ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 681.5.09

АЛГОРИТМ БЕЗОПАСНОГО УПРАВЛЕНИЯ СИСТЕМОЙ ПОДАЧИ ИНЕРТНОГО ГАЗА ПО ДАВЛЕНИЮ И ВРЕМЕННЫМ ОГРАНИЧЕНИЯМ

Фролов Денис Александрович,
Национальный исследовательский университет «МИЭТ», Москва, Зеленоград
e-mail: den.frolov2004@mail.ru

Аннотация

Рассмотрен алгоритм управления системой подачи инертного газа в герметизируемую технологическую камеру. Управляющая логика построена как конечный автомат, учитывающий разрешающие блокировки, текущее давление, время достижения минимального уровня, продолжительность стабилизации и условия завершения процесса. Сформулированы правила включения исполнительных механизмов, контроля недостижения давления, ограничения максимального давления, обработки потери разрешающего сигнала и перехода в безопасное состояние. Для исключения частых переключений предложено применение гистерезиса по давлению. Описана реализация временных ограничений средствами таймеров программируемого логического контроллера и фиксация кода первичной причины отказа. Результаты сценарной проверки показывают, что разделение рабочих и аварийных переходов обеспечивает детерминированное отключение подачи газа при нарушении контролируемых условий и предотвращает бесконечное ожидание набора давления.

Ключевые слова: инертный газ, программируемый логический контроллер, промышленная безопасность, автомат состояний, давление, тайм-аут, блокировка, аварийное отключение.

SAFE CONTROL ALGORITHM FOR AN INERT GAS SUPPLY SYSTEM BASED ON PRESSURE AND TIME CONSTRAINTS

Denis A. Frolov,
National Research University of Electronic Technology (MIET), Moscow, Zelenograd, Russian Federation

ABSTRACT

The paper considers a control algorithm for supplying inert gas to a sealable technological chamber. The control logic is implemented as a finite-state machine that accounts for permissive interlocks, current pressure, the time required to reach a minimum pressure level, stabilization duration, and process completion conditions. Rules are formulated for enabling actuators, detecting failure to reach pressure, limiting maximum pressure, processing the loss of a permissive signal, and switching the system to a safe state. Pressure hysteresis is proposed to prevent frequent

actuator switching. The implementation of time constraints using programmable logic controller timers and the preservation of the primary fault code are described. Scenario-based verification shows that separating normal and emergency transitions provides deterministic shutdown of the gas supply when monitored conditions are violated and prevents indefinite waiting for the required pressure.

Keywords: inert gas, programmable logic controller, industrial safety, finite-state machine, pressure, timeout, interlock, emergency shutdown.

Введение

Инертная атмосфера применяется в технологических установках для снижения содержания кислорода, предотвращения окисления и обеспечения требуемых условий процесса. Управляющая система должна не только включать подачу газа, но и контролировать достижение давления, состояние исполнительных механизмов, разрешающие блокировки и длительность отдельных этапов. Простая логика «включить и ожидать датчик» опасна тем, что при утечке, закрытом клапане, неисправном насосе или недостоверном сигнале процесс может оставаться в неопределённом состоянии неограниченное время.

Общие принципы проектирования безопасных машин требуют выявлять опасности, оценивать риски и применять меры их снижения [1]. Для частей систем управления, выполняющих функции безопасности, ISO 13849-1 устанавливает требования и рекомендации по проектированию и интеграции, включая программное обеспечение [2]. IEC 61508 рассматривает функциональную безопасность электрических, электронных и программируемых электронных систем [3, 4]. Эти документы не задают конкретный алгоритм подачи газа, но обосновывают необходимость определённых безопасных состояний, диагностируемых отказов и контролируемых переходов. В научных работах по безопасному управлению производственными системами с ПЛК рассматриваются разделение функциональной и защитной логики, булевы ограничения безопасности и их формальная проверка [9–11].

