участка неработоспособность по марковской модели (5) составила 0,0146 ч в год, по имитации — 0,0144 ч, что также подтверждает корректность модели. Отметим, что одиночный контроллер участка неработоспособен в среднем 2,48 ч в год, то есть дублирование с покрытием 0,95 сокращает этот показатель более чем в 150 раз.

Перейдем к сопоставлению архитектур. Показатели отказоустойчивости участка, рассчитанные по формулам (3), (4) и (10), сведены в таблицу 2.

Таблица 2

Показатели отказоустойчивости гибкого производственного участка при различных архитектурах распределенной системы управления приводами

Показатель	A1	A2	A3	A4
Производительность с учетом деградации, % номинальной	99,625 ±0,003	99,701 ±0,003	99,740 ±0,003	99,819 ±0,002
Потери эквивалентного времени работы, ч в год	32,84 ±0,27	26,19 ±0,25	22,74 ±0,23	15,89 ±0,19
Изменение потерь относительно архитектуры A1, %	—	−20,3	−30,8	−51,6
Доля времени работы с полной производительностью, %	99,313	99,451	99,501	99,657
Доля времени работы хотя бы с частичной производительностью, %	99,731	99,785	99,820	99,872
Число полных остановов участка в год	8,89	9,18	4,76	4,76
Средняя длительность полного останова, ч	2,65	2,06	3,31	2,35
Число остановов станций в год	21,28	21,48	13,57	13,58

Приведены средние значения и полуширина 95-процентного доверительного интервала по 20 прогонам продолжительностью 1000 лет. Рассчитано авторами по результатам имитационного моделирования.

Данные таблицы 2 свидетельствуют о том, что каждое расширение состава механизмов отказоустойчивости сокращает потери. Кольцевое резервирование сетей (A2) уменьшает их на 20,3 %, введение горячего резерва контроллера участка и быстрого переключения на уровне приводов (A3) — на 30,8 %, а авторская архитектура A4 — на 51,6 %, то есть более чем вдвое. Следует отметить неоднозначный результат архитектуры A2.

Число полных остановов участка при переходе к кольцевым сетям не сократилось, а возросло с 8,89 до 9,18 в год, тогда как средняя длительность останова уменьшилась с 2,65 до 2,06 ч. Объяснение мы видим в соотношении времени восстановления кольца и времени срабатывания сторожевого таймера приводов: восстановление за 200 мс многократно превышает время срабатывания таймера, поэтому обрыв кабельного сегмента по-прежнему останавливает станцию, хотя и на время повторного пуска, а не ремонта, а дополнительный сегмент, замыкающий кольцо, увеличивает число возможных мест отказа.

Переход к архитектуре A3 сократил число полных остановов почти вдвое, до 4,76 в год, главным образом за счет резерва контроллера участка, программные сбои которого в архитектурах A1 и A2 каждый раз останавливали весь участок, а также за счет маскирования обрывов кабеля на уровне приводов робота и ТНС.

Показательно, что средняя длительность останова в архитектуре A3 выросла до 3,31 ч: короткие остановы устранены, и в их структуре стали преобладать длительные отказы сервоприводов робота и ТНС. Архитектура A4 не изменила числа остановов, но сократила их среднюю длительность до 2,35 ч, поскольку отказ узла станции оборачивается не ожиданием ремонта в течение 12 ч, а трехминутным возобновлением работы на узле-партнере.

Отдельного внимания заслуживает чувствительность результатов к покрытию, которое на практике определяется полнотой встроенного диагностирования и качеством реализации переключения. Зависимость потерь от покрытия, рассчитанная по формулам (3)–(5), отражена на рисунке 2.

