УДК 004.5:006.032

СУЧАСНІ СТАНДАРТИ З РОЗРОБЛЕННЯ ТРИВОЖНОЇ СИГНАЛІЗАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ КЕРУВАННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Пупена О.М.[1], Шишак А.В.[2]

[1,2] – Національний університет харчових технологій, Київ, Україна
ORCID: [1]http://orcid.org/0000-0001-9089-8325, [2]http://orcid.org/0000-0001-9860-7430
E-mail: [1] pupena_san@ukr.net, [2]al_sh_94@ukr.net

DOI:

Анотація. *Автоматизована система керування технологічним процесом передбачає наявність функцій тривожної сигналізації, які виконують надзвичайно важливу роль. Від ефективності роботи підсистеми тривожної сигналізації залежить передусім безпека людей, виробництва та функціонування автоматизованої системи керування технологічним процесом в цілому. В Україні розробленню, впровадженню та експлуатації систем тривожної сигналізації приділяється недостатньо уваги. Тому це невеличке дослідження присвячено передусім трактуванню сучасного стандарту ISA-18.2 «Management of Alarm Systems for the Process Industries», який є визнаною хорошою інженерною практикою. Стаття розділена на дві публікації. У цій частині розкриваються основні сутності, на яких базуються механізми організації систем тривожної сигналізації. Наступна стаття буде присвячена роз'ясненню робочих процесів життєвого циклу системи, які стандарт передбачає для розроблення, впровадження та експлуатації систем тривожної сигналізації.*

Abstract. *The automated process control system involves alarm functions, which have an extremely important role. The effectiveness of the alarm system depends primarily on the safety of people, the production and operation of the automated process control system in general. In Ukraine, insufficient attention is given to the design, implementation and operation of alarm systems. Therefore, this small study is devoted primarily to the interpretation of the modern ISA-18.2 standard "Management of Alarm Systems for the Process Industries", which is recognized as a good engineering practice. The article is divided into two publications. The first part reveals the main concepts on which management of alarm systems is based. The second part is devoted to the explanation of the work processes of the system life cycle, which the standard provides for the development, implementation and operation of alarm systems.*

Ключові слова: Система тривожної сигналізації, тривога, SCADA, HMI, ISA-18.2.
Keywords: Alarm system, Alarm, SCADA, HMI, ISA-18.2.

Вступ. Функції **тривожної сигналізації** (з англ. **alarm**) є одними з найважливіших в системах SCADA/HMI, тому входять в комплектність усіх засобів цього типу, і нерідко є окремою підсистемою. Добре пророблені функції запобігають аварійним ситуаціям, і можуть не тільки запобігти збиткам, але і зберегти життя людей і навколишнє середовище. З іншого боку, якщо підсистема або окремі функції погано реалізовані це може звести нанівець всю її роботу. Останнє, нажаль, часто спостерігається на вітчизняних підприємствах, де нерідко функції тривожної сигналізації просто ігноруються. Наступний приклад може здатися багатьом дуже знайомим.

Класичним способом контролю роботи двигунів є використання в якості зворотного зв'язку додаткових контактів, які замикаються при спрацюванні пускачів. Таким чином система тривожної сигналізації відслідковує сигнал керування та зворотній зв'язок по функції логічного AND з урахуванням затримки часу. Припустимо, при впроваджені системи АСУТП, замовник взяв на себе частину робіт щодо забезпечення керування та контролю спрацювання двигунів на насосах та інших механізмах. При цьому він взяв на себе також роботи по прокладанню кабельних проводок та підключенню. У результаті виявилося, що на момент пуско-налагоджуваних робіт замовник не виконав цю частину роботи, що привело до великої кількості тривог, які пов'язані з двигунами. Враховуючи, що ці тривоги

займають велику кількість повідомлень в журналі, інші тривоги невидимі та ігноруються оператором. Зрештою, тривожна сигналізація взагалі не сприймається оператором, оскільки та постійно видає тривожні повідомлення.

У наведеному прикладі, здавалось би, винуватий замовник, але це не зовсім так. Система керування повинна передбачати механізми відключення (блокування) таких тривог. Це тільки один з прикладів недостатньо продуманої підсистеми тривожної сигналізації, однак таких прикладів дуже багато. У дослідженнях організації «Управління по охороні праці Великобританії» (HSE) наведено багато прикладів [1, 2], коли недостатньо продумана система тривожної сигналізації приводила до фатальних наслідків, які супроводжувалися забрудненням навколишнього середовища, нанесенням шкоди здоров'ю та, навіть, смертю великої кількості людей. На відміну від України, у всіх високорозвинених країнах, охорона праці розглядається як економічний важіль у боротьбі з необґрунтованими збитками. Завдання таких організацій як «Управління по охороні праці Великобританії», «Адміністрація з безпеки та гігієни праці» (OSHA, «Міністерство праці США»), «Федеральний інститут з безпеки і гігієни праці» (BAuA, Німеччина) охоплюють сфери від наукових досліджень, розробки практичних рекомендацій, впровадження в виробництво методів покращення стану безпеки та гігієни праці до консультування підприємців та навчання спеціалістів і службовців в галузі безпеки та гігієни праці на виробництві. Такі практичні рекомендації та наукові дослідження достатньо серйозно зосереджуються на темі організації систем тривожної сигналізації. Дослідницькі роботи у сфері тривожної сигналізації в автоматизованих системах керування технологічними процесами в Україні нам не відомі. Тим не менше, наші співробітники, а також колеги «по цеху» мають достатній досвід розробки АСКТП особливо в харчовій промисловості і бачили достатньо багато реалізацій систем керування від різних інтеграторів, щоб ми зробили певні висновки, щодо типової ситуації в Україні.

1. Велика кількість розробників (систем АСКТП) приділяють системам тривожної сигналізації недостатньо уваги, а інколи зовсім ігнорують.
2. Більшість розробників не мають спеціально отриманих компетенцій саме в розробці підсистем тривожної сигналізації.
3. Пропоновані рішення по підсистемам тривожної сигналізації сильно залежать від постачальника забезпечення SCADA/HMI.
4. Більшість замовників не освічені в питаннях, навіть, важливості функцій тривожної сигналізації, не кажучи про можливості та необхідні вимоги, тому не можуть проконтролювати правильно пророблене ТЗ та якість виконання робіт.

Наведена вище ситуація сильно залежить від галузі та масштабу підприємств як замовника, так і інтегратора АСКТП. Звичайно, для функціонально-небезпечних об’єктів тільки ряд з наведених пунктів має місце. Тим не менше, для інших типів об’єктів недостатньо пророблена система тривожної сигналізації може привести не тільки до збитків, а і до фатальних випадків.

Такий стан, на нашу думку, зумовлений певним рядом чинників:

- нестача кваліфікованих кадрів або їх недостатня підготовка;
- нестача освітнього матеріалу доступного українською мовою як для замовника (підприємства), так і для виконавця (інтегратора);
- відсутність належних українських стандартів, які принаймні могли б служити кращими практиками для розробників та експлуатації;
- низький рівень вартості впровадження АСКТП, що нерідко приводить до відкидання підсистеми тривог для здешевлення;
- використання дешевого інструментарію, який в недостатній мірі підтримує необхідні функції підсистеми тривог.