При реализации логики на программируемом контроллере удобно использовать языки IEC 61131-3 и стандартные таймеры [5, 6]. Однако корректность зависит не от наличия таймера как такового, а от того, в каком состоянии он запускается, когда сбрасывается, и какая реакция формируется при истечении времени. Для промышленного применения требуется явная модель состояний, исключающая одновременное выполнение несовместимых действий и сохраняющая первичную причину аварии.

Цель исследования

Целью работы является формирование алгоритма безопасного управления системой подачи инертного газа по измеряемому давлению и временным ограничениям. Алгоритм должен разрешать запуск только при выполнении блокировок, прекращать процесс при недостижении давления за установленное время, ограничивать верхний уровень давления, исключать частые переключения и обеспечивать детерминированный переход в безопасное состояние.

Материалы и методы исследования

Рассматривается система, включающая источник инертного газа, запорный или регулирующий клапан, исполнительный механизм подачи, датчик давления и программируемый логический контроллер. Входными сигналами являются команда запуска Start, команда остановки Stop, признак закрытия камеры DoorClosed, готовность исполнительного механизма DriveReady, измеренное давление p и внешняя авария

ExternalAlarm. Выходами являются разрешение исполнительного механизма, команда клапану, признак активного процесса и код аварии.

Безопасным состоянием принимается отключение исполнительного механизма и закрытие управляемого клапана. Это программное определение должно быть согласовано с фактической схемой: для оборудования с иным физически безопасным положением клапана выходные значения корректируются на уровне проекта. После возникновения аварии код причины фиксируется до подтверждённого сброса, чтобы последующий отказ не скрывал первичное событие.

Разрешение запуска формируется как логическое произведение команды оператора и обязательных блокировок:

$$S_{start} = Start \wedge DoorClosed \wedge DriveReady \wedge \neg ExternalAlarm \wedge \neg LatchedAlarm.$$

Если выражение ложно, система остаётся в состоянии ожидания, а интерфейс отображает невыполненное условие. При разрешённом запуске конечный автомат последовательно проходит состояния проверки условий, подачи газа, стабилизации и рабочего режима. Завершение выполняется отдельным состоянием, в котором выходы переводятся в безопасное положение, таймеры сбрасываются и формируется признак готовности к следующему циклу.

Переходы автомата выполняются только в одном направлении за цикл контроллера. Изменение номера состояния и выходных команд разделяется таким образом, чтобы аварийная ветвь имела приоритет над штатным переходом. Во всех активных состояниях контролируются разрешающие сигналы и достоверность давления. Потеря обязательной блокировки немедленно переводит систему в аварию.

В момент включения подачи сохраняется начальное время t_0 и запускается таймер T_{press}. Если минимальное давление p_{min} не достигнуто до истечения допустимого времени, формируется авария недостижения давления:

$$((t - t_0) > T_{press}) \wedge (p < p_{min}) \Rightarrow E_{pressure\_timeout} = 1.$$

Таймер действует только в состоянии набора давления и обязательно сбрасывается при выходе из него. Такой подход исключает перенос накопленного времени в следующий цикл. После достижения p_{min} система переходит к стабилизации и запускает отдельный таймер T_{stab}. Рабочий режим разрешается только после непрерывного выполнения условия давления в течение заданного интервала; кратковременное падение ниже порога сбрасывает таймер стабилизации.

Верхний предел p_max контролируется независимо от текущего этапа подачи. При $p \geq p_{max}$клапан закрывается, исполнительный механизм отключается и фиксируется авария превышения давления. Для режима поддержания давления применяются два порога, разделённые зоной гистерезиса:

$$p_{on} = p_{set} - \Delta p, \quad p_{off} = p_{set} + \Delta p.$$

где p_{set} — целевое давление, Δp — половина зоны гистерезиса. Подача включается при $p \leq p_{on}$ и отключается при $p \geq p_{off}$. Внутри диапазона $[\, p_{on} ; p_{off} \,]$ сохраняется предыдущее состояние выхода. Это уменьшает количество переключений при шуме датчика и малых колебаниях давления. Значение Δp выбирается с учётом погрешности измерения, динамики камеры и допустимого диапазона процесса.