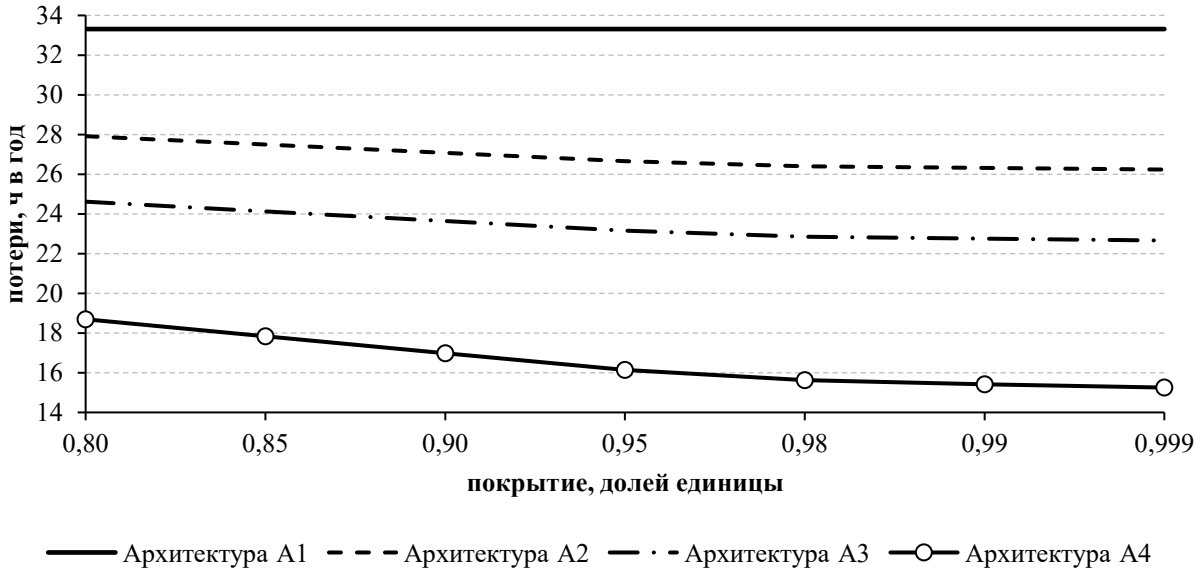


Рисунок 2. *Потери эквивалентного времени работы гибкого производственного участка в зависимости от покрытия при различных архитектурах распределенной системы управления приводами, ч в год (рассчитано авторами по результатам имитационного моделирования)*

Потери в базовой архитектуре от покрытия не зависят, поскольку резервирование в ней отсутствует. Для архитектур с резервированием зависимость монотонна, но различна по крутизне. При снижении покрытия с 0,999 до 0,80 потери архитектуры А2 возрастают с 26,23 до 27,92 ч в год, архитектуры А3 — с 22,66 до 24,62 ч, а архитектуры А4 — с 15,25 до 18,69 ч, то есть на 22,6 %. Именно авторская архитектура наиболее требовательна к качеству диагностирования, так как перенос функций выполняется только после обнаружения отказа узла. Вместе с тем даже при покрытии 0,80 архитектура А4 обеспечивает меньшие потери, чем архитектура А3 при практически идеальном покрытии 0,999. Следовательно, эффект функциональной реконфигурации устойчив к несовершенству диагностирования и не является следствием оптимистичных допущений.

Выясним, какие группы элементов определяют потери в каждой архитектуре. Потенциал сокращения потерь, рассчитанный по формуле (9), приведен в таблице 3.

Таблица 3

Потенциал сокращения потерь эквивалентного времени работы гибкого производственного участка по группам элементов распределенной системы управления приводами, ч в год

Группа элементов	А1	А2	А3	А4
Сервоприводы	14,75	14,76	14,77	14,78
Кабельные сегменты сети уровня приводов	7,40	1,46	0,42	0,42
Узлы управления станций, аппаратные отказы	5,32	5,32	5,33	0,29
Узлы управления станций, программные сбои	2,17	2,17	2,17	0,31
Контроллер участка	2,49	2,49	0,01	0,01
Магистральная сеть участка	0,80	0,04	0,04	0,04
Потери, всего	**32,97**	**26,27**	**22,76**	**15,85**

Сумма потенциалов может незначительно отличаться от общих потерь вследствие совпадения во времени отказов элементов разных групп. Рассчитано авторами по результатам имитационного моделирования на интервале 20 тыс. лет.