У цивілізованому світі до проблеми розробки ефективної тривожної сигналізації ставляться дуже серйозно, що привело до появи ряду стандартів та практичних рекомендацій. Зокрема, нам відомі наступні практичні рекомендації та стандарти, присвячені саме системам тривожної сигналізації:

- Alarm Management NAMUR-Worksheet NA 102, 2008-10-02 Edition, від NAMUR – Асоціація користувачів технологій автоматизації технологічних процесів (від нім. Interessengemeinschaft Automatisierungstechnik der Prozessindustrie);
- IEC 62541-9, OPC Unified Architecture – Part 9: Alarms and conditions;
- IEC 62682, Management of Alarm Systems for the Process Industries;
- EEMUA 191, Alarm Systems – A Guide to Design, Management and Procurement, 3rd Edition, від EEMUA – Асоціація користувачів інженерного обладнання та матеріалів (від англ. the Engineering Equipment and Materials Users Association).

Слід відмітити, що існують також інші стандарти та практичні рекомендації, присвячені системам тривожної сигналізації, зокрема [3, 4, 5, 6]. Частина з них прийняті в Україні, але ці стандарти розглядають усі системи тривожної сигналізації, як такі, які не пов’язані зі SCADA/HMI, або не приділяють їм достатньої уваги. Це сильно ускладнює використання їх в життєвому циклі розроблення системи.

Щоб спеціалісти, які задіяні в процесі розроблення системи тривожної сигналізації змогли проектувати і розробляти ефективні АСУТП, в одному з комітетів ISA (International Society of Automation) було розроблено стандарт ISA-18.2 «Організація функціонування систем тривожної сигналізації в переробних галузях промисловості» (з англ. «Management of Alarm Systems for the Process Industries»). Як зазначено в стандарті, «у звітах про розслідування серйозних інцидентів неефективні системи тривожної сигналізації часто наводяться як визначальні фактори впливу» [7]. Цей стандарт надає методологію, застосування якої призведе до поліпшення безпеки, якості та функціонування переробних галузей промисловості. Стандарт ISA-18.2 включає практики викладені в інших стандартах і практичних рекомендаціях.

У ході розробки ISA-18.2 було докладено всіх зусиль, щоб зберегти термінологію і практики відповідно до попередньої роботи всіх організацій і комітетів, що передували йому. У 2014-му році був прийнятий стандарт IEC 62682, який є аналогом ISA-18.2. Це значить, що даний стандарт можна гармонізувати з українськими, хоча б методом підтвердження. В Україні цей стандарт є одним із пріоритетним для пророблення в технічному комітеті ТК 185 «Промислова автоматизація».

Мета дослідження. У даній статті ми намагаємося розкрити основний зміст стандарту, для того, щоб спеціалісти могли оцінити його важливість та ознайомитися з принципами організації систем тривожної сигналізації, які зарекомендували себе у світі як кращі практики. Результат аналізу стандарту ISA-18.2, викладений в даній публікації, може бути поштовхом до впровадження у виробництво загальноприйнятої хорошої інженерної практики ще до прийняття стандарту в Україні. У цій статті основна увага приділяється сутностям, термінології та функціям систем тривожної сигналізації, а у наступній – будуть розглядатися процеси життєвого циклу. Ми розглядатимемо системи тривожної сигналізації через призму стандарту ISA-18.2 саме в 2-й редакції (2016 рік), як найбільш актуального на сьогоднішній день. Тим не менше, враховуючи практики використання в інструментах SCADA/HMI можуть зустрітися певні альтернативні варіанти термінів.

Результати дослідження.

Місце підсистеми тривожної сигналізації в системі автоматизованого керування

Стандарт ISA-18.2 означує **систему тривожної сигналізації** (з англ. **alarm system)** як набір апаратного і програмного забезпечення, яке виявляє стан тривоги, повідомляє про це оператору і записує в журнал зміни стану. При цьому наголошується, що оператор є частиною цієї системи. Є також різні означення у вітчизняних стандартах, зокрема у ДСТУ 3960-2000, де система тривожної сигналізації – це електричне обладнання, призначене для виявлення та попередження про наявність небезпеки. Ми будемо використовувати означення саме ISA-18.2, як більш сучасне та застосовне для SCADA/HMI, та термін «система тривожної сигналізації», так як це звучить в українському стандарті.

Стандарт побудований на принципах розгляду системи тривожної сигналізації через призму життєвого циклу, що характерно для більшості сучасних стандартів ISA (і не тільки), зокрема спорідненого до нього ISA-101 «Human Machine Interfaces for Process Automation Systems», що розглядає системи людино-машинного інтерфейсу. Це типова практика системної інженерії, яка останні кілька десятків років сильно впливає на інженерію в цілому. Більшість функцій та сутності тривожної сигналізації в стандарті ISA-18.2 не розкриваються детально, а лише коротко описуються. Однак, слід відмітити, що, по-перше, найбільш фундаментальні сутності, а також структура в стандарті описані на достатньому рівні, щоб їх зрозуміти. По-друге, після виходу першої версії стандарту вийшло також ряд технічних звітів, які надають вказівки щодо впровадження підходів викладених в ISA-18.2 (деталізують сутності та функціонування). У цій статті ми зупинимося на найбільш фундаментальних сутностях, описаних в стандарті, «вирвавши» їх з контексту життєвого циклу. На нашу думку, читачеві буде зручніше спочатку ознайомитися з функціями систем тривожної сигналізації, а вже потім розглянути життєвий цикл.

Стандарт розглядає систему тривожної сигналізації в контексті взаємодії з іншими системами. До області її діяльності можуть входити БСКТП / BPCS (базова система керування технологічними процесами / the basic process control system), СПАЗ / SIS (система протиаварійного захисту / the safety instrumented system) та інші автономні системи (packaged systems), кожна з яких використовує свої датчики вимірювання для слідкування за умовами проходження процесу і логіку генерування тривог (див. рис. 1). Система тривожної сигналізації забезпечує передачу інформації про тривогу оператору через ЛМІ / HMI, який зазвичай являє собою екран комп'ютера, або на панель оповіщення (annunciator panel). До додаткових функцій системи тривожної сигналізації належать ведення журналу тривог (alarm log), сховища тривог (alarm historian) та розрахунок показників ефективності функціонування системи.