Аварийный обработчик имеет единый набор действий: закрытие клапана, отключение исполнительного механизма, сброс рабочих таймеров, снятие признака активного процесса и фиксация кода ошибки. Сброс аварии разрешается только при отсутствии внешнего аварийного сигнала, безопасном давлении и снятой команде запуска. Это предотвращает автоматический повторный запуск после кратковременного восстановления сигнала.

Штатная остановка также выполняется через состояние завершения, а не непосредственным переходом в ожидание. При необходимости в этом состоянии может

выдерживаться время закрытия клапана, проверяться обратная связь и сохраняться итоговый статус цикла. Требования к электрическому оборудованию машин, цепям управления и остановки должны учитываться совместно с программной логикой [8]. Программная логика не заменяет аппаратные устройства защиты от превышения давления; предохранительная арматура и независимые цепи аварийного отключения определяются проектом оборудования.

Проверка выполнялась на дискретных последовательностях входных сигналов, моделирующих нормальный цикл и характерные нарушения. Подход к проверке временной логики основан на задании контролируемых входных последовательностей и сопоставлении фактического состояния таймера с ожидаемым, как в примере тестирования блока TON средствами CODESYS Test Manager [7]. Для каждого сценария оценивались конечное состояние, выходные команды, состояние таймеров и сохранённый код причины. Результаты приведены в таблице 1.

Таблица 1.
Результаты сценарной проверки алгоритма

Сценарий	Ожидаемая реакция	Результат проверки логики
Нормальный набор давления	Переход через стабилизацию в рабочий режим	Переход выполняется после достижения p_{min} и истечения T_{stab}
Давление не достигнуто	Авария по истечении T_{press}	Подача отключается, фиксируется $E_{pressure\_timeout}$
Превышение p_{max}	Немедленное аварийное отключение	Аварийная ветвь имеет приоритет над штатными переходами
Открытие камеры во время подачи	Отключение и фиксация блокировки	Потеря DoorClosed переводит автомат в аварию
Колебание около p_{set}	Переключение только на границах гистерезиса	Внутри диапазона сохраняется предыдущее состояние
Повторный Start при активной аварии	Запуск запрещён	LatchedAlarm блокирует переход из ожидания
Сброс и новый цикл	Таймеры начинают отсчёт с нуля	Рабочие таймеры сбрасываются в завершении и аварии

Сценарный анализ показывает, что использование единого таймера для нескольких этапов создаёт риск переноса времени и ложного срабатывания, поэтому набор давления и стабилизация должны контролироваться отдельными экземплярами.

Гистерезис снижает частоту переключений, но не является фильтром недостоверного датчика. Для обнаружения обрыва, выхода за физически возможный диапазон или отсутствия изменения давления при включённой подаче необходимы отдельные диагностические условия. Пороговые значения и времена не должны быть жёстко зашиты в программный код; их следует хранить как конфигурационные параметры с проверкой допустимых диапазонов и контролем прав доступа.

Заключение

Алгоритм управления подачей инертного газа целесообразно реализовывать как конечный автомат с отдельными состояниями ожидания, проверки условий, набора давления, стабилизации, рабочего режима, завершения и аварии. Запуск разрешается только при выполнении блокировок, а любой активный этап контролируется по давлению и времени.

Ограничение времени набора давления предотвращает бесконечное ожидание при утечке или неисправности исполнительного механизма. Независимый контроль p_{max}, гистерезис поддержания давления, фиксация первичной причины и запрет автоматического повторного запуска после аварии обеспечивают детерминированную реакцию программной логики. Сценарная проверка подтверждает корректность переходов для нормального цикла, недостижения давления, превышения верхнего порога и потери разрешающих сигналов. Конкретные значения порогов, тайм-аутов и аппаратные меры защиты должны определяться проектом и оценкой риска установки.