Из таблицы 3 следует, что структура потерь при переходе от базовой архитектуры к авторской меняется коренным образом. В архитектуре А1 сервоприводы обусловливают 14,75 ч потерь в год, или 44,7 %, кабельные сегменты сети уровня приводов — 7,40 ч,

аппаратные отказы и программные сбои узлов станций — 7,49 ч, контроллер участка — 2,49 ч. Каждый механизм отказоустойчивости устраняет «свою» составляющую. Кольцевые сети уровня приводов с переключением в пределах цикла сокращают потери от кабельных сегментов в 17,5 раза, горячий резерв контроллера участка практически исключает связанные с ним потери (с 2,49 до 0,01 ч), а функциональная реконфигурация снижает потери от отказов узлов станций с 7,49 до 0,59 ч. Потери от отказов сервоприводов при этом остаются неизменными, и в архитектуре А4 на них приходится 14,78 ч из 15,85 ч, или 93,3 %.

Полученный результат имеет принципиальное значение: средства системы управления не способны маскировать отказ исполнительного устройства, и дальнейшее повышение отказоустойчивости участка требует мер на уровне самих приводов — прогнозного диагностирования их состояния, сокращения времени замены модулей и применения отказоустойчивых многофазных двигателей, способных продолжать работу при обрыве цепи управления силовым ключом [24].

Вклад механизмов подтверждается и обратной процедурой — поочередным исключением каждого из них из архитектуры А4 при сохранении остальных. Исключение функциональной реконфигурации увеличивает потери на 43,6 %, отказ от кольцевой сети уровня приводов — на 44,1 %, исключение резерва контроллера участка — на 15,6 %, кольцевой магистрали — на 4,8 %. Замена переключения в пределах цикла на восстановление за 200 мс увеличивает потери на 6,5 %. Таким образом, наибольший эффект дают механизмы, обращенные к наиболее часто отказывающим элементам — программному обеспечению узлов и кабельным соединениям уровня приводов, тогда как резервирование магистрали участка, к которому на практике обращаются в первую очередь, вносит наименьший вклад.

Остановимся на условии (6), от которого зависит эффективность резервирования сети уровня приводов. Потери эквивалентного времени работы участка, обусловленные отказами кабельных сегментов, при различных механизмах резервирования и периодах цикла обмена представлены в таблице 4.

Таблица 4

Потери эквивалентного времени работы гибкого производственного участка от отказов кабельных сегментов сети уровня приводов в зависимости от механизма резервирования и периода цикла обмена, ч в год

Механизм резервирования	Время восстановления связи	$T_ц$ = 0,5 мс	$T_ц$ = 1 мс	$T_ц$ = 2 мс	$T_ц$ = 4 мс
Без резервирования (линейная топология)	—	7,45	7,45	7,45	7,45
Кольцо, протокол резервирования среды класса 200 мс	200 мс	1,48	1,48	1,48	1,48
Кольцо, протокол резервирования среды класса 30 мс	30 мс	1,48	1,48	1,48	1,48
Кольцо, протокол резервирования среды класса 10 мс	10 мс	1,48	1,48	1,48	0,44
Кольцо с переключением в пределах цикла обмена	не более $T_ц$	0,44	0,44	0,44	0,44
Бесшовное резервирование с дублированием кадров	0	0,01	0,01	0,01	0,01

Время срабатывания сторожевого таймера принято равным трем периодам цикла обмена; покрытие для бесшовного резервирования принято равным 0,999, для остальных механизмов — 0,95. Рассчитано авторами