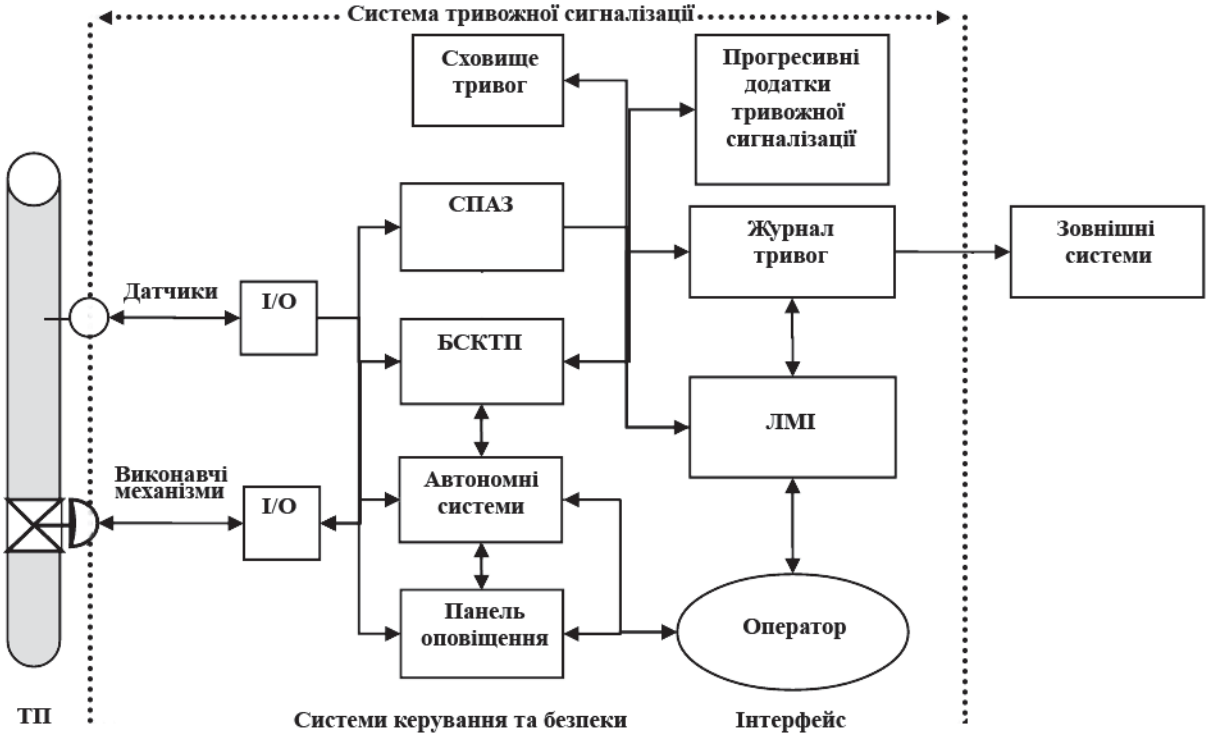

Рис. 1 – Функціональна структура тривожної сигналізації

На рис.1 в зоні дій системи тривожної сигналізації показані елементи, які стосуються не тільки її функцій. В стандарті зазначено, що ці засоби не входять в зону її діяльності, але можуть мати функції, які стосуються систем тривожної сигналізації. Зокрема:

- датчики (з англ. process sensors) та виконавчі механізми (з англ. final control elements) можуть також вміщувати функції тривог;
- СПАЗ система протиаварійного захисту (з англ. safety instrumented system), яка описана в стандартах IEC 61511 (аналог ANSI/ISA-84.00.01-2004), а також в IEC 61508, можуть передавати тривоги та діагностичні покази;
- панелі оповіщення (з англ. annunciator panel), які описані стандартом ISA-18.1-1979 (R2004), можуть інтегруватися в систему тривожної сигналізації;
- системи пожежної сигналізації і протипожежного захисту (з англ. fire detection and suppression systems), а також системи охоронної сигналізації (з англ. security systems) можуть передавати тривоги та діагностичні покази.

Усі процеси життєвого циклу систем тривожної сигналізації входять до **організації систем тривожної сигналізації** (Alarm management, або керування тривогами, надалі **ОСТС**). До цих процесів входить означення, документування, проектування, експлуатація, моніторинг та обслуговування систем тривожної сигналізації. Згідно стандарту **тривога (**з англ. **alarm)** – це звукові та/або візуальні засоби індикації для оператора про несправність устаткування, відхилення від процесу, ненормальні умови, які потребують своєчасного реагування. Слід відмітити, що у зарубіжних та вітчизняних стандартах є інші означення тривоги, зокрема в ДСТУ 3960-2000 та ДСТУ EN 50136-1-1-2014, які дещо відрізняються.

Таким чином, основна частина ОСТС полягає в означенні тривоги. Істотним елементом цього означення є забезпечення своєчасного реагування оператора на тривогу та допомога в усвідомленні наступних дій, які потрібно провести. Це означення підкріплене методами організації функціонування тривог описаних в цьому стандарті.

Модель взаємодії оператора з процесом

Розробники АСКТП нерідко забувають, що система тривожної сигналізації розроблена саме для оператора, який в даному контурі займає головне місце. Саме його реакція і дії визначають досягнення цілей функціонування тривог. Система тривожної сигналізації лише допомагає оператору виявити тривогу та надати йому інструменти для швидкого орієнтування в ситуації. Дії щодо виправлення нештатної ситуації він повинен сформувати і провести самостійно. Тому в стандарті велику увагу приділяють опису моделі контуру тривоги через взаємодію оператора з процесом (див. рис.2). У відповідь на порушення або несправність процес або система зазнають певних змін. Якщо ця зміна істотно відхиляється від заданого стану, оператор повинен вжити певних заходів, щоб повернути процес до норми. Це відбувається в три етапи.

- Виявлення (з англ. detect): оператор дізнається про відхилення від бажаного стану за допомогою сигналу тривоги, викликаного порушенням. Структура системи тривожної сигналізації та інтерфейс оператора повинні сприяти виявленню відхилень.
- Діагностування (з англ. diagnose): у відповідь на відхилення оператор використовує свої знання та навички для інтерпретації інформації, діагностування ситуації та визначення необхідних коригувальних дій. Діагностувати ситуацію оператору допомагають процедури реагування на тривогу.
- Реагування (з англ. respond): вживаються коригувальні дії для компенсації збурення. У відповідь на відхилення оператор приймає коригувальні дії і контролює процес, щоб визначити, чи було виправлене це відхилення.

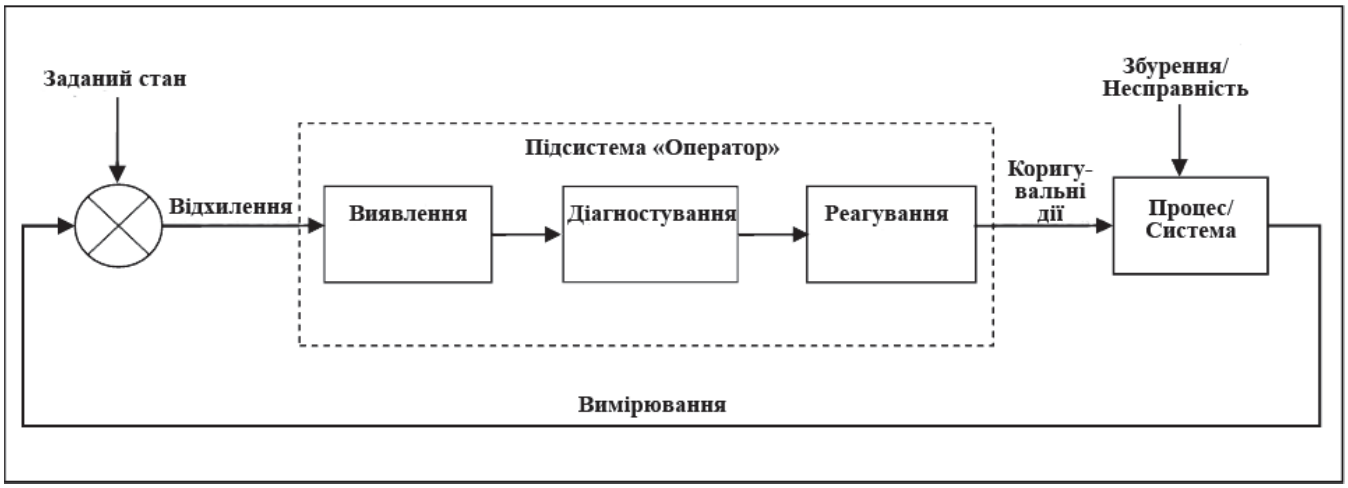

Рис. 2 – Модель контуру тривоги через взаємодію оператора з процесом

Кожен із цих етапів є дуже важливим і потребує окремої уваги на усіх етапах життєвого циклу. Однак людина в цьому контурі є найбільш непередбачуваною ланкою і це також треба врахувати. На здатність оператора виконувати функції підсистеми впливає багато факторів, у тому числі:

- навантаження;
- ергономіка операторської консолі;
- обмеження короткострокової або робочої пам'яті;
- втома;
- знання;
- мотивація.

