Investigation of the compressed air energy storage (CAES) system utilizing systems-theoretic process analysis (STPA) towards safe and sustainable energy supply

Zhang, Aibo; Yin, Zhaoyuan; Wu, Zhiying; Xie, Min; Liu, Yiliu; Yu, Haoshui

Published in:
Renewable Energy

DOI (link to publication from Publisher):
10.1016/j.renene.2023.02.098

Creative Commons License
CC BY 4.0

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

Link to publication from Aalborg University

Citation for published version (APA):
Zhang, A., Yin, Z., Wu, Z., Xie, M., Liu, Y., & Yu, H. (2023). Investigation of the compressed air energy storage (CAES) system utilizing systems-theoretic process analysis (STPA) towards safe and sustainable energy supply. *Renewable Energy*, *206*, 1075-1085. https://doi.org/10.1016/j.renene.2023.02.098

Contents lists available at ScienceDirect

Renewable Energy

journal homepage: www.elsevier.com/locate/renene

Investigation of the compressed air energy storage (CAES) system utilizing systems-theoretic process analysis (STPA) towards safe and sustainable energy supply

Aibo Zhang [a,b], Zhaoyuan Yin [c], Zhiying Wu [c,d], Min Xie [b,c], Yiliu Liu [e,**], Haoshui Yu [f,*]

[a] School of Mechanical Engineering, University of Science and Technology Beijing, Beijing, China
[b] Centre for Intelligent Multidimensional Data Analysis Limited, Hong Kong Science Park, Hong Kong
[c] Department of Advanced Design and Systems Engineering, City University of Hong Kong, Hong Kong
[d] Centre for Artificial Intelligence & Robotics, Hong Kong Institute of Science & Innovation, Chinese Academy of Sciences, Hong Kong Science Park, Hong Kong
[e] Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, Norway
[f] Department of Chemistry and Bioscience, Aalborg University, Esbjerg, Denmark

ARTICLE INFO

Keywords:
Renewable energy
Energy storage
CAES system
STPA method
Hazard identification
Risk management

ABSTRACT

Renewable energy attracts increasing attention from both industry and academia under the context of carbon neutrality. For wind and solar energy, the strong dependence on natural processes results in the imbalance between energy production and real demands. Energy storage technologies, e.g., Compressed Air Energy Storage (CAES), are promising solutions to increase the renewable energy penetration. However, the CAES system is a multi-component structure with multiple energy forms involved in the process subject to high temperature and high-pressure working conditions. The CAES system is a complex process flowsheet consisting of charging and discharging process. The process should be optimized to achieve the best thermodynamic and economic performance. Under the optimal design conditions, it might lead to severe consequences once a failure occurs, e.g., harm to humans, the environment, and assets. Limited attention and scarce available information have been paid to the CAES system risk management yet. Hence, this paper applies the System-Theoretic Process Analysis (STPA), which is a top-down method based on system theory, to identify the CAES system safety hazards. The results are expected to provide a preliminary guideline for practitioners regarding the safety and reliability of the CAES system. As a result, a more reliable CAES system can contribute to a more flexible energy system with more efficient and economic utilization of fluctuating renewable energy.

1. Introduction

Renewable energies, such as solar, wind energy, etc., are one of the main solutions for decarbonization of electricity supply and alleviating climate change. One barrier of utilizing such new energies lies in their intermittence and instability in production. Energy storage technologies, thus, promisingly mediate to clear the obstruction and increase the system reliability to a certain extent [1,2]. Energy storage emphasizes the capture and storing of the surplus energy output of renewable energy sources during times of energy over-production and then be drawn upon at a later time to bridge the imbalances between production and demand.

There are multiple choices of energy storage technologies either deployed or under consideration including pump-hydro, compressed air, battery, liquid air, thermal energy storage systems, etc. [3–5]. Among them, compressed air energy storage (CAES) systems have advantages in high power and energy capacity, long lifetime, fast response, etc. [6]. CAES system has two separate processes in terms of time, namely the charging and discharging process. The charging process of CAES system uses electrical power during the off-peak hours to compress the ambient air, converting electricity into mechanical and thermal energy and thus storing the excess electricity. The pressurized air then is stored in huge space (salt caverns, saline aquifers, etc.) at quite high pressures (e.g., 50 bar or even higher) and pending to be heated and expanded through a turbine to generate electricity in the discharging process when the electricity is needed. CAES can be classified into multiple categories

[*] Corresponding author.
[**] Corresponding author.
E-mail addresses: yiliu.liu@ntnu.no (Y. Liu), hayu@bio.aau.dk (H. Yu).

https://doi.org/10.1016/j.renene.2023.02.098
Received 12 October 2022; Received in revised form 31 January 2023; Accepted 18 February 2023
Available online 25 February 2023

following the criterion on the treatment way of the compression heat or the volume and pressure of the compressed air in the container. CAES can be classified as adiabatic, diabatic, or isothermal, with the retention of the compression heat in a thermal storage system, expulsion into the environment irreversibly or reversibly at a constant temperature, respectively [7]. Also, CAES can be categorized into isochoric and isobaric following the latter classification criterion [8]. The potential candidates for utility-scale energy at the present time are the isochoric diabatic and isochoric adiabatic CAES systems [2]. The application of CAES system is still in its infancy, though two plants, which use diabatic processes, have been built in Huntorf (Germany) and McIntosh (Alabama, America) plants of 290 MW and 110 MW, respectively [9]. It is worth mentioning that the third CAES plant is planned with a generator capacity of 324 MW with an expected operation date in 2025 located in Bethel energy center, Texas, USA [10].

Over the past decades, publications concerning hazard identification and assessment of energy systems have been growing along with the increasing demand for renewable energy to reduce accidents with their associated impacts. Authors in Ref. [11] establish a target risk assessment framework for the wave-wind-solar-compressed air energy storage system through fuzzy theory. Target risk response strategies in several aspects, e.g., management, economy, and internal and external environment, are thus proposed based on the risk calculation result. Rosewater et al. [12] conduct the safety study of a lithium-ion battery-based grid energy storage system by the systems-theoretic process analysis (STPA) method to capture casual scenarios for accidents. The fire and explosion hazards of the commercial/industrial battery energy storage systems are identified and mitigation measures to reduce these relevant risks are followed [13]. Qi et al. [14] examine the potential hazards for various kinds of industrial electrical energy storage systems, including compressed and liquid air energy storage, CO_2 energy storage, and Power-to-Gas etc., and provide guidelines for the elimination and mitigation of identified hazards via both administrative and engineering controls. Singh et al. [15] focus on the risk assessment and safety barriers of typical gird energy storage systems, and its most hazardous initiating event is then analyzed based on the fundamental event tree method. Specifically, the rupture of compressed storage tank in CAES is identified as a catastrophic failure. The ignition and explosion risk of using depleted natural gas reservoirs as the storage vessel for CAES is presented and possible mitigating measures follow [16]. From the system engineering perspective, the sufficiently safe operation of the connected renewable energy network requires a need for heightened understanding of the potential hazards in the CAES system and more extensive measures to reduce the accidents, covering its lifecycle covering from design, plan, operation, and to decommission stages [17].

Currently, many technologies of the CAES system are still under development with a focus on improving energy storage efficiency and energy density, which are considered as the design performance indicators [18–20]. The thermodynamics performance and service time of the CAES system undoubtedly take up the priority place in the stakeholders' consideration of renewable energy systems. However, safety concerns are inherently accompanied by and deserving attention, which results from several aspects, e.g., the contained considerable amount of energy, extreme working conditions, and multiple components operating intermittently to cover a range of functions. In terms of the function and structure of a CAES system, it typically consists of several key subsystems, including charging subsystem, discharging subsystem, and air storage subsystem. Each subsystem following the function is composed of several components, e.g., compressors in the charging subsystem and gas turbines in the discharging subsystem. These components are required to possess the ability to swing quickly from the generation to compression modes and cycle usually on a daily basis. Moreover, the involvement of high-pressure and high-temperature air in the whole process challenges stable component performance. Unrecoverable damage on the component bringing consequence might occur if the working condition is beyond the specification, e.g., the mechanical explosion caused by the over-pressure of the air storage or the internal leakage of the heat exchanger due to the high temperature, etc. These characteristics can pose significant potential safety problems to the persons, facilities, and/or the environment, and thus safety-related concerns should thus be a priority when designing and implementing or upgrading the existing CAES. It is, therefore, of great significance for reasonable hazard identification and well-founded responses in CAES project's whole life cycle.