Данные таблицы 4 свидетельствуют о пороговом характере зависимости. Пока условие (6) не выполняется, потери не зависят ни от класса протокола, ни от периода цикла: протоколы классов 200 и 30 мс дают одинаковые 1,48 ч в год, поскольку при любом из них обрыв сегмента вызывает срабатывание таймера и повторный пуск станции. Выигрыш относительно линейной топологии (7,45 ч) достигается здесь только сокращением длительности останова, а число остановов станций даже возрастает с 7,01 до 8,32 в год за счет сегмента, замыкающего кольцо. Протокол класса 10 мс удовлетворяет условию (6) лишь при цикле 4 мс, когда таймер срабатывает через 12 мс; потери при этом снижаются до 0,44 ч, а число остановов — до 0,42 в год. Для циклов обмена 0,5–2 мс, применяемых при управлении осями обрабатывающих

центров, условие выполнимо только для механизмов, переключающихся в пределах цикла, или для бесшовного резервирования с дублированием кадров, при котором потери снижаются до 0,01 ч в год.

Практический вывод состоит в том, что протоколы резервирования среды, хорошо зарекомендовавшие себя на уровне магистрали участка, где допустимое время прерывания обмена составляет сотни миллисекунд, переносить на уровень приводов нецелесообразно: формально резервированная сеть остается для приводов нерезервированной.

Оценим теперь допустимость переноса функций, на которой основан эффект архитектуры А4. Результаты проверки условий (7) и (8) представлены в таблице 5.

Таблица 5

Проверка допустимости переноса функций отказавшего узла управления станции на узел-партнер по условиям планируемости задач

Узел-исполнитель	Принимаемые функции	Загрузка до переноса	Загрузка после переноса	Граница по формуле (7)	Отношение R_i/D_i по формуле (8), наибольшее	Вывод
ОЦ	ОЦ той же пары	0,42	0,88	0,72	0,50	допустим
Робот-загрузчик	ТНС	0,56	0,79	0,72	0,38	допустим
ТНС	робота-загрузчика	0,21	0,81	0,72	0,42	допустим
ОЦ	робота-загрузчика	0,42	1,02	0,72	срок превышен	недопустим
ТНС	ОЦ	0,21	0,67	0,72	0,30	допустим, не используется

Загрузка процессора выражена в долях единицы; объединенный набор включает девять задач. Рассчитано авторами

Из таблицы 5 следует, что достаточное условие (7) отвергает перенос во всех трех используемых парах, поскольку загрузка после переноса (0,79–0,88) превышает границу 0,72. Точный анализ времени отклика (8) показывает, что все задачи объединенных наборов укладываются в допустимые сроки с запасом: наибольшее отношение времени отклика к сроку не превышает 0,50. Расхождение объясняется кратностью периодов задач (1, 2, 10, 20 и 100 мс), при которой граница К. Лю и Дж. Лейленда заведомо пессимистична.