При розробленні системи тривожної сигналізації це все необхідно враховувати, інакше ці фактори можуть привести до проблем. Зокрема, кількість активних тривог та частота зміни їх стану можуть стати причиною неефективності роботи системи тривожної сигналізації. У стандарті це зветься **переповненням тривог** (з англ. **alarm flood**) – ситуація, при якій частота виникнення тривог більша, ніж оператор може їх ефективно опрацювати (наприклад, більше, ніж 10 тривог за 10 хвилин). Для усунення цього негативного ефекту в стандарті ISA-18.2 означено багато механізмів та рекомендацій щодо побудови життєвого циклу ОСТС, деякі з них наведені нижче.

Автомат станів тривог

Принципово важливим для означення функцій тривог є формалізація їх автомату станів. У нашій практиці зустрічалися неодноразові випадки, коли не тільки обслуговуючий персонал, а і розробники не могли чітко пояснити роботу тривог, закладену постачальниками інструментів SCADA/HMI. Іншим типовим випадком є власно придумані автомати станів, або відсутність їх (автоматів) як таких. **Недостатньо формалізований автомат станів може привести до невірного його тлумачення учасниками життєвого циклу підсистеми тривожної сигналізації і може привести до непередбачуваних наслідків!** Навіть, якщо в проекті буде реалізовано власний автомат станів, відмінний від стандартного, його треба обов'язково описати в документації у відповідному розділі проекту. У стандарті означення автомату станів є одним із фундаментальних механізмів, на яких базуються всі інші сутності.

Тривога може знаходитися в кількох станах, зміни яких можуть бути викликані різними джерелами в системі керування, включаючи польовий пристрій (наприклад, датчики і виконавчі механізми), система керування (БСКТП чи СПАЗ) та ЛМІ (оператор). У стандарті ISA-18.2 наведена діаграма автомата станів тривоги, що показана на рис.3. Стани тривоги представлені на рисунку колами, в яких наводиться опис стану, що включає літерну мітку (ідентифікатор стану), назву стану, опис умови проходження процесу та комбінацію статусів:

- статус тривоги;
- статус підтвердження.

Таким чином, стан – це узагальнюючий показник, який залежить від плинного значення статусів та від попереднього стану.

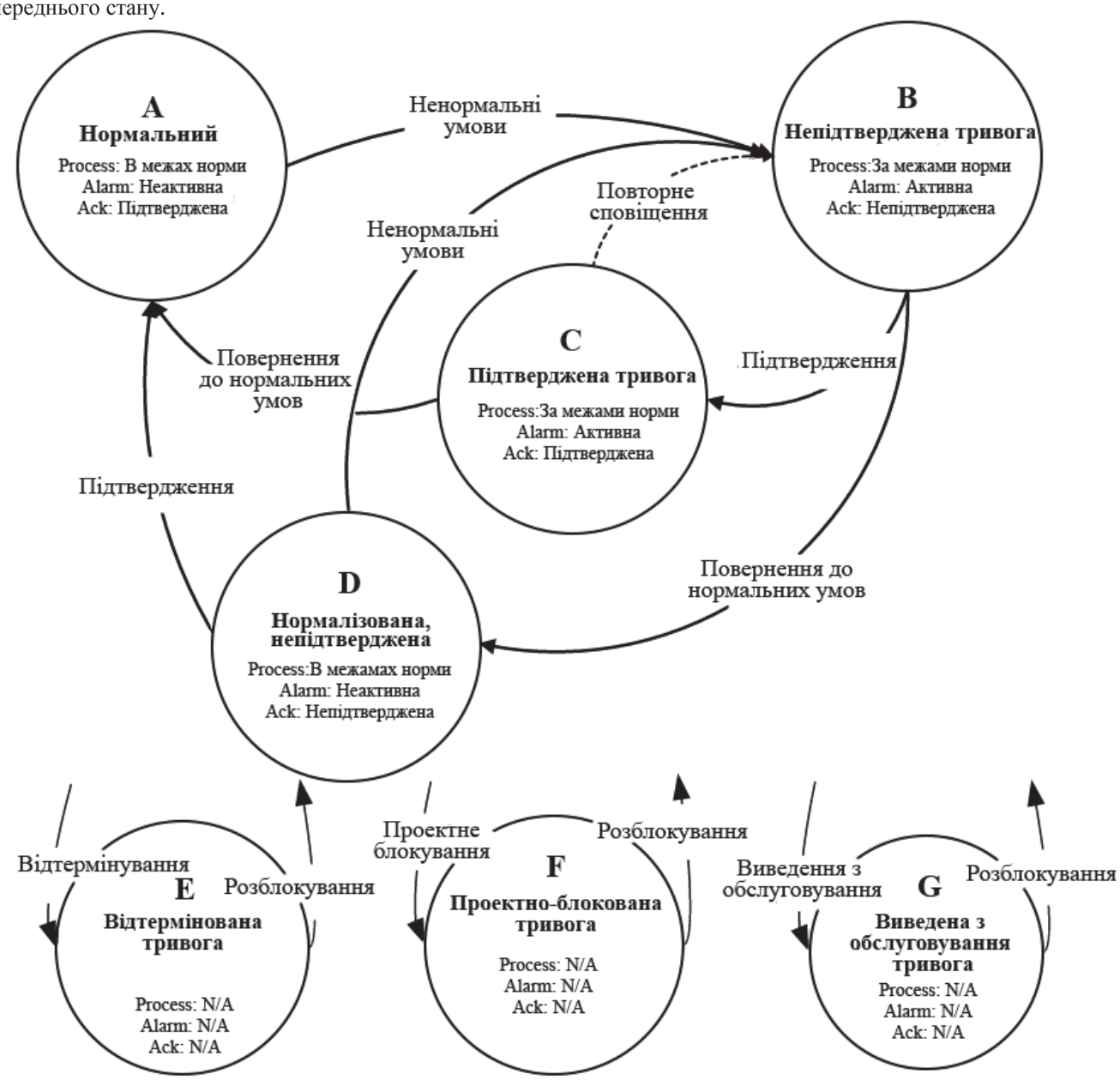

Рис. 3 – Автомат станів тривог згідно ISA-18.2

У нижній частині діаграми показані можливі стани блокованих тривог (з англ. alarm suppression). Стрілки на рис.3 відповідають переходам між станами. Діаграма не показує безпосередньо вплив зон нечутливостей чи затримок на спрацювання, які включені в оцінку статусу тривоги (тобто, активної або неактивної). Більшість з них є очевидними, тому при описі станів прокоментуємо тільки деякі з них. **Нормальний стан тривоги** (A – Normal, **NORM**) означується як стан, в якому процес працює в межах нормальних характеристик, сигнал тривоги не активний і попередні виникнення тривоги були підтверджені. Стан **непідтвердженої тривоги** (B – Unacknowledged state, **UNACK**) є початковим станом тривоги, що стає активною внаслідок ненормальних умов. У цьому стані тривога є не підтвердженою. Стан **підтвердженої тривоги** (C – Acknowledged state, **ACKED**) – це стан, в якому тривога є активною але оператор підтвердив сигнал тривоги. **Нормалізована непідтверджена тривога** (D – Return to normal unacknowledged state, **RTNUN**) – це стан, в якому процес знаходиться в межах норми, але тривога стала неактивною до того, як оператор її підтвердив.