Nevertheless, as the aforementioned statement, CAES is still in its infancy, which means limited public information regarding risk management experience is available. The absence of appropriate models describing their characteristics in the operation phase contributes to the incapability of typical hazard identification methods techniques on CAES projects, e.g., hazard and operability study (HAZOP), fault tree analysis (FTA), failure mode and effect analysis (FMEA), and so on [21]. STPA method is thus a potential solution to meet the need of hazard analysis in CAES system, which is capable for identifying hazards and analyzing risk during a system's initial development process [22]. The STPA is a relatively new hazard analysis technique based on system theory with treating safety as a control problem, which makes it desirable for complex systems [23,24]. It is a top-down method to capture dysfunctional (unsafe or insecure) behaviors, as well as the organizational and human factors, rather than focusing on the physical failures [25,26]. It indicates that STPA method has a broader potential scenarios analysis, including those for which no failure occurs, and the problems arising due to unsafe and unintended interactions between system components, which is beneficial in identifying more causal scenarios besides the common ones with the other traditional methods [27]. STPA method has been applied in several different domains [28–30], demonstrating its universal applicability.

Thus, considering the scarce prior knowledge of safety controls in the CAES system, this study aims to fill the blank of CAES risk analysis by taking the advantage of the STPA method in the hazard identification and safety requirements. The application of STPA is expected to provide a picture of safety controls and specification of safety constraints for practitioners and stakeholders of the CAES projects. In addition, the established STPA framework in this study, serving as a preliminary study, is feasible to be expanded and enriched along with expert knowledge and brainstorming when designing or implementing a new CAES project or upgrading the existing ones.

The potential highlights of this study can be summarized as follows:

- Based on the common characteristics of CAES systems, the hazard assessment is conducted following the three processes, namely the charging, storage, and discharging process;
- The potential safety concerns and hazards of the CAES system are investigated;
- A STPA-based framework is proposed to identify unsafe control actions and specify the safety requirements of the CAES system.

This paper is organized as follows: Section 2 elaborates on the CAES system and safety concerns in detail. Section 3 provides the description of the STPA method and applies the STPA to CAES system. It is intended to identify the major hazards and specify the corresponding safety requirements. Section 4 presents the discussions based on the findings from STPA. The concluding remarks are presented in Section 5.

2. CAES description

2.1. System structure, operation, and characteristics

A CAES system is an electricity storage technology and most appropriate for large-scale use and longer storage applications [31]. A CAES system may come in a variety of configurations to meet the specific operating conditions. It generally consists of compressors, driving motors, storage containers (tanks, caverns), gas turbines, and other components to complete a full cycle from the compression of air and storage of compressed air for power generation at a later time when required [32]. The CAES system stores the electrical energy in a mechanical form through the compression of the air to high pressure (e.g., 50 bar or even higher) and holds the air in some specific containers, e.g., tanks, underground caverns, and saline aquifers. It is considered as a promising technology to integrate highly intermittent renewable energy sources, like wind and solar energy, into power grid to satisfy fluctuating electricity demands and maintain the stability and reliability of the power grid [33]. As outlined in its concept, the CAES system leverages two separate processes, namely the charging and discharging process, to decouple the generation and consumption of the power in the time and space domains [34].

In the charging process, ambient air is pressurized by the multistage compressor using off-peak electricity from the grid or/and renewable energy, accompanied by the concentrated heat energy in the decreasing volume of air. To maintain proper operating temperatures, the excessive heat has to be transferred through heat transfer fluids in the heat exchangers to decrease the temperature of the compressed air before going out into the storage. When the pressure of the storage tank reaches the maximum value, the charging process is completed. During the discharging process, the compressed air is first heated by the heat exchangers and then expand through gas turbines to generate electricity, thus the stored mechanical energy is converted back to electricity [35,36].

There are generally diabatic and adiabatic CAES methods with the difference located in the treatment of the compression heat produced in the system. Briefly, the heat generated during compression is simply treated as waste and released to the cooling medium in diabatic CAES system, while, the adiabatic CAES system integrates the thermal energy storage (TES) system to capture and store the heat and reuse the compression heat later in the discharging process [37]. Despite the efficiency consideration, the adiabatic CAES is more complicated in structure due to the integration of the TES system. It implies that the adiabatic CAES system might have safety concerns related to the TES system in the operational phase, besides the ones in the air charging and discharging process which is consistent with the diabatic CAES system. A TES system normally can be classified into two groups: low- and high-temperature TES, consisting of an energy transfer medium in a reservoir/tank, pumps, piping network, and the integrated heat exchangers with the CAES system in the structure. Diathermic oil and water, in consistency with most temperature regulation systems, are considered as the medium in the TES system [36]. In the charging process, a pump with adapted seals and bearings circulates the medium from the cold tank to the hot tank to cool the high-temperature compressed air and recover the heat of compression and store it. While in the discharging process, the TES medium is circulated from the hot to the cold tank through a pump that heats the high-pressure air to be fed into gas turbines to enhance the thermal efficiency [38,39]. A schematic diagram of the CAES system with the integration of the TES system is depicted in Fig. 1. The main parameters of two current existing CAES plants are listed in Table 1.

CAES systems usually operate under off-design conditions, which result from several factors, e.g., the intermittency and volatility of integrated renewable energies, and changes in environmental conditions such as ambient temperature and pressure [41,42]. The off-design operation makes the CAES system always operate in unsteady states, which brings difficulties to the optimal system operation and control, and consequently threatens the system and process safety.

2.2. Safety concerns

As with most technologies, CAES has safety concerns, involving potentially high risks for the health, facilities, and/or the environment due to the exposure to high temperature, high pressure, high voltage, strong current, etc. To avoid ambiguity, the widely accepted definitions in engineered systems of certain terminologies, including safety, hazard, and risk, are adopted in this study. Specifically, the risk for engineered systems is related to accidents where an abrupt event may give negative outcomes, e.g., loss or damage to people, equipment, and/or environment. Safety refers to the state being 'safe' as the absence or at least acceptable risk of accidents and incidents. A hazard refers to a physical or chemical condition that may cause potential harm to something valued as humans, equipment, and/or the environment [14].

Many systems nowadays are based on electrical, electronic, or programmable electronic (E/E/PE) technology with no exception for the

Table 1
Huntorf and McIntosh CAES technical data ([31,40]).

Technical data	290 MW CAES in Huntorf, Germany	110 MW CAES in McIntosh, Alabama, USA
Power	290 MW@50HZ	226 MW@60HZ
Air storage for	1160 MWh = 4hrs@290 MW	2640 MWh = 24hrs@ 110 MW
Cavern Volume	310,000m^3 (2 caverns)	538,000m^3
Turbines Mass Flow Rate	416 kg/s	154 kg/s
Compressors Mass Flow Rate	104 kg/s	96 kg/s
Depth of the cavern	600m	450m
Pressure tolerance	50–70 bar	45–76 bar

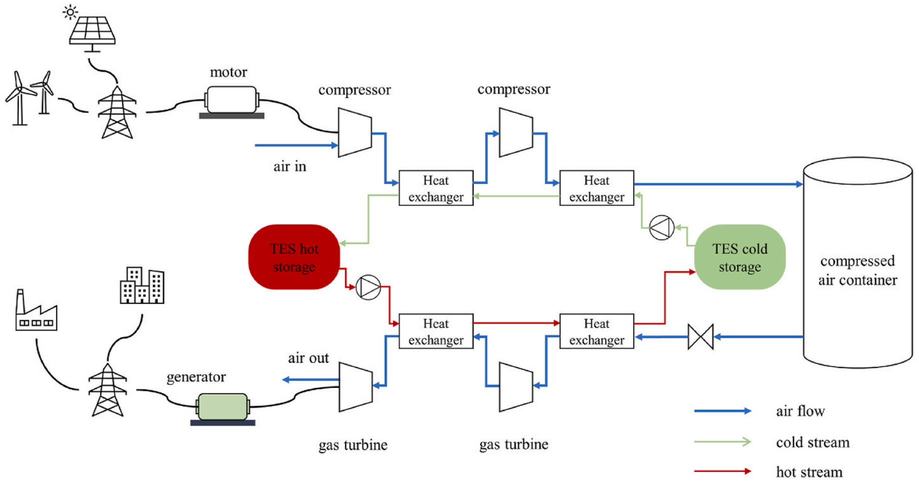

Fig. 1. Schematic diagram of the CASE system with the integration of the TES system.