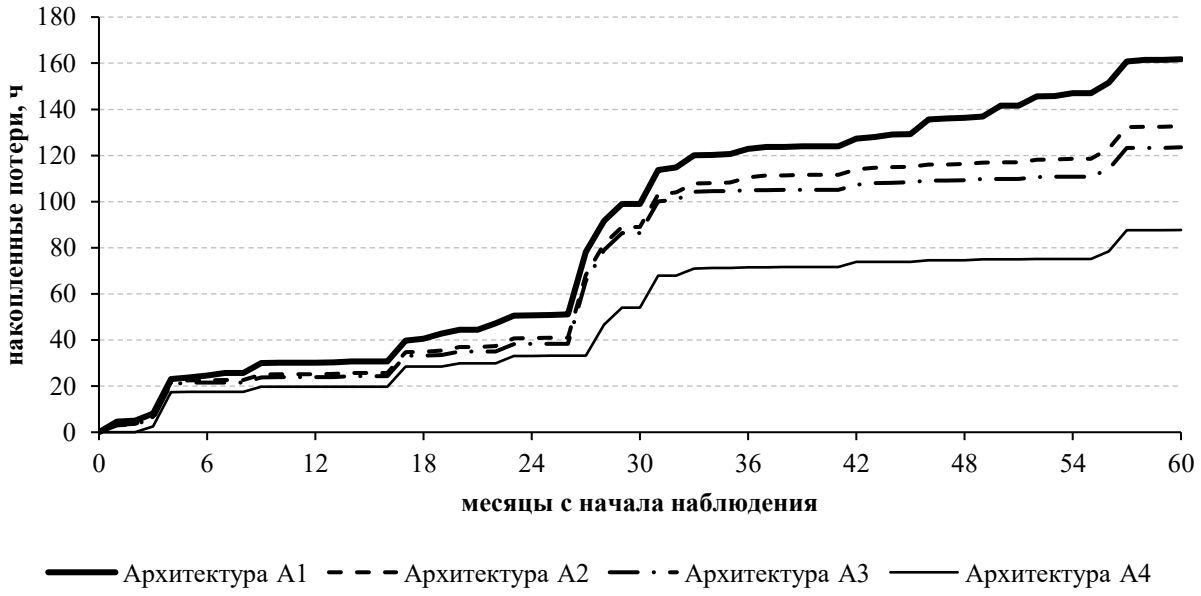


Рисунок 3. *Накопленные потери эквивалентного времени работы гибкого производственного участка при различных архитектурах распределенной системы управления приводами на одной реализации отказов, ч (рассчитано авторами по результатам имитационного моделирования)*

Перенос функций робота-загрузчика на узел обрабатывающего центра недопустим при любом методе проверки, так как суммарная загрузка превышает единицу. Именно этим обусловлен выбор пар взаимного резервирования: однотипные обрабатывающие центры резервируют друг друга, а наиболее загруженный узел робота — наименее загруженный узел ТНС. Для практики отсюда следует, что функциональная реконфигурация требует закладывать резерв вычислительной мощности узлов на этапе проектирования: при загрузке узла обрабатывающего центра выше 0,48 взаимное резервирование однотипных станций становится невозможным.

Различие архитектур наглядно проявляется на отдельной реализации функционирования участка. Накопленные потери эквивалентного времени работы на интервале пяти лет при одной и той же последовательности отказов элементов представлены на рисунке 3.

Траектории имеют ступенчатый характер: каждая ступень соответствует отказу, остановившему участок или его часть. Наиболее крупные ступени, общие для всех архитектур, образованы отказами сервоприводов, которые никакая архитектура не маскирует. Вместе с тем на 27-м месяце потери архитектур A1–A3 возрастают скачком на 27,1 ч вследствие аппаратного отказа узла управления станции, после которого станция простаивает до завершения ремонта, тогда как в архитектуре A4 этот отказ практически не отражается на траектории. За пять лет накопленные потери составили в архитектуре A1 — 161,7 ч, в архитектуре A4 — 87,7 ч, что согласуется со средними значениями, приведенными в таблице 2.

Полученные оценки имеют ограничения. Значения показателей безотказности и ремонтопригодности элементов приняты расчетными и при переходе к конкретному участку должны быть заменены статистикой эксплуатации; при этом сопоставительные выводы, как показал анализ чувствительности к покрытию, сохраняются в широком диапазоне параметров. Модель предполагает экспоненциальные распределения наработки и восстановления и независимость отказов, не учитывая отказы по общей причине, которые для дублированных структур могут быть значимыми.Перенос функций управления движением на узел другой станции предполагает, что приводы всех станций доступны через детерминированную сеть с общим циклом обмена; без такой сети реконфигурация ограничивается функциями логики и координации. Вместе с тем качественные выводы согласуются с заключением Ю. Чжана и Дж. Цзяна о преимуществах активных схем отказоустойчивости, опирающихся на диагностирование и перестройку системы [6], и с позицией В. Вяткина о целесообразности переносимых функциональных блоков [14]. Наш результат дополняет эти положения количественной мерой, связывающей механизмы отказоустойчивости с сохраняемой производительностью участка.

Заключение

Подводя итог, приведем собственные выводы, которые, по нашему мнению, можно рассматривать как приращение научного знания в области обеспечения отказоустойчивости распределенных систем управления приводами.