Таким чином у стандарті наведений типовий автомат станів, який реалізований у всіх добре відомих брендових засобах SCADA/HMI. Деякі з інструментальних засобів передбачають два автомати станів: стандартний і такий, що не передбачає наявності статусу підтвердження. Тим не менше, останній не передбачений стандартом.

Окрім наведених вище «класичних» станів, стандарт передбачає можливість блокування тривог, який повинен убезпечити систему тривожної сигналізації від ефекту переповнення тривог (з англ. alarm flood), про який згадувалося вище. Це стани: відтермінована (з англ. Shelved), проектно-блокована (з англ. Suppressed-by-design) та виведена з обслуговування (з англ. Out-of-service). На цих станах варто зупинитися детальніше, так як далеко не всім розробникам АСКТП вони відомі.

Стан **відтермінованої тривоги** (E – Shelved state, **SHLVD**) – це стан, в якому тривога тимчасово блокується оператором, тобто для неї надалі не проводиться оповіщення. Перехід до відтермінованої (будь-який стан → E) відбувається тоді, коли оператор командою з ЛМІ відтерміновує сигнал тривоги, щоб уникнути її появи на дисплеях активних тривог. Відтермінування – ручна операція, а от розблокування (з англ. unshelve) може відбуватися як автоматично (після заданого часу) так і вручну оператором. Якщо тривога в цей час активна, перехід повинен здійснюватися в стан непідтвердженої тривоги, якщо не активна – в нормальний стан. Таким чином функція відтермінування передбачає, що оператор задає час, протягом якого тривога буде заблокована. Система тривожної сигналізації повинна забезпечувати виконання наступних функцій:

- можливість відтермінувати тривогу;
- відображення на дисплеях відтермінованих тривог або еквівалентних до них списків;
- задавання часу для відтермінування;
- контроль доступу до відтермінування індивідуальних тривог;
- можливість розблокування тривоги;
- формування в журналах записів про відтермінування.

Стан **проектно-блокованої тривоги** (F – Suppressed-by-design, **DSUPR**) – це стан, в якому тривога блокується з причини певних умов експлуатації або стану установки, і для неї не потрібно проводити оповіщення. Тривога в цьому стані знаходиться під контролем логіки, що визначає актуальність тривоги. Перехід до стану проектно-блокованої тривоги (будь-який стан → F) відбувається тоді, коли виникли умови або стан процесу, що означені в проекті для блокування тривоги. Означене проектом блокування зазвичай є автоматичною операцією. Перехід від проектно-блокованої тривоги до нормального стану або стану непідтвердженої тривоги (F → A або B) відбувається тоді, коли виникли умови, або змінився стан технологічного процесу, що означений для розблокування тривоги. Це зазвичай відбувається автоматично.

Щодо проектно-блокованих тривог система тривожної сигналізації повинна забезпечувати виконання наступних функцій:

- відображення проектно-блокованих тривог;
- формування записів в журнал для кожної проектно-блокованої тривоги.

Стан **виведеної з обслуговування тривоги** (G – Out-of-service state, **OOSRV**) – це стан, в якому тривога блокується вручну, як правило, при проведенні технічного обслуговування, і тому у цьому стані не потрібно проводити оповіщення. Тривога в цьому стані знаходиться під контролем технічного обслуговування. Виведена з обслуговування тривога – це не те саме, що виведення з обслуговування обладнання або його частини. Обладнання може бути виведене з обслуговування, тоді як відповідні тривоги – ні. Перехід до цього стану (будь-який стан → G) відбувається тоді, коли тривога виводиться з обслуговування (блокується) з метою технічного обслуговування обладнання або з інших причин. Як правило, виведення з обслуговування - це ручна операція. Перехід від стану виведеної з обслуговування тривоги до нормального стану або непідтвердженої тривоги (G → A або B) відбувається, як правило, також вручну, після закінчення обслуговування.

Щодо виведених з обслуговування тривог, система повинна виконувати функції:

- індивідуальне виведення та повернення кожної тривоги з/до обслуговування;
- відображення списку на дисплеї зведення виведених з обслуговування тривог або еквівалентного до нього;
- контроль доступу до виведення тривог з обслуговування;
- ведення запису виведення кожної тривоги з обслуговування.

На відміну від класичного автомату станів, механізм блокування далеко не завжди передбачається розробником, що приводить до наслідків, описаних на початку статті. Не дивлячись на те, що сучасні SCADA/HMI включають ці функції (або принаймні певні з них) «в коробці», вони часто просто ігноруються.

Також слід відмітити, що назви станів зовсім не співпадають у різних інструментах. Це не дивно, адже стандарт вийшов кілька років тому. Маємо сподівання, що з часом терміни будуть узгоджуватися, що значно спростить розробку і експлуатацію тих систем, які включають засоби автоматизації від різних фірм-постачальників.

Для узагальнення розуміння автомату станів в стандарті наводиться таблиця станів (див. таблицю1).

Таблиця 1 – Стани тривоги

ID	Скорочено	Назва стану	Стан технологічного процесу	Статус тривоги	Статус оповіщення	Статус підтвердження
A	NORM	Нормальний	В межах норми	Неактивна	Немає оповіщення	Підтверджена
B	UNACK	Непідтверджена тривога	За межами норми	Активна	Оповіщується	Непідтверджена
C	ACKED	Підтверджена тривога	За межами норми	Активна	Оповіщується	Підтверджена
D	RTNUN	Нормалізована непідтвердженої тривога	В межах норми	Неактивна	Оповіщується	Непідтверджена
E	SHLVD	Відтермінована тривога	В межах або за межами норми	Неактивна або активна	Заблокована	N/A
F	DSUPR	Проектно-блокована тривога	В межах або за межами норми	Неактивна або активна	Заблокована	N/A
G	OOSRV	Виведена з обслуговування тривога	В межах або за межами норми	Неактивна або активна	Заблокована	N/A

Діаграма поведінки тривоги в часі

Означення автомату станів це тільки перший крок для створення вдалої системи тривожної сигналізації. Для правильного налаштування тривог треба чітко розуміти всю послідовність етапів, яка проходить в контурі тривоги, показаної на рис.2. Слід не забувати, що задача тривожної системи сигналізації – це ***своєчасно*** проінформувати оператора про відхилення, допомогти йому усвідомити причину такого відхилення і максимально допомогти в прийнятті рішення. Якщо оператор не встигне зробити необхідні дії, в результаті недостатньої усвідомленості, несвоєчасного прийняття дій або за інших причин, об'єкт може перейти в аварійно небезпечний стан. Для того, щоб краще зорієнтуватися у виборі налаштувань для тривог в стандарті приводиться приклад діаграми поведінки тривоги в часі (див. рис.4). На рисунку показана вимірювана технологічна змінна, яка зростає від нормального стану до ненормального (тривожного) за двох можливих сценаріїв, що залежать від того, чи приймає оператор коригувальні дії.