Список литературы:

1. ISO 12100:2010. Safety of machinery — General principles for design — Risk assessment and risk reduction. Geneva: ISO, 2010.
2. ISO 13849-1:2023. Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design. Geneva: ISO, 2023.
3. IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements. Geneva: IEC, 2010.
4. IEC 61508-3:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements. Geneva: IEC, 2010.
5. IEC 61131-3:2025. Programmable controllers — Part 3: Programming languages. Geneva: IEC, 2025.
6. CODESYS Group. Timer: TON, TOF and TP Function Blocks. Standard Library Documentation. URL: https://content.helpme-codesys.com/en/libs/Standard/3.5.18.0/Timer/fld-Timer.html (дата обращения: 25.07.2026).
7. CODESYS Group. Testing the TON Function Block. CODESYS Test Manager Documentation. URL: https://content.helpme-codesys.com/en/CODESYS%20Test%20Manager/_tm_iec_unit_test_example_ton.html (дата обращения: 25.07.2026).
8. IEC 60204-1:2016+AMD1:2021. Safety of machinery — Electrical equipment of machines — Part 1: General requirements. Geneva: IEC, 2021.
9. Riera B., Coupat R., Philippot A., Annebicque D., Gellot F. Control design pattern based on safety logical constraints for manufacturing systems: application to a palletizer // IFAC Proceedings Volumes. 2014. Vol. 47, no. 2. P. 388–393. DOI: 10.3182/20140514-3-FR-4046.00054.
10. Pichard R., Philippot A., Riera B. Consistency Checking of Safety Constraints for Manufacturing Systems with Graph Analysis // IFAC-PapersOnLine. 2017. Vol. 50, no. 1. P. 1193–1198. DOI: 10.1016/j.ifacol.2017.08.273.
11. Pichard R., Philippot A., Riera B. Safe PLC Controller Implementation IEC 61131-3 Compliant based on a Simple SAT Solver: Application to Manufacturing Systems //

Proceedings of the 15th International Conference on Informatics in Control, Automation and Robotics. 2018. Vol. 1. P. 231–239. DOI: 10.5220/0006885502310239.

References:

1. ISO 12100:2010. Safety of machinery — General principles for design — Risk assessment and risk reduction. Geneva: ISO, 2010.
2. ISO 13849-1:2023. Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design. Geneva: ISO, 2023.
3. IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements. Geneva: IEC, 2010.
4. IEC 61508-3:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements. Geneva: IEC, 2010.
5. IEC 61131-3:2025. Programmable controllers — Part 3: Programming languages. Geneva: IEC, 2025.
6. CODESYS Group. Timer: TON, TOF and TP Function Blocks. Standard Library Documentation. Available at: https://content.helpme-codesys.com/en/libs/Standard/3.5.18.0/Timer/fld-Timer.html (accessed 25 July 2026).
7. CODESYS Group. Testing the TON Function Block. CODESYS Test Manager Documentation. Available at: https://content.helpme-codesys.com/en/CODESYS%20Test%20Manager/_tm_iec_unit_test_example_ton.html (accessed 25 July 2026).
8. IEC 60204-1:2016+AMD1:2021. Safety of machinery — Electrical equipment of machines — Part 1: General requirements. Geneva: IEC, 2021.
9. Riera B., Coupat R., Philippot A., Annebicque D., Gellot F. Control design pattern based on safety logical constraints for manufacturing systems: application to a palletizer. IFAC Proceedings Volumes. 2014;47(2):388–393. DOI: 10.3182/20140514-3-FR-4046.00054.
10. Pichard R., Philippot A., Riera B. Consistency Checking of Safety Constraints for Manufacturing Systems with Graph Analysis. IFAC-PapersOnLine. 2017;50(1):1193–1198. DOI: 10.1016/j.ifacol.2017.08.273.
11. Pichard R., Philippot A., Riera B. Safe PLC Controller Implementation IEC 61131-3 Compliant based on a Simple SAT Solver: Application to Manufacturing Systems. In: Proceedings of the 15th International Conference on Informatics in Control, Automation and Robotics. 2018;1:231–239. DOI: 10.5220/0006885502310239.