1. *Обоснован подход к оценке отказоустойчивости распределенной системы управления приводами по сохраняемой производительности гибкого производственного участка.* В отличие от коэффициента готовности системы управления, производительность с учетом деградации (3) учитывает неравноценность отказов: останов обрабатывающего центра снижает выпуск на четверть, а останов робота-загрузчика или контроллера участка прекращает его полностью.

2. *Предложено определение отказоустойчивости распределенной системы управления приводами с позиций производственной результативности.*

Отказоустойчивость распределенной системы управления приводами гибкого производственного участка представляет собой свойство системы сохранять производительность участка при отказах ее элементов полностью либо с допустимым снижением, обеспечиваемое совокупностью аппаратных, сетевых и программных механизмов, эффективность которых определяется не только наличием резерва, но и полнотой диагностирования, временем переключения и резервом вычислительной мощности узлов.

3. *Установлено пороговое условие эффективности резервирования сети уровня приводов* (6): резервирование маскирует отказ кабельного сегмента лишь при времени восстановления связи, не превышающем времени срабатывания сторожевого таймера приводов. Протоколы с временем восстановления 30–200 мс сокращают лишь длительность остановов, увеличивая их число, и при типичных циклах обмена не заменяют механизмов, переключающихся в пределах цикла.

4. *Показано, что наибольший вклад в отказоустойчивость участка вносит функциональная реконфигурация.* Авторская архитектура сокращает потери эквивалентного времени работы участка с 32,84 до 15,89 ч в год, то есть на 51,6 %, причем исключение переноса функций увеличивает потери на 43,6 %. Перенос допустим лишь при выполнении условия планируемости (8), которое для пар однотипных станций требует загрузки узлов не выше 0,48.

5. *Выявлен предел отказоустойчивости, достижимый средствами системы управления:* после введения всех механизмов 93,3 % остаточных потерь приходится на отказы самих сервоприводов.

В практическом плане результаты обосновывают три рекомендации. При проектировании распределенной системы управления приводами следует начинать с соотнесения времени восстановления сетевого резервирования со временем срабатывания сторожевых таймеров приводов и выбирать механизмы, удовлетворяющие условию (6). Резервирование целесообразно направлять прежде всего на элементы с наибольшей частотой отказов — программное обеспечение узлов и кабельные соединения уровня приводов, а не на магистраль участка. Резерв вычислительной мощности узлов для переноса функций необходимо закладывать на этапе проектирования, проверяя его точным анализом времени отклика, а не только достаточным условием (7). Перспективными направлениями исследования могут стать учет отказов по общей причине, моделирование переноса функций при неэкспоненциальных распределениях времени восстановления и совместная оптимизация резервирования системы управления и прогнозного диагностирования сервоприводов.

ЛИТЕРАТУРА

1. von Neumann, J. Probabilistic logics and the synthesis of reliable organisms from unreliable components / J. von Neumann // Automata Studies / ed. by C.E. Shannon, J. McCarthy. — Princeton: Princeton University Press, 1956. — С. 43–98.
2. Moore, E.F. Reliable circuits using less reliable relays / E.F. Moore, C.E. Shannon — DOI: 10.1016/0016-0032(56)90559-2. // Journal of the Franklin Institute. — 1956. — Т. 262, № 3. — С. 191–208.
3. Avizienis, A. Design of fault-tolerant computers / A. Avizienis — DOI: 10.1145/1465611.1465708 // Proceedings of the AFIPS Fall Joint Computer Conference. — New York: ACM, 1967. — С. 733–743.
4. Avižienis, A. Basic concepts and taxonomy of dependable and secure computing / A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr — DOI: 10.1109/TDSC.2004.2. // IEEE Transactions on Dependable and Secure Computing. — 2004. — Т. 1, № 1. — С. 11–33.