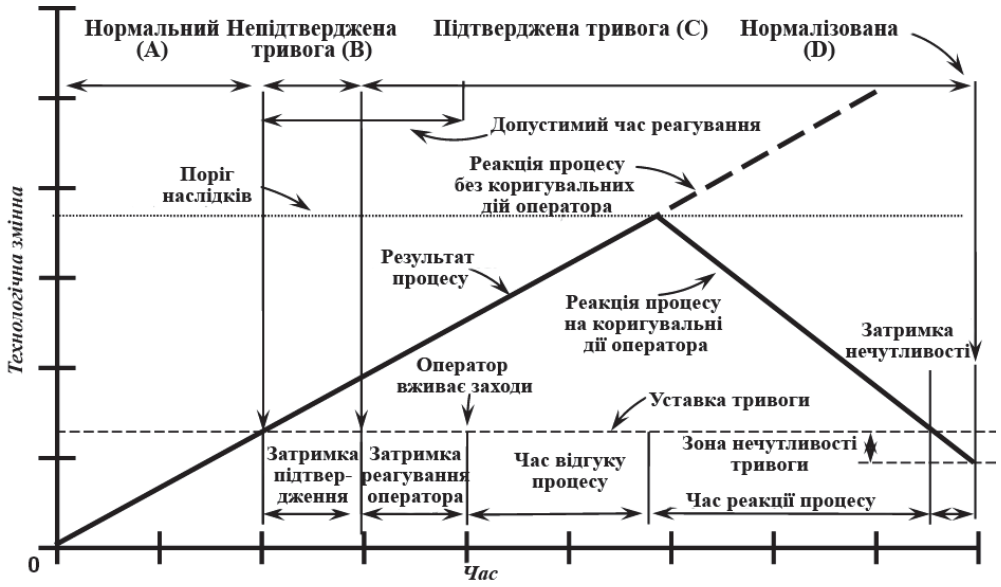

Рис. 4 – Діаграма поведінки тривоги в часі

Нормальний стан (A) означується як стан, в якому технологічний процес працює в межах звичайних характеристик. Коли вимірювальне значення перетинає уставку тривоги (з англ. alarm setpoint), вона переходить в стан непідтвердженої (B). Сигнал не відразу підтверджується оператором, проходить певний час (затримка підтвердження / acknowledge delay), після якого оператор підтверджує тривогу, і вона переходить у стан підтвердженої тривоги (C). Оператор може вжити заходів як до так і після підтвердження тривоги. Протягом цього часу тривога знаходиться в активному стані. Фактичний час реагування (з англ. actual response time) для сигналу тривоги – це максимальний час, що проходить між оповіщенням про тривогу і моментом, коли оператор повинен вжити заходів для уникнення наслідків. Він включає в себе виявлення сигналу тривоги, діагностування ситуації та визначення оператором коригувальних дій, а також виконання цих дій. Верхня межа часу відгуку – допустимий час реагування (з англ. allowable response time) – це максимальний час, що проходить між оповіщенням і моментом, коли оператор повинен вжити заходів для уникнення наслідків. Якщо дія не буде виконана за цей час, то наслідки будуть негативними. На рисунку затримка реагування оператора (з англ. operation response delay) відображається в межах допустимого часу. Результатом правильної дії оператора в межах допустимого часу реагування повинно бути повернення до нормального стану (D). Поріг наслідків (з англ. consequence threshold) є значенням змінної процесу, при якому починається виникнення наслідків (див. рис.4). Це може відбутися тоді, коли оператор не виконує жодних дій, вживається неправильна або недостатня дія, або дія не завершується протягом допустимого часу відповіді. Вплив зони нечутливості тривоги (з англ. alarm deadband) показаний на рис.4 через затримку нечутливості (з англ. deadband delay). На рисунку показано, що після перетину уставки тривога відразу не повертається до нормального стану, а проходить певний час.

Ця модель дозволяє на всіх етапах життєвого циклу ґрунтовно підійти до вибору правильних налаштувань. Навіть усвідомлення процесів такого вибору без формального їх виконання допомагає розробнику при створенні підсистем тривожної сигналізації.

Типи, класи, групи та пріоритети тривог

При означенні тривог в проекті необхідно чітко задати, за яких причин вони повинні виникати. Враховуючи, що типи умов можуть бути різними, в стандарті ISA-18.2 означене поняття **тип тривоги** (з англ. alarm type) – атрибут тривоги, який вказує на умову спрацювання тривоги. У таблиці 2 наведені типи тривог, які означені в стандарті ISA-18.2.

Таблиця 2 – Типи тривог

Назва (англ.)	Назва (укр.)	Умова спрацювання
absolute alarm	абсолютна тривога	вихід за уставку тривоги; наприклад, дуже високе, високе, низьке, дуже низьке значення
deviation alarm	тривога відхилення	різниця між двома значеннями перевищує уставку тривоги; наприклад, відхилення сигналів вимірювань між первинними та резервними приладами або відхилення між дійсним та заданими значеннями змінної процесу
rate-of-change alarm	тривога швидкості зміни змінної	швидкість зміни змінної процесу (dPV/dt) перевищує уставку
discrepancy alarm	тривога невідповідності	очікуваний стан установки або пристрою та його фактичний стан відрізняються; наприклад, після команди на двигун немає зворотного сигналу про те, що він запустився
calculated alarm	обчислювальна тривога	генерується по розрахунковому значенню, а не по прямим вимірюванням процесу
recipe-driven alarm	керована рецептом тривога	вихід за уставку, що змінюється системою в залежності від рецепту, який в даний час виконується
bit-pattern alarm	тривога по бітовому шаблону	шаблон цифрових сигналів (комбінація кількох бітів) відповідає встановленому

controller-output alarm	тривога по виходу регулятора	вихід за уставку вихідного сигналу алгоритму керування (наприклад, ПІД-регулятору); в противагу абсолютній тривозі використовується не прямий вимірювальний сигнал процесу, а вихід регулятора
system diagnostic alarm	системно-діагностична тривога	несправність в системі апаратного чи програмного забезпечення або компонентів; генерується системою керування, а не застосунком; наприклад, комунікаційна помилка
instrument diagnostic alarm	тривога діагностування приладу	несправність польового пристрою або його сигналу; наприклад, тривога виходу сигналу за межі
adjustable alarm	налаштовувана оператором тривога	вихід за уставку, яка може бути змінена вручну оператором
adaptive alarm	адаптивна тривога	вихід за уставку, яка змінюється алгоритмом; наприклад, уставка розраховується на основі швидкості вироблення продукції
re-alarming alarm	повторно сигналізована тривога	після спрацювання тривоги, виникають нові умови для повторного оповіщення
statistical alarm	статистична тривога	результат статистичної обробки технологічної змінної чи змінних не задовольняє вказаному в умові тривоги
first-out alarm	першо-причинна тривога	спрацювання умови раніше, ніж у інших з вказаної послідовності; наприклад, при вимкненні кількох одиниць обладнання в короткий проміжок часу, одне з них, яке вимкнулося раніше буде причиною;
bad-measurement alarm	тривога помилки вимірювання	сигнал вимірювальної величини знаходиться за межами очікуваного діапазону (наприклад, 3,8 мА для сигналу від 4 до 20 мА)

Кожен тип потребує окремого розгляду. Не всі з перерахованих типів тривог можуть бути доступними в SCADA/HMI. Крім того, у деяких випадках може знадобитися інший тип тривог, який не входить в перелік таблиці 2. Також дозволяється комбінувати типи.

У системі тривожної сигналізації кількість тривог може сягати сотні і тисячі. Означення таких тривог потребує опису та означення пріоритетів, дій які необхідно зробити оператору при їх виникненні, правила адміністрування та таке інше. Якщо це робити для кожної тривоги окремо, обсяг робіт та необхідних знань для операторів буде надзвичайно великим та неефективним. Замість цього, в стандарті ISA-18.2 рекомендується використовувати класифікацію тривог, та означення необхідних параметрів вже не для конкретної тривоги, а для всього класу. **Клас тривог** (з англ. alarm class) – сукупність тривог з загальними вимогами щодо організації функціонування тривог (наприклад, вимоги до тестування, підготовки, моніторингу та планової перевірки). Приклад класу – тривоги протиаварійного захисту. Одна тривога може входити до кількох класів одночасно, тобто класи можуть перекриватися.