CAES system. It starts by collecting signals from the input elements which are used to monitor a certain process, e.g., temperature, pressure, level, or flow, and then sends signals to the logic controller or programmable controller to make decisions on how to act on the input, the specific action would be conducted through the actuation of final elements [43]. These logic controllers or programmable controllers follow predefined requirements, supervised by human operators, to monitor and ensure the main components, like compressors and gas turbines, work safely.

In the context of the CAES process and system, as depicted in Fig. 1, the main component in the charging process is the compressors, with assistance from other vital components, e.g., motors, heat exchangers, pipelines, etc. The motor regulates the speed of the air compressor by providing power to the compressor head, forcing air through an airline, and stored in the container. Inlet guide vanes (IGVs) or inlet butterfly valves (IBVs) are installed as the regulators for the airflow and pressure entering the compressor. In addition, the air filters prevent the efficiency reduction of the compressor from fouling resulting from the entering of dust or residues. The temperature control valve provides temperature control of lubrication oil within the set interval. Driven by the circulating pump, the thermal medium within the tube of heat exchangers transfers the heat but is separated by a solid wall to follow the designed routine preventing mixing or direct contact. The prerequisite of smooth air storage is that the air pressure at the outlet of the compressor should be always greater than the pressure of the air in the storage container. During the discharging process, the air pressure in the storage container decreases gradually from a relatively high along with the electricity generation of the gas turbine. A throttling valve is configured between the air container and heat exchangers to regulate the pressure of the compressed air into the gas turbines [11]. The remaining air in the container will not continue to drive the turbine when the pressure is lower than the specified inlet pressure of the turbine. The load and release pressure are generally regulated through the main valve opening and the flow rate of the cryopump. In addition, the purpose of regulating the circulating heat transfer medium is to ensure that the outlet temperature of reheater water at all parts remains above the dew point [42]. The main embedded E/E/PE systems to regulate the performance of a CAES system for the regulations can be described in Fig. 2.

These main components in the CAES system are theoretically expected to operate under a steady state, indicating that the behavior of the system or process is constant in time. However, there are several factors influencing the actual performance and breaking the steady state, such as component status, operation conditions, energy requirements, etc. [44]. External disturbance, e.g., environmental or operational changes, may bring potential hazards and lead to accidents whose occurrence probability is low but could lead to undesirable consequences once occur. The first significant safety concern is the fire/chemical explosion within the process equipment. It raises from the fact that all the elements necessary for fire or explosion are contained simultaneously in the CAES system, namely oxygen from the air, fuel from the lubricating system or diathermic oil, and heat from the compression process. A possible mix may occur if the tube in the heat exchanger leaks [14]. Meanwhile, the container failure may happen because of the overpressure of the stored high-pressure air lacking the regulation from the main valve consequently leading to damage to the surroundings. If the underground caverns are chosen for air storage, the potential risks could be surface subsidence and cavern failure, in which pressure in the carven is the main contributor from the operational perspective. This kind of cavern failure accident may cause a huge economic loss and environmental impact [45,46]. The third concern is the potential economic loss related to the core component failure or the insufficient electricity supply when the CAES system fails to meet the demand for electricity during peak periods. It might result from the damage of costly CAES components or reduced operation rate, e.g., compressors, and gas turbines.

In addition to the necessary facilities related to the CAES process and system, an emergency response system should be deployed as well to take quick and effective actions in the event of an emergency with the intention to ease the severity of the situation and limit the consequences. Following the aforementioned statement, emergencies may need to be planned, including serious injuries, explosions, and fire. The emergency response is out of the scope of this study, but the emergency response system is considered but simplified as a system consisting of 1) sensors on sites to collect and send the information of the emergency, 2) the controller (e.g., fire Marshal) to make a decision based on the signal information from the sensors and deliver to the actual actuators (e.g., Firefighters), and 3) the actuators to take the actions eventually.

It is concluded that the CAES system is a multi-component system with multiple forms of energy transfers from mechanical, electrical, and thermal engineering [8], and presents intermittent operations in the face of uncertainties from variations of the integrated energy systems [9]. Complexity structure, dynamic demand response, and sustainability concerns accentuate the need for safe and reliable CAES system operations.

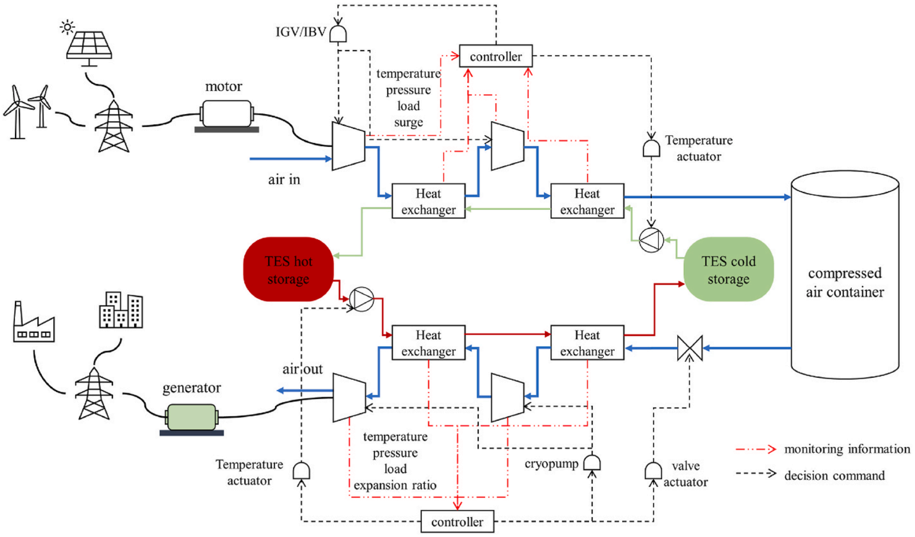

Fig. 2. Main controllers in the CAES system.

3. Methodology of hazard identification for CAES system

As a relatively new safety analysis method, STPA has the advantage of identifying hazards and analyzing risk during the system's initial development process. When it comes to the CAES systems, even though the concept is not new, there is still scarce knowledge regarding the in-service system safety and risk management, which calls for a more systematic method in the hazard identification method. The objective of this study, thus, is to preliminarily apply the STPA method to the CAES system to identify potential hazards and provide clues for practitioners in risk management.

3.1. STPA and its procedure

STPA was developed based on systems theory and system thinking emphasizing the dynamic behavior analysis of the systems in hazard identification [24]. It is a method through the analysis of the interactions among its components and the ways in which those can be unsafe to identify inadequate control and examine the system's safety. The nature of such interactions shall ensure that the system as a whole remains within safety limits [47]. It indicates that any violation of the defined safety constraints may lead to the emergency of a hazard [48].

The main difference between STPA and conventional hazard analysis methods, such as FTA, FMEA, locates that safety is treated as a system's control (constraint) problem in STPA rather than a component failure problem [26]. It is able to reduce the uncertainties in the probabilities calculation of a system transitioning to an unsafe state due to a lack of empirical data, particularly in the initial phases of system development [22,49]. STPA method satisfies the need for complicated modern systems where accidents would occur due to faulty single components and inter-component communication mismatches. More potential causes of accidents, therefore, could be captured, e.g., component failure accidents, unsafe interactions among components, complex human, software behavior, design error, and flawed requirements etc. STPA method has been demonstrated with advantage in situations where there are many 'unknown-unknowns', or difficulties in the prediction of hazardous situations before they happen [23,50]. The STPA procedure generally consists of four steps as described below and depicted in Fig. 3:

Step 1: Establish the system engineering foundation to clarify the analysis scope;
Step 2: Model the control structure showing transmission of control actions and feedbacks;
Step 3: Identify unsafe control actions (UCAs) that could lead to a hazardous state;
Step 4: Determine the occurrence (finding causal factors) of each potentially UCA which is identified in step 3.