5. Blanke, M. Diagnosis and Fault-Tolerant Control / M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki. — 3rd ed. — Berlin, Heidelberg: Springer, 2016. — 695 с. — DOI: 10.1007/978-3-662-47943-8.
6. Zhang, Y. Bibliographical review on reconfigurable fault-tolerant control systems / Y. Zhang, J. Jiang — DOI: 10.1016/j.arcontrol.2008.03.008. // Annual Reviews in Control. — 2008. — Т. 32, № 2. — С. 229–252.
7. Isermann, R. Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance / R. Isermann. — Berlin, Heidelberg: Springer, 2006. — DOI: 10.1007/3-540-30368-5.
8. Мироновский, Л. А. Функциональное диагностирование динамических систем / Л. А. Мироновский. — Санкт-Петербург: Изд-во МГУ, ГРИФ, 1998. — 188 с. — ISBN 5-88141-040-8. — EDN: NGLDSD.
9. Жирабок, А. Н. Метод обеспечения отказоустойчивости систем управления с полной или частичной развязкой от дефектов / А. Н. Жирабок, В. Ф. Филаретов, А. В. Зуев, А. Е. Шумский — DOI: 10.31857/S0005231024070026. // Автоматика и телемеханика. — 2024. — № 7. — С. 15–31.— EDN: XSBNVL.
10. Hespanha, J.P. A survey of recent results in networked control systems / J.P. Hespanha, P. Naghshtabrizi, Y. Xu — DOI: 10.1109/JPROC.2006.887288. // Proceedings of the IEEE. — 2007. — Т. 95, № 1. — С. 138–162.
11. Felser, M. Real-time Ethernet — industry prospective / M. Felser — DOI: 10.1109/JPROC.2005.849720. // Proceedings of the IEEE. — 2005. — Т. 93, № 6. — С. 1118–1129.
12. Kirrmann, H. IEC 62439 PRP: bumpless recovery for highly available, hard real-time industrial networks / H. Kirrmann, M. Hansson, P. Müri — DOI: 10.1109/EFTA.2007.4416946. // 2007 IEEE Conference on Emerging Technologies and Factory Automation (ETFA 2007). — 2007. — С. 1396–1399.
13. Koren, Y. Reconfigurable manufacturing systems / Y. Koren, U. Heisel, F. Jovane, T. Moriwaki, G. Pritschow, G. Ulsoy, H. Van Brussel — DOI: 10.1016/S0007-8506(07)63232-6. // CIRP Annals. — 1999. — Т. 48, № 2. — С. 527–540.
14. Vyatkin, V. Software engineering in industrial automation: state-of-the-art review / V. Vyatkin — DOI: 10.1109/TII.2013.2258165. // IEEE Transactions on Industrial Informatics. — 2013. — Т. 9, № 3. — С. 1234–1249.
15. Martinov, G.M. Method of decomposition and synthesis of the custom CNC systems / G.M. Martinov, N.V. Kozak, R.A. Nezhmetdinov, A.S. Grigoriev, A.I. Obukhov, L.I. Martinova — DOI: 10.1134/S0005117917030122 // Automation and Remote Control. — 2017. — Т. 78, № 3. — С. 525–536.
16. Гнеденко, Б. В. Математические методы в теории надежности: основные характеристики надежности и их статистический анализ / Б. В. Гнеденко, Ю. К. Беляев, А. Д. Соловьев. — Изд. 2-е, испр. и доп. — Москва: ЛИБРОКОМ, 2012. — 582 с. — (Физико-математическое наследие: математика (теория вероятностей)). — ISBN 978-5-397-03638-2. — EDN: QMHTEV.
17. Meyer, J.F. On evaluating the performability of degradable computing systems / J.F. Meyer — DOI: 10.1109/TC.1980.1675654 // IEEE Transactions on Computers. — 1980. — Т. C-29, № 8. — С. 720–731.