Крім об’єднання за класом тривог, є сенс їх групувати за ознакою приналежності до обладнання або частини процесу. **Група тривог** (з англ. alarm group) – набір тривог, які мають спільні взаємозв’язки з частиною технологічного процесу, установкою, набором обладнання або послугою. Таке групування може значно спростити аналіз причин виявлення відмов як в реальному часі, так і в пост-аналізі.

При виникненні кількох тривог, оператору необхідно швидко визначитися з тим, яку з них необхідно опрацювати першою. Для цього в стандарті визначено поняття **пріоритет тривоги** (з англ. alarm priority) – це відносна важливість, призначена тривозі в системі, для позначення терміновості реагування на тривогу (наприклад, серйозність наслідків і допустимий час реагування). При розробці пріоритети вибираються, виходячи з того, що вищі пріоритети назначаються рідше, ніж нижчі. Більша кількість тривог мають найнижчий пріоритет (найменш важливі), а менша кількість – найвищий (найважливіші). Отримані пріоритети повинні бути узгодженими з наслідками і допустимим часом реагування. Таким чином, тривоги з найнижчим пріоритетом мають мати найменш тяжкі наслідки і найбільший допустимий час реагування, а найвищого – найсерйозніші наслідки (наприклад, пожежні та сигналізації загазованості) і найменший допустимий час реагування.

Атрибути тривог

Властивості означені в стандарті як **атрибути тривог** (з англ. alarm attribute) повинні бути описані та сконфігуровані в системі для кожної з тривог. Тривоги повинні містити наступні атрибути: опис тривоги (з англ. alarm description), уставку тривоги (з англ. alarm setpoint) або логічну умову (з англ. logical condition), пріоритет тривоги (з англ. alarm priority), зону нечутливості тривоги (з англ. alarm deadband), затримку на спрацювання (з англ. on-delay) або затримку на відключення (з англ. off-delay) тривоги, групу тривоги (з англ. alarm group), повідомлення тривоги (з англ. alarm message). У багатьох випадках вказані вище атрибути задаються в підсистемі тривог статично, проте нерідко їх значення повинні змінюватися оператором або програмно (наприклад, в адаптивних тривогах). Зміна цих атрибутів може бути пов'язана з типом виготовлюваного продукту або станом технологічного процесу.

Людино-машинний інтерфейс для систем тривожної сигналізації

Враховуючи, що саме людина є ключовим елементом контуру тривожної сигналізації, велика увага в організації системи тривожної сигналізації приділяється людино-машинному інтерфейсу. Він повинен чітко відображати неблоковані активні тривоги з вказівкою їх станів, пріоритетів, типів та іншої додаткової інформації. Крім відображення, ЛМІ повинен надати можливість оператору здійснювати наступні дії: індивідуально підтвердити тривогу, заглушити звукове оповіщення тривоги (без дії підтвердження), виводити тривоги з обслуговування, змінювати параметри тривоги, ініціювати відтермінування тривоги, підтримувати функцію проектно-блокованих тривог, відображати повідомлення тривоги за запитом оператору, забезпечувати доступ до певних функцій тільки авторизованим для цього користувачам.

Для забезпечення вказаних вище функцій відображення та дій, ЛМІ має надавати певні інструментальні засоби. Стандарт передбачає підтримку як мінімум таких засобів ЛМІ: дисплей зведення тривог (з англ. alarm summary), відображення тривог на дисплеях процесів (мнемосхемах), відображення (індикація) тривог на дисплеях деталізації тегів, дисплей зведення відтермінованих тривог, дисплей зведення проектно-блокованих тривог, дисплей зведення виведених з обслуговування тривог.

Для однозначного розрізнення станів тривог на ЛМІ A-D (див. рис.3) використовуються комбінації візуальних індикаторів та/або звукових сигналів. Надалі показані рекомендації до способів оповіщення, які часто використовуються на практиці.

Рекомендації щодо звукової сигналізації та індикації в залежності від станів наведені в таблиці 3.

Таблиця 3 – Поведінка звукової сигналізації та індикації в залежності від стану тривоги

Стан тривоги	Звукова сигналізація	Візуальна індикація		
		Колір	Символ	Миготіння
Нормальний	Ні	Ні	Ні	Ні
Непідтверджена тривога	Так	Так	Так	Так
Підтверджена тривога	Ні	Так	Так	Ні
Нормалізована, непідтверджена	Ні	Комбінація		Опція
Відтермінована	Ні	Опція		N/A
Проектно-блокована	Ні	Опція		N/A
Виведена з обслуговування	Ні	Опція		N/A

Розширені та прогресивні методи організації тривог.

Окрім основних («класичних») функцій, додаткову функціональність системи тривожної сигналізації можуть надати так звані розширені та прогресивні методи організації тривог. Згідно стандарту ISA-18.2 ці методи передбачають додаткові шари логіки, програмування або моделювання, які використовуються для зміни атрибутів тривог. **Прогресивне керування тривогами** (з англ. **advanced alarming**) змінює поведінку тривоги, базуючись на різних методах. До методів прогресивного керування тривогами входять:

- керування тривогами на основі логіки (з англ. logic based alarming);
- динамічне керування тривогами (з англ. dynamic alarming);
- стано-орієнтоване керування тривогами, наприклад на основі стану (з англ. state-based alarming) або режиму (з англ. mode-based alarming);

- адаптивні тривоги (з англ. adaptive alarms).

Розширені та прогресивні методи керування тривогами часто використовуються в тому випадку, коли базовий функціонал тривожної сигналізації не досягає цілей продуктивності, зазначених у методології системи тривожної сигналізації. Складність розширених і прогресивних методів керування тривогами потребує додаткових ресурсів для проектування, впровадження та обслуговування. Щоб зменшити залежність реалізації методик від можливостей SCADA/HMI розробники нерідко реалізовують ці функції на рівні ПЛК, зокрема, як це робиться в PAC Framework [8],[9].

Системи тривожної сигналізації можуть бути посилені шляхом прив'язки до інформації в основній базі даних тривоги (наприклад, дії оператора або наслідки). Це розширення надає можливість при виникненні тривоги надати оператору інформацію з центральної бази даних тривоги або навпаки – занести туди проведені дії оператора. Інформація також може бути пов'язана з іншими джерелами, включаючи: операційні процедури, журнали операторів, історію обслуговування або проектні документи.

Деякі розширені і прогресивні методи керування тривогами потребують можливість зміни певних атрибутів тривоги (наприклад, зміну уставки або пріоритету тривоги). Така модифікація потребується за причини зміни умов експлуатації процесу або установки. До таких належить стано-орієнтоване керування тривогами – прогресивний метод, який змінює атрибути тривоги на основі означених робочих станів для обладнання або процесів. Стани часто визначаються через:

- статус змінної;
- означеної змінної процесу, яка досягає певної межі;
- логіку, яка розглядає багато змінних і показників;
- вибору оператора.

Окремої уваги заслуговує керування тривогами для так званих Batch процесів для багато-рецептурних виробництв. Batch виробництво (порційне) – це виробництво, в якому кожен продукт виготовляється поетапно за окремим рецептом. По суті, рецепт означує набір етапів, та задані параметри. Тут є багато особливостей, які характерні саме для таких процесів і які треба врахувати в порівнянні до неперервних виробництв:

- установка не завжди працює, а отже багато вимірювальних величин будуть поза нормальними межами;
- задані значення параметрів залежать від рецепту;
- деякі технологічні тривоги залежать від рецепту і задаються при його створенні.