3.2. STPA for the CAES system

It is expected to obtain more relevant safety and risk issues of the CAES system by leveraging STPA which is a top-down method and based on the functional control diagram of the system. The hazardous identification of the CAES system follows the general procedure of STPA as stated in Section 3.1.

3.2.1. Define the purpose of analysis

This study aims to investigate the main hazardous scenarios of the CAES system, independent from the electricity network, potentially serving as the foundation for risk management in the future. The first step, thus, is to specify potential system-level accidents (SLAs), system-level hazards (SLHs), and system-level safety constraints (SLSCs).

The main system-level accidents and potential losses have been identified in Section 2.2. Consistency with the aforementioned statements, the first safety concern is related to the fire/chemical explosion due to the mixture of air and flammable fluids. It corresponds to the safety constraint that contents in the CAES system must always flow separately in the designed routes and directions. Also, the pressure in the air container should be always within the design limit to avoid a mechanical explosion which might bring economic loss and/or environmental impact. For the economic loss due to component failure or reduced production, it requires that the component should be protected from extreme working conditions and be kept running during the operation cycle. Table 2 summarizes the major SLAs, SLHs, and SLSCs of the CAES system.

3.2.2. Model of the safety control structure

The next step is to identify the safety control structure of CAES system. The hierarchical control structure is a functional representation of the system that explicitly uses control actions and feedback signals to illustrate the communication between controllers (whether physical, digital or human) and the controlled process (e.g., the normal CAES system operations). The control functions are a function of the process model, control algorithms, and feedback signals that are built into the components and systems. A genetic control structure is depicted in Fig. 4.

The blocks in Fig. 4 represent functional entities in the system. Each control structure could be zoomed in based on the responsibility of control. The control structures help designers to understand the dynamic

Table 2
System-level accidents, hazards, and safety constraints of the CAES system.

System-level accident	System-level hazard	System-level safety constraint
SLA1: People injuries, economic loss and/or asset damage due to the chemical explosion or fires	SLH1: Air leaks into flammable organic fluids (or vice versa) used for thermal storage (A-CAES).	SLSC1: Contents in CAES must always flow in designed routes and directions
SLA2: Economic loss and/or environmental impact resulting from the container (e.g., cavern) failure	SLH2: Storage pressure is excessively high or low	SLSC2: Pressure must never be beyond the design limit
SLA3: Valuable CAES components are damaged	SLH3: Equipment operates outside normal operation conditions	SLSC3: Main components in CAES must be protected from extreme operating conditions
SLA4: The charging/discharging process is reduced or interrupted unnecessarily	SLH4: CAES system stops compressing or releasing when not necessary	SLSC4: CAES should respond properly to the needs

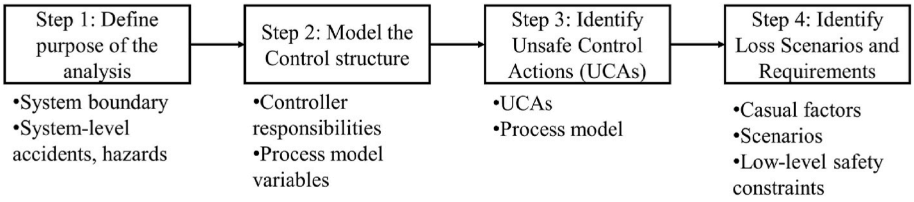
Step 1: Define purpose of the analysis
Step 2: Model the Control structure
Step 3: Identify Unsafe Control Actions (UCAs)
Step 4: Identify Loss Scenarios and Requirements
•System boundary
•System-level accidents, hazards
•Controller responsibilities
•Process model variables
•UCAs
•Process model
•Casual factors
•Scenarios
•Low-level safety constraints

Fig. 3. A typical STPA procedure.

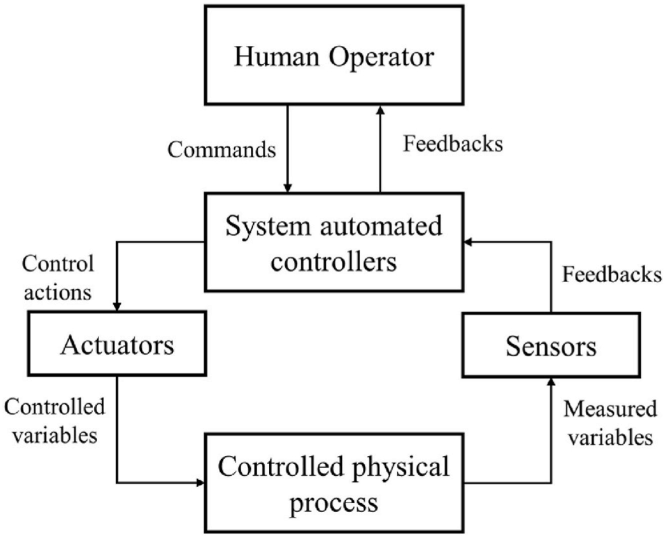

Fig. 4. A genetic control structure.

controller interactions associated with the shifting of operational modes, thus supporting the following steps.

In the context of CAES system, the control structures can be roughly categorized into three controllers: the human operator, system controllers, and the inspection and maintenance (I&M) intervention controller. The I&M controller here refers to the technicians independent of the operator following the scheduled programs to conduct interventions to maintain the system integrity. The role of the human operator is to manage the whole CAES automation, and directly or indirectly control the operation to respond to the needs of other integrated systems, referring to the startup of the charging or discharging process. The related safety responsibilities are to supervise the charging/discharging process running safely and efficiently to meet the needs. The system automated controllers following these predetermined programs to regulate pressure, temperature, surge etc., must contain a model to control the process/components in CAES system. Safety responsibilities of system controllers include, but are not limited to, maintaining the charging/discharging process in a safe state, providing system information to the human operator, etc. Moreover, safety responsibilities could be assigned to each control structure entity upon the refinement of the SLSCs. The process is to seek answers regarding what does each entity need to do so that together the SLSCs will be enforced. For example, in the charging process, to ensure smooth storage of air, the air pressure at the outlet of the compressor should be always greater than the pressure of the air in the storage container. The process model for the pressure controller includes the high/low/within the design of the outlet and inlet pressure for each compressor, the difference (normal/abnormal) between the outlet pressure and the inlet of the storage container, and the pressure state in the container (high/low/within in the design limits). The control structure is that the system automated controller sends the command of speed up/down of the compressor to the actuator based on the monitored pressure information, see depicted in Fig. 5.

The main safety responsibilities and process models in the charging and discharging processes are summarized in Figs. 6 and 7, respectively. Note that the safety responsibilities and process models are non-exhaustive, which can be extended based on the specific CAES system configuration and expert knowledge.

3.2.3. Identify unsafe control actions

Each control action identified in the safety control structure has the potential to generate a hazardous system state [25]. Specifically, there are four ways that an unsafe control action (UCA) may occur [25]: 1) the control action required for safety is not provided or is not followed; 2) the control action is being provided when not needed; 3) the potentially safe control action is provided too late, too early, or out of sequence; and 4) the safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action). It implies that a control action should be provided appropriately at the correct time with the correct duration. The enumeration of each UCA is a lengthy process but useful in identifying the context and the triggers that could lead to the hazards described above in Step 1. Taking the control action 'supply cooling fluid to heat exchanger', identified as CA-6 in Table 3, as an example, it could be UCA, in three possible ways, if the cooling fluid is not provided, supplied too late, or stopped too soon (interrupted) when the flow of hot gas is started in the exchanger, as it may lead to the thermal failure of tubes [51], which is related to the identified SLH1 and SLH3 in Table 2. Temperature-actuated modulating control valves thus should be used to regulate cooling liquid flow from the design perspective.

Following the procedure, the main UCAs involved in the charging and discharging process can be identified. UCAs could be referenced with typical failure mechanisms and control patterns of components and systems installed and operated in a similar working condition to the CAES system to solute the challenge of scarce practical information. Even though the existence of uncertainty and difference, the UCAs identification could provide a preliminary study for practitioners, which could be expanded upon the expert knowledge of the CAES system thereafter.

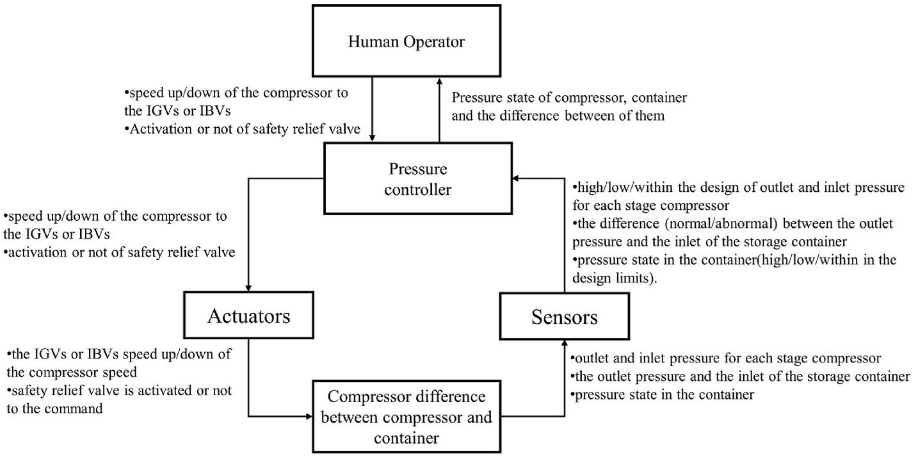
Human Operator
•speed up/down of the compressor to the IGVs or IBVs
•Activation or not of safety relief valve
Pressure state of compressor, container and the difference between of them
Pressure controller
•speed up/down of the compressor to the IGVs or IBVs
•activation or not of safety relief valve
•high/low/within the design of outlet and inlet pressure for each stage compressor
•the difference (normal/abnormal) between the outlet pressure and the inlet of the storage container
•pressure state in the container(high/low/within in the design limits).
Actuators
Sensors
•the IGVs or IBVs speed up/down of the compressor speed
•safety relief valve is activated or not to the command
Compressor difference between compressor and container
•outlet and inlet pressure for each stage compressor
•the outlet pressure and the inlet of the storage container
•pressure state in the container

Fig. 5. Safe control structure of the pressure between compressor and container.

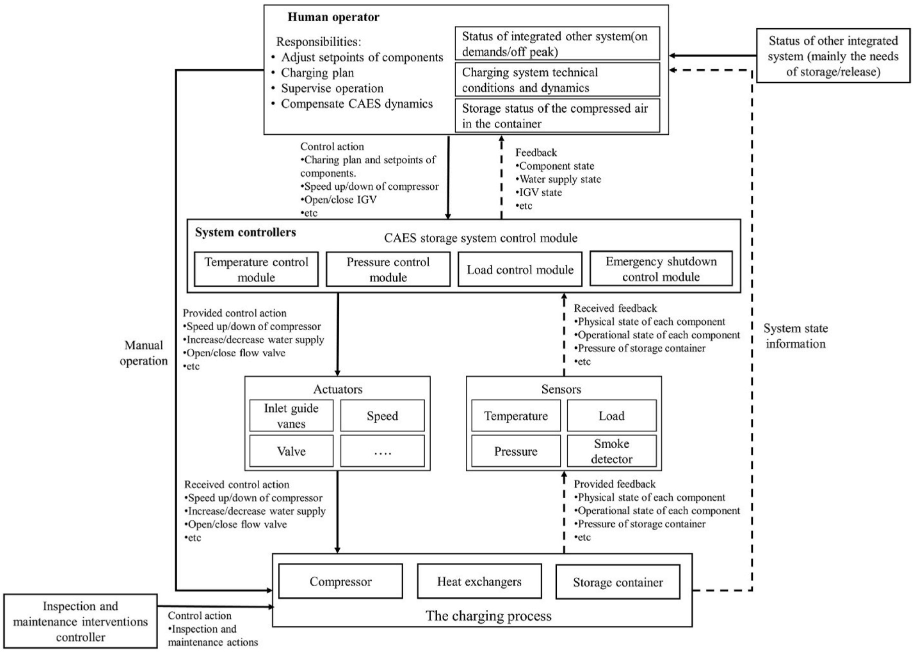
Human operator
Responsibilities:
• Adjust setpoints of components
• Charging plan
• Supervise operation
• Compensate CAES dynamics
Status of integrated other system(on demands/off peak)
Charging system technical conditions and dynamics
Storage status of the compressed air in the container
Status of other integrated system (mainly the needs of storage/release)
Control action
•Charing plan and setpoints of components.
•Speed up/down of compressor
•Open/close IGV
•etc
Feedback
•Component state
•Water supply state
•IGV state
•etc
System controllers
CAES storage system control module
Temperature control module
Pressure control module
Load control module
Emergency shutdown control module
Manual operation
Provided control action
•Speed up/down of compressor
•Increase/decrease water supply
•Open/close flow valve
•etc
Received feedback
•Physical state of each component
•Operational state of each component
•Pressure of storage container
•etc
System state information
Actuators
Inlet guide vanes
Speed
Valve
….
Sensors
Temperature
Load
Pressure
Smoke detector
Received control action
•Speed up/down of compressor
•Increase/decrease water supply
•Open/close flow valve
•etc
Provided feedback
•Physical state of each component
•Operational state of each component
•Pressure of storage container
•etc
Compressor
Heat exchangers
Storage container
The charging process
Inspection and maintenance interventions controller
Control action
•Inspection and maintenance actions

Fig. 6. The schematic hierarchical control structure diagram of the charging process.

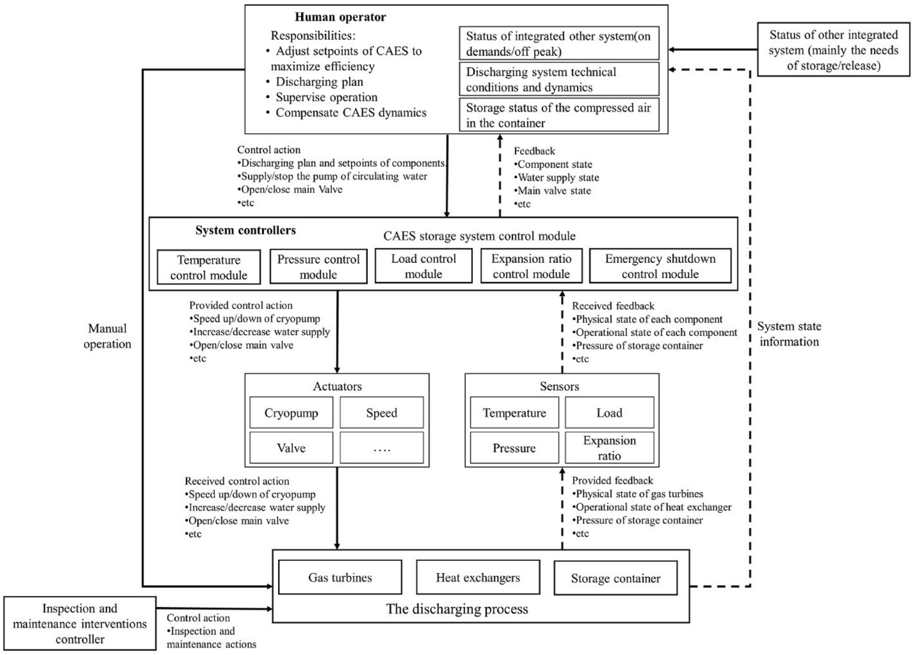
Human operator
Responsibilities:
• Adjust setpoints of CAES to maximize efficiency
• Discharging plan
• Supervise operation
• Compensate CAES dynamics
Status of integrated other system(on demands/off peak)
Discharging system technical conditions and dynamics
Storage status of the compressed air in the container
Status of other integrated system (mainly the needs of storage/release)
Control action
•Discharging plan and setpoints of components.
•Supply/stop the pump of circulating water
•Open/close main Valve
•etc
Feedback
•Component state
•Water supply state
•Main valve state
•etc
System controllers
CAES storage system control module
Temperature control module
Pressure control module
Load control module
Expansion ratio control module
Emergency shutdown control module
Manual operation
Provided control action
•Speed up/down of cryopump
•Increase/decrease water supply
•Open/close main valve
•etc
Received feedback
•Physical state of each component
•Operational state of each component
•Pressure of storage container
•etc
System state information
Actuators
Cryopump
Speed
Valve
….
Sensors
Temperature
Load
Pressure
Expansion ratio
Received control action
•Speed up/down of cryopump
•Increase/decrease water supply
•Open/close main valve
•etc
Provided feedback
•Physical state of gas turbines
•Operational state of heat exchanger
•Pressure of storage container
•etc
Gas turbines
Heat exchangers
Storage container
The discharging process
Inspection and maintenance interventions controller
Control action
•Inspection and maintenance actions

Fig. 7. The schematic hierarchical control structure diagram of the discharging process.

3.2.4. Identify loss scenarios

Following UCA identifications, this step identifies scenarios and causal factors for each UCA for figuring out the related low-level safety constraints. There are several possible loss scenarios and casual factors for each UCA. For a specific UCA, the relevant job is to brainstorm how different parts in the control loop can be responsible for the UCA, mainly seeking the answers from three aspects: 1) in what scenarios does an unsafe controller behavior lead to the UCA; 2) in what scenarios do faulty beliefs about the system lead to the identified UCA, and 3) what if the process model and the control algorithm were accurate but process equipment itself was at fault? To visualize the whole structure, a brief case related to the temperature of the compressor is elaborated on here to explain the identification process of the loss scenarios.

> Case: **CA-4-1**: Compressor temperature cannot be regulated when the compressor is overheating [SLH3, SLH4]

Fig. 8 shows the control loop for CA-4-1. As physical controllers, the CA-4-1 may occur due to a failure related to the temperature controller.

Scenario 1 for CA-4-1: The compressor temperature controller fails when the temperature is overheating, causing the regulation action to not be provided [CA-4-1]. As a result, the duration of the overheating in compressors might cause compressor damage or failure in the charging process [SLH3, SLH4].

Table 3
Identifying UCAs in the CAES system (part of).

No	Control action (CA)	Unsafe control action				
		CA not provided causes hazard	CA provided when not required causes hazard	CA provided too early causes hazard	CA provided too late causes hazard	CA stopped too soon or applied too long
CA-4	Regulate compressor temperature when the compressor is overheating	[CA-4-1] Compressor temperature cannot be regulated when the compressor is overheating [SLH3, SLH4]	N/A	N/A	N/A	N/A
CA-5	Integrity check of heat exchangers	[CA-5-1] Regular inspections on the heat exchanger are missing [SLH1, SLH3]	N/A	N/A	N/A	N/A
CA-6	Supply cooling fluid in heat exchangers	[CA-6-1] Cooling fluid is not provided when the hot gas flow is delivered [SLH1, SLH3, SLH4]	N/A	N/A	[CA-6-2] Cooling fluid is provided too late after the delivery of hot gas flow [SLH1, SLH3, SLH4]	[CA-6-3] Cooling fluid supplying stops too soon (interruption) during the delivery of hot gas flow [SLH1, SLH3, SLH4]
CA-7	Leak testing of heat exchangers tubes	[CA-7-1] Leak testing of heat exchanger tubes are missing and precaution for leak protection is not taken [SLH3, SLH4]	N/A	N/A	N/A	N/A
CA-8	Regulate inlet flow rate or pressure of the steam of heat exchangers	[CA-8-1] Flow rate or pressure is not regulated when it is out of limits [SLH3, SLH4]	N/A	N/A	[CA-8-2] Flow rate or pressure is regulated too late when it is out of limits [SLH3, SLH4]	N/A

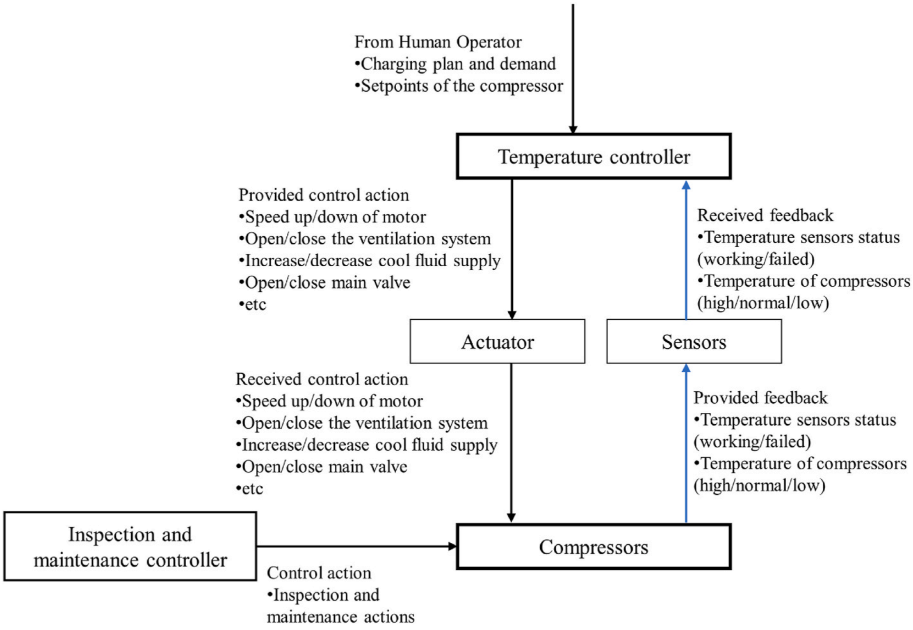
From Human Operator
•Charging plan and demand
•Setpoints of the compressor
Temperature controller
Provided control action
•Speed up/down of motor
•Open/close the ventilation system
•Increase/decrease cool fluid supply
•Open/close main valve
•etc
Received feedback
•Temperature sensors status (working/failed)
•Temperature of compressors (high/normal/low)
Actuator
Sensors
Received control action
•Speed up/down of motor
•Open/close the ventilation system
•Increase/decrease cool fluid supply
•Open/close main valve
•etc
Provided feedback
•Temperature sensors status (working/failed)
•Temperature of compressors (high/normal/low)
Inspection and maintenance controller
Compressors
Control action
•Inspection and maintenance actions

Fig. 8. Control loop of the CA-4-1.

Secondly, the temperature in the regulator may not match the real status of the compressor. But the control actions are determined based on the controller's internal beliefs, leading to the occurrence of process model flaws.

Scenario 2 for CA-4-1: The compressor is overheating. The temperature controller does not provide the regulation action [CA-4-1] because the controller incorrectly believes the temperature is within the normal limits. This flawed process will occur if the regulation indication of temperature is not received upon regulation. The temperature regulation indication may not be received when needed if some abnormal situations occur, e.g., failure of the temperature sensor, temperature feedback is delayed, etc. As a result, insufficient temperature regulation is provided upon the overheating in compressors [SLH3, SLH4].

Thirdly, the improper or no execution of control actions might cause UCAs as well, which may be caused by actuator failure, actuator errors or misbehaviors, loss of power to the actuator, etc. In CA-4-1, there are two identified actuators, the thermal relief valve, and the ventilation system. The relevant loss scenarios could be identified as follows:

Scenario 3 for CA-4-1: The temperature controller sends the regulation command when the compressor is overheating, but the regulation is not applied due to the thermal valve failure, slow response, or a wiring error. As a result, insufficient temperature regulation is provided upon the overheating in compressors [SLH3, SLH4].

Scenario 4 for CA-4-1: The temperature controller sends the regulation command when the compressor is overheating, but the regulation is not applied due to the ventilation system failure or slow response. As a result, insufficient temperature regulation is provided upon the overheating in compressors [SLH3, SLH4].

For the inspection and maintenance controller, system engineers will act as the actuator following the specific operational procedures or manuals from the manufacturers. Referring to the previous studies, the main part of components related to temperature include the oil and lubrication, inlet air filter, and other routine maintenance. Insufficient maintenance actions may contribute to loss scenarios.

Scenario 5 for CA-4-1: The temperature controller sends the regulation command, and the regulation is applied, but the compressor temperature does not decelerate due to the poor compressor condition, e.g., clogged inlet air filter, the lack of oil and lubrication, etc. As a result, insufficient temperature regulation is provided upon the overheating in compressors [SLH3, SLH4].

After the identification of these loss scenarios of CA-4-1, the relevant possible causal factors and low-level safety requirements appear, as depicted in Table 4.

The whole procedure helps analysts understand the interactions inside the compressor and the connections with external elements. Similarly, other UCAs can be analyzed from the aforementioned three aspects with their specific possible causal factors, low-level safety constraints become visible consequently.

4. Results and discussions

Since these potential risks are accompanied by severe consequences once they occur, CAES plants should be built to a specific level of safety. More attention should be paid to how to design and manage the CAES system in their life cycles with the intention to control the risk and maintain the specific safety level. Driven by the situation of scarce reported knowledge of risk and safety issues. STPA thus has been applied to identify possible loss scenarios and their causal factors that would provide valuable information for risk management to avoid such loss scenarios.

4.1. Findings in hazard identification

The CAES system with the involvement of multi-components attempts to complete the charging and discharging process to respond to the dynamic demand for electricity. It requires these components to cooperate and work in their optimal conditions to avoid the occurrence of failures and accidents. There are 19 CAs with 33 potential UCAs identified in this study.

Table 4
Loss scenarios identification of CA-4-1.

No	UCA	Possible causal factors	Low-level safety constraint
[CA-4-1]	Compressor temperature cannot be regulated as desired [SLH3, SLH4]	[CA-4-1-CF-1] Compressor temperature regulator is malfunction [CA-4-1-CF-2] The temperature information is wrong (sensors malfunction) [CA-4-1-CF-3] The thermal relief valve is dysfunctional [CA-4-1-CF-4] Inadequate ventilation leads to the overheating of the compressor [CA-4-1-CF-5] Oil and lubrication are too less [CA-4-1-CF-6] The compressor does not undergo regular maintenance [CA-4-1-CF-7] Clogged oil cooler and inlet air filter	[CA-4-1-SC-1] Provide reliable logic controller [CA-4-1-SC-2] Sensors should be selected meeting the specific requirements [CA-4-1-SC-3] Sensors should be tested and verified following the procedure [CA-4-1-SC-4] The thermal valve should be tested and maintained regularly; a spare thermal valve is recommended to be installed [CA-4-1-SC-5] The compressor should be sufficiently ventilated [CA-4-1-SC-6] The oil level and filters should be monitored and maintained regularly [CA-4-1-SC-7] The compressor parts should be routinely maintained and kept up to date

Among these identified 33 UCAs, some UCA may lead to more than one SLH. There are 7 UCAs related to the SLH1, mainly with the heat exchanger and ESS. While the SLH2-relevant UCAs locate on the inlet and outlet valves of the air container. Most of the control actions we considered here are to prevent component damage and/or operate in optimal conditions resulting in more identified UCAs related to SLH3 and SLH4. However, there is no strict distinction between UCAs leading to SLH3 and SLH4 since, to some extent, it is challenging to prioritize the SLH for a specific UCA, which relies more on expert knowledge and real historical data.

The low-level safety constraints identified in Section 3.2.4 specify the contributors to successfully completing the charging and discharging process. The application of STPA visualizes a wide range of accident causes or conditions in the CAES system, founding the preparation for the prevention of these accidents. In the early stage of the specific CAES project, inherent safety measures addressing the design features of the components should be given priority. The selection and design of main components should depend on the size of the CAES system and comply with relevant rules and regulations and international standards, e.g., ISO 19859 for gas turbines [52]. For example, the operational characteristics of the gas turbines in formulating a CAES system directly impact the overall energy conversion efficiency and the rated power generation during the discharging period [3]. It implies that main parameters, such as pressure, temperature, speed, etc., are the main considerations when selecting the optimum gas turbines. In addition, numerous other characteristics should be considered as well, e.g., corrosion resistance, friction, abrasion, and wear for mechanical items. For SLA1, *People injuries, economic loss, and/or asset damage due to the chemical explosion or fires*, three necessary elements in the fire triangle might be existing simultaneously. For example, CA-7-1, *Leak testing of heat exchanger tubes are missing and precaution for leak protection is not taken*, identifies the main causal factors in the operational phase related to the leakage testing of heat exchanger tubes. But it is insufficient since the design phase is not involved. Regarding SLA1, theoretically, there might be two ways in improving the CAES system in the design phase based on the identified hazards: the first is to remove one of the elements in the fire triangle, e.g., substituting water for the flammable diathermic oil as a heat medium, while the second recommendation to prevent SLA1 could be to adopt more reliable materials with heat, and corrosion resistance in the main components to prevent the mixture of the element in the fire triangle, e.g., heat exchangers and compressors. Redundant structures might be adopted for the inlet and outlet valves of the air container thanks to their roles in contributing to SLA 2, as described in Section 4.1. However, these recommended risk measures assume the top priority of system safety. In reality, it has to be admitted, that the CAES system design, besides safety, should balance several factors from compatibility, economic, and efficiency perspectives.

The safety of the CAES system should move one more step in advance than the wide application to avoid abnormal situations. The preliminary identified UCAs in the CAES system can be utilized for formulating recommendations for the risk control measures, referring to the existing measures and practices from resembling systems. Taking the loss scenarios for CA-4-1 as an example, the temperature controller (Scenario 1) might be in a failed state when it is required, then the recommendations regarding performance requirements and management might refer to some general international standards, e.g., IEC 61508 [53], then to be validated and updated with the industrial experience as input. As for the sensor issues, on one hand, as the low-level safety requirement says the sensor should be selected to meet the specific working condition, and be validated and tested following the procedures; on the other hand, installing redundant sensor channels should also be considered as a potential improvement to mitigate the loss Scenario 2 for CA-4-1. Besides these technological measures, the human factors should be considered as well. Even though the CAES system is developing towards more intelligent and software-intensive with E/E/PE technologies, humans still and will be involved in all life phases of the CAES system, from design through construction, operation, maintenance, etc., to disposal. The high frequent appearance of operator-related identified scenarios shreds of evidence the importance. Human operators and practitioners should identify safety-critical tasks and follow the specific procedures to carry out activities to ensure components in the CAES system remain reliable, safe, and efficient, maximize the lifetime of systems and reduce the risk of failure. Skill training activities are also essential for reducing the uncertainty for operators in routine working and responding to incidents in the CAES system. More details related to the human reliability analysis in the risk assessment could be found in Ref. [21].

4.2. Biases and limitations

The procedure of UCAs' identification helps analysts and practitioners to understand the interactions among each component and the external elements. The identified results are inexhaustive and dependent on the different analysis levels. Detailly, in this study, the component-level refers to the unit such as compressors, and gas turbines, which can be furtherly decomposed either from the structural or functional perspective into a lower level, e.g., rotors, blades, etc. Further hazard identification should rely on the expert knowledge or prior studies transferred from these same facilities in similar working conditions.

The first limitation of this study is that a generalized structure of the CAES system is considered here. The discussion mainly focuses on the main component and some typical controls, e.g., temperature, pressure, etc., while, the diversity of components is excluded in the CAES system [32]. The proposed STPA in this study needs to be updated in two ways. First, the safety control structure should be dug and up to date based on a deeper decomposition of each component. Second, the operational data could benefit in helping the STPA adapt to the dynamic reality through the validation of the original assumptions in the original analysis.

Second, the CAES system is still in the early stage with scarce information available related to the operational stage. The STPA, ideally, could enhance risk management of the CAES system starting from the Concept of Operation stage, whose hazard analysis could be delivered to the operator as part of the service. However, some hazard identification results in this study are referred from similar devices with different working conditions, which inevitably bring uncertainties. Transfer learning of prior knowledge is helpful in the early phase, but real operational data and expert knowledge are needed to validate and correct this knowledge.

Finally, more clustering studies and analyses should be conducted. The CAES system is studied separately while the other integrated system is considered as a demand in this study. When the other system is integrated with, e.g., the renewable energy source network and the electricity grid, additional sources of variations and disturbances during operation might be introduced as well, for example, the connection hazards.

Despite some of the limitations encountered, this study has pioneered a general picture of the hazard identification of the CAES system based on the STPA, specifying the corresponding safety requirements and evaluation criteria. These findings provide clues for the risk assessment of the CAES system later.

5. Concluding remarks

The CAES system integrated with renewable energy sources has a bright future in the energy market to boost the decarbonization of power sector. How to realize the reliable and safe operation of the CAES system raises challenges due to its complex structure, dynamic demand response, and sustainability concerns, which have been barely considered and mentioned in the open literature. This work conducts major hazard identifications of the CAES system using the STPA framework, and the identified UCAs provide useful insights on its design and operational practice toward a safe and sustainable energy supply.

The application of STPA on the CAES system focus on preliminarily developing a high-level control structure, but with the capability to evolve with the practitioners' experience and knowledge. The STPA method shows its ability in identifying inadequate control and suggest additional control actions qualitatively but fails to quantify how sufficient a control action is. In future work, a comprehensive model will be developed to involve the digital systems, deeper decomposition of the components, and controllers to capture more detailed UCAs. Also, quantitative analysis on a certain UCA will be conducted to specify the tolerable risk, guiding the resource allocation for risk control.

CRediT authorship contribution statement

Aibo Zhang: Conceptualization, Methodology, Writing - original draft. **Zhaoyuan Yin:** Methodology, Investigation, Writing - original draft. **Zhiying Wu:** Validation, Visualization. **Min Xie:** Funding acquisition, Supervision, Writing - review & editing. **Yiliu Liu:** Methodology, Supervision, Writing - review & editing. **Haoshui Yu:** Conceptualization, Methodology, Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgements

This work is supported by National Natural Science Foundation of China (71971181 and 72032005) and by Research Grant Council of Hong Kong (11203519, 11200621). It is also funded by Hong Kong Innovation and Technology Commission (InnoHK Project CIMDA).

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.renene.2023.02.098.

References

[1] A.H. Alami, K. Aokal, J. Abed, M. Alhemyari, Low pressure, modular compressed air energy storage (CAES) system for wind energy storage applications, Renew. Energy 106 (2017) 201–211, https://doi.org/10.1016/J.RENENE.2017.01.002.

[2] H. Yu, S. Engelkemier, E. Gençer, Process improvements and multi-objective optimization of compressed air energy storage (CAES) system, J. Clean. Prod. 335 (2022), 130081.

[3] M.S. Guney, Y. Tepe, Classification and assessment of energy storage systems, Renew. Sustain. Energy Rev. 75 (2017) 1187–1197, https://doi.org/10.1016/J.RSER.2016.11.102.

[4] A.G. Olabi, C. Onumaegbu, T. Wilberforce, M. Ramadan, M.A. Abdelkareem, A. H. Al – Alami, Critical review of energy storage systems, Energy 214 (2021), 118987, https://doi.org/10.1016/J.ENERGY.2020.118987.

[5] Z. Zhang, T. Ding, Q. Zhou, Y. Sun, M. Qu, Z. Zeng, Y. Ju, L. Li, K. Wang, F. Chi, A review of technologies and applications on versatile energy storage systems, Renew. Sustain. Energy Rev. 148 (2021), 111263, https://doi.org/10.1016/J.RSER.2021.111263.

[6] H. Mozayeni, X. Wang, M. Negnevitsky, Dynamic analysis of a low-temperature adiabatic compressed air energy storage system, J. Clean. Prod. 276 (2020), 124323, https://doi.org/10.1016/J.JCLEPRO.2020.124323.

[7] M. Budt, D. Wolf, R. Span, J. Yan, A review on compressed air energy storage: basic principles, past milestones and recent developments, Appl. Energy 170 (2016) 250–268, https://doi.org/10.1016/J.APENERGY.2016.02.108.

[8] Y.-M. Kim, J.-H. Lee, S.-J. Kim, D. Favrat, Potential and evolution of compressed air energy storage: energy and exergy analyses, Entropy 14 (2012), https://doi.org/10.3390/e14081501.

[9] H. Ibrahim, A. Ilinca, J. Perron, Energy storage systems—characteristics and comparisons, Renew. Sustain. Energy Rev. 12 (2008) 1221–1250, https://doi.org/10.1016/J.RSER.2007.01.023.

[10] APEX, Bethel Energy Center. http://www.apexcaes.com/bethel-energy-center, 2019.

[11] Y. Wu, T. Zhang, Risk assessment of offshore wave-wind-solar-compressed air energy storage power plant through fuzzy comprehensive evaluation model, Energy 223 (2021), 120057, https://doi.org/10.1016/J.ENERGY.2021.120057.

[12] D. Rosewater, A. Williams, Analyzing system safety in lithium-ion grid energy storage, J. Power Sources 300 (2015) 460–471, https://doi.org/10.1016/J.JPOWSOUR.2015.09.068.

[13] J. Conzen, S. Lakshmipathy, A. Kapahi, S. Kraft, M. DiDomizio, Lithium ion battery energy storage systems (BESS) hazards, J. Loss Prev. Process. Ind. 81 (2023), 104932, https://doi.org/10.1016/J.JLP.2022.104932.

[14] M. Qi, Y. Liu, R.S. Landon, Y. Liu, I. Moon, Assessing and mitigating potential hazards of emerging grid-scale electrical energy storage systems, Process Saf. Environ. Protect. 149 (2021) 994–1016.

[15] A.K. Singh, R.S. Kumar, A. Pusti, Consequence analysis of most hazardous initiating event in electrical energy storage systems using event tree analysis, J. Fail. Anal. Prev. 22 (2022) 1646–1656, https://doi.org/10.1007/s11668-022-01464-z.

[16] P.W. Cooper, M.C. Grubelich, S.J. Bauer, Potential Hazards of Compressed Air Energy Storage in Depleted Natural Gas Reservoirs, United States, 2011, https://doi.org/10.2172/1029814.

[17] ESA, ESA Corporate Responsibility Initiative: U.S, Energy Storage Operational Safety Guidelines, 2019.

[18] A. Arabkoohsar, M. Dremark-Larsen, R. Lorentzen, G.B. Andresen, Subcooled compressed air energy storage system for coproduction of heat, cooling and electricity, Appl. Energy 205 (2017) 602–614, https://doi.org/10.1016/J.APENERGY.2017.08.006.

[19] A. Arabkoohsar, L. Machado, R.N.N. Koury, Operation analysis of a photovoltaic plant integrated with a compressed air energy storage system and a city gate station, Energy 98 (2016) 78–91, https://doi.org/10.1016/J.ENERGY.2016.01.023.

[20] A. Arabkoohsar, Mechanical Energy Storage Technologies, Academic Press, 2020.

[21] M. Rausand, Risk Assessment: Theory, Methods, and Applications, John Wiley & Sons, 2013.

[22] N.G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, The MIT Press, 2016.

[23] X. Yang, I.B. Utne, S.S. Sandøy, M.A. Ramos, B. Rokseth, A systems-theoretic approach to hazard identification of marine systems with dynamic autonomy, Ocean Eng. 217 (2020), 107930, https://doi.org/10.1016/J.OCEANENG.2020.107930.

[24] N. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, The MIT Press, 2012.

[25] N. Leveson, J. Thomas, STPA Handbook, 2018.

[26] S.M. Sulaman, A. Beer, M. Felderer, M. Höst, Comparison of the FMEA and STPA safety analysis methods–a case study, Software Qual. J. 27 (2019) 349–387, https://doi.org/10.1007/s11219-017-9396-0.

[27] C. Bensaci, Y. Zennir, D. Pomorski, A Comparative Study of STPA Hierarchical Structures in Risk Analysis: the Case of a Complex Multi-Robot Mobile System, Eur. Conf. Electr. Eng. Comput. Sci, IEEE, 2018, pp. 400–405.

[28] S. Sultana, P. Okoh, S. Haugen, J.E. Vinnem, Hazard analysis: application of STPA to ship-to-ship transfer of LNG, J. Loss Prev. Process. Ind. 60 (2019) 241–252, https://doi.org/10.1016/J.JLP.2019.04.005.

[29] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, S. Sezer, STPA-SafeSec: safety and security analysis for cyber-physical systems, J. Inf. Secur. Appl. 34 (2017) 183–196, https://doi.org/10.1016/J.JISA.2016.05.008.

[30] D. Dghaym, T.S. Hoang, S.R. Turnock, M. Butler, J. Downes, B. Pritchard, An STPA-based formal composition framework for trustworthy autonomous maritime systems, Saf. Sci. 136 (2021), 105139, https://doi.org/10.1016/J.SSCI.2020.105139.

[31] A. Arabkoohsar, Chapter Three - compressed air