18. Arnold, T.F. The concept of coverage and its effect on the reliability model of a repairable system / T.F. Arnold — DOI: 10.1109/T-C.1973.223703 // IEEE Transactions on Computers. — 1973. — Т. C-22, № 3. — С. 251–254.
19. Trivedi, K.S. Reliability and Availability Engineering: Modeling, Analysis, and Applications / K.S. Trivedi, A. Bobbio. — Cambridge: Cambridge University Press, 2017. — DOI: 10.1017/9781316163047.
20. Liu, C.L. Scheduling algorithms for multiprogramming in a hard-real-time environment / C.L. Liu, J.W. Layland — DOI: 10.1145/321738.321743. // Journal of the ACM. — 1973. — Т. 20, № 1. — С. 46–61.
21. Joseph, M. Finding response times in a real-time system / M. Joseph, P. Pandya — DOI: 10.1093/comjnl/29.5.390. // The Computer Journal. — 1986. — Т. 29, № 5. — С. 390–395.
22. Birnbaum, Z.W. On the importance of different components in a multicomponent system / Z.W. Birnbaum // Multivariate Analysis — II / ed. by P.R. Krishnaiah. — New York: Academic Press, 1969. — С. 581–592.
23. Dugan, J.B. Dynamic fault-tree models for fault-tolerant computer systems / J.B. Dugan, S.J. Bavuso, M.A. Boyd — DOI: 10.1109/24.159800 // IEEE Transactions on Reliability. — 1992. — Т. 41, № 3. — С. 363–377.
24. Лашкевич, М. М. Регулирование тока в многофазных двигателях с расщеплёнными обмотками при обрыве цепи управления силовым ключом / М. М. Лашкевич, К. Г. Федорова, А. Юсеф и др. — DOI: 10.24160/1993-6982-2024-4-11-20. // Вестник Московского энергетического института. — 2024. — № 4. — С. 11–20.— EDN: RFFJXY.

Nepogoda Filipp Vladimirovich
K.G. Razumovsky Moscow State University of Technologies and Management, Moscow, Russia

Goncharov Andrey Vitalyevich
K.G. Razumovsky Moscow State University of Technologies and Management, Moscow, Russia
E-mail: a.goncharov@mgutm.ru

Shakhovskoy Andrey Vladimirovich
K.G. Razumovsky Moscow State University of Technologies and Management, Moscow, Russia
E-mail: a.shakhovskoy@mgutm.ru

Rotanov Evgeny Gennadyevich
K.G. Razumovsky Moscow State University of Technologies and Management, Moscow, Russia
E-mail: e.rotanov@mgutm.ru

Ensuring fault tolerance of a distributed drive control system of a flexible manufacturing section

Abstract. Distributed drive control systems used in flexible manufacturing sections reduce cabling and simplify changeover, yet the growing number of nodes and network connections increases the number of elements whose failure stops a station or the whole section. The paper substantiates an approach in which the fault tolerance of the control system is assessed not by the share of time in the operable state but by the retained productivity of the section, and redundancy mechanisms are compared by their contribution to reducing lost working time. The modelled section comprises four machining centres, a loading robot and an automated storage and transport system with 32 servo drives, six station control nodes and a section controller. Four architectures are compared: a baseline with line networks; ring media redundancy; an additional hot-standby section controller with drive-level switchover within one communication cycle; and the proposed architecture, which also transfers the functions of a failed station node to a partner node. Calculations are performed with Markov models and discrete-event simulation over 20 thousand years of operation, verified against an analytical solution. The proposed architecture reduces the equivalent lost operating time of the section from 32,84 to 15,89 hours per year, i.e. by 51,6 %, and almost halves the number of complete stoppages. Ring redundancy of the drive-level network is shown to be effective only when the recovery time does not exceed the drive watchdog time; with 200 ms recovery it increases the number of station stoppages and only shortens them. Function transfer is feasible for pairs of identical stations and for the robot — storage system pair according to the schedulability condition, whereas hosting the robot functions on a machining-centre node is infeasible. With all mechanisms in place, 93 % of the residual losses are due to failures of the servo drives themselves, which sets the limit of fault tolerance attainable by control-system means. The results can be used when selecting the architecture and redundancy protocols of control systems for flexible manufacturing.

Keywords: fault tolerance; distributed control system; servo drive; flexible manufacturing section; redundancy; real-time industrial network; functional reconfiguration; performability; availability

Дата публикации: 30.10.2026