Це тільки деякі з особливостей Batch-керування, більше про це можна прочитати в стандарті ISA-88, коротко про це описано в [10]. У будь-якому випадку, тривоги у Batch-процесах потребують зміни атрибутів в залежності від умов, станів і етапів процесу. Якщо це не враховується, система тривожної сигналізації приречена на переповнення тривог. Крім того, у звичайних системах тривожної сигналізації дані та записи тривоги зазвичай фіксують календарний час. Для інформативності журналів тривог для Batch процесів більш важливим є відносний час, тобто час від початку партії або кроку процесу. У цьому випадку особливістю прогресивних методів є можливість фіксувати календарні відмітки часу початку кроку або етапу партії і виводити тривоги відносно цього часу. Слід також враховувати, що такі виробництва часто вимагають прив’язки записів тривог до номеру партії. У такому випадку, при виборі номеру партії можна вивести усі записи тривог та повідомлення, які відбувалися під час виготовлення продукту.

Висновки.

Наявність міжнародних стандартів з закріпленими в них кращими практиками позитивно впливає на усі етапи життєвого циклу систем автоматизації або її складових. Стандарт ISA-18.2 не є виключенням. Після його появи було відмічено певні позитивні зміни в наявних інструментах та шаблонах, доступних в засобах SCADA/HMI. По аналізу цього стандарту в частині наведених моделей та функцій можна зробити наступні висновки:

- стандарт надає базові моделі для розуміння місця та призначення (під)системи тривожної сигналізації в структурі АСКТП, що дає змогу більш ефективно проектувати такі системи;
- стандарт означує чіткий єдиний автомат станів, що обумовлює його закріплення як основного у всіх засобах та проектах SCADA/HMI;
- стандарт означує типовий набір функцій системи тривожної сигналізації, що дає можливість зосередитися розробнику на їх реалізації та описувати вимоги до них в ТЗ;
- в стандарті визначено багато термінів, які в майбутньому повинні стати основними в засобах SCADA/HMI;
- стандарт може бути основою для підготовки спеціалістів, задіяних в життєвому циклі АСКТП.

Ми сподіваємося, що даний стандарт в редакції IEC 62682 в найближчому майбутньому буде прийнятим в Україні методом перекладу, що значно підвищить якість розроблювальних АСКТП. Однак наразі робота над стандартами проходить на волонтерських засадах, що уповільнює цей процес. Маємо сподівання, що дана стаття хоч якимось чином компенсує необізнаність українських спеціалістів та допоможе їм зорієнтуватися в майбутньому. Наступна публікація буде присвячена розумінню робочих процесів, які необхідно провести для ефективного розроблення, впровадження та експлуатації системи тривожної сигналізації.

Список використаних джерел

[1] The costs to Britain of workplace accidents and work-related ill health in 1995/96 – Sudbury: HSE Books, 1999. – 133 c. – (Secon edition).
[2] Out of control: Why control systems go wrong and how to prevent failure [Електронний ресурс] // Hse.gov.uk – Режим доступу до ресурсу: http://www.hse.gov.uk/pubns/books/hsg238.htm.
[3] ISO 11064-3:1999 [Електронний ресурс] – Режим доступу до ресурсу: https://www.automation.com/library/resources/pas-and-epri-publish-alarm-management-applications-guidelines.
[4] 49 CFR § 195.446 - Control room management. [Електронний ресурс] // LII / Legal Information Institute. – 2017. – Режим доступу до ресурсу: https://www.law.cornell.edu/cfr/text/49/195.446.
[5] IEC Functional Safety and IEC 61508. [Електронний ресурс] // Iec.ch. – 2010. – Режим доступу до ресурсу: https://www.iec.ch/functionalsafety/.
[6] PAS and EPRI publish Alarm Management Applications Guidelines [Електронний ресурс] // Automation.com. – 2008. – Режим доступу до ресурсу: https://www.automation.com/library/resources/pas-and-epri-publish-alarm-management-applications-guidelines.
[7] ANSI/ISA-18.2-2016, Management of Alarm Systems for the Process Industries [Електронний ресурс] // Isa.org. – 2016. – Режим доступу до ресурсу: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=46962374.
[8] PAC Framework [Електронний ресурс] // i4u. – 2018. – Режим доступу до ресурсу: https://sites.google.com/view/i4uinua/%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97/pac-framework?fbclid=IwAR1plmVn_xc5pZPSx2c8TjaH8-GaGe2u8x-fdEwKz5q4zHq8qkGRVmazPII.
[9] Pupena O. Development of the framework for the controllers of the process base management system to meet the requirements for integration with other subsystems and to implement service functions and diagnostics service / O. Pupena, R. Mirkevich, O. Klymenko, V. Polupan // Енергетика і автоматика. - 2017. - № 4. - С. 78-89.
[10] COMPUTER INTEGRATED MANUFACTURING: OVERVIEW OF MODERN STANDARDS / O.Pupena, I. Elperin, R. Mirkevich, O. Klymenko. // Automation of technological and business processes. – 2017. – №8. – С. 63–74.

References

[1] The costs to Britain of workplace accidents and work-related ill health in 1995/96. (1999). 2nd ed. Sudbury: HSE Books.
[2] Hse.gov.uk. (2003). Out of control: Why control systems go wrong and how to prevent failure - HSG238. [online] Available at: http://www.hse.gov.uk/pubns/books/hsg238.htm [Accessed 25 Jun. 2019].
[3] 11064-3:1999, I. (2009). ISO 11064-3:1999. [online] ISO. Available at: https://www.iso.org/standard/19044.html [Accessed 26 Jun. 2019].
[4] LII / Legal Information Institute. (2017). 49 CFR § 195.446 - Control room management. [online] Available at: https://www.law.cornell.edu/cfr/text/49/195.446 [Accessed 26 Jun. 2019].
[5] Iec.ch. (2010). IEC Functional Safety and IEC 61508. [online] Available at: https://www.iec.ch/functionalsafety/ [Accessed 26 Jun. 2019].
[6] Automation.com. (2008). PAS and EPRI publish Alarm Management Applications Guidelines. [online] Available at: https://www.automation.com/library/resources/pas-and-epri-publish-alarm-management-applications-guidelines [Accessed 26 Jun. 2019].
[7] Isa.org. (2016). ANSI/ISA-18.2-2016, Management of Alarm Systems for the Process Industries. [online] Available at: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=46962374 [Accessed 26 Jun. 2019].
[8] Sites.google.com. (2018). i4u - PAC Framework. [online] Available at: https://sites.google.com/view/i4uinua/%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97/pac-framework?fbclid=IwAR1plmVn_xc5pZPSx2c8TjaH8-GaGe2u8x-fdEwKz5q4zHq8qkGRVmazPII [Accessed 16 Jul. 2019].
[9] Pupena, O., Mirkevich, R., Klymenko, O. and Polupan, V. (2017). Development of the framework for the controllers of the process base management system to meet the requirements for integration with other subsystems and to implement service functions and diagnostics service. Енергетика і автоматика, 4, pp.78-89.
[10] Pupena, O., Elperin, I., Mirkevich, R. and Klymenko, O. (2016). COMPUTER INTEGRATED MANUFACTURING: OVERVIEW OF MODERN STANDARDS. Automation Technological and Business - Processes, 8(3), pp.63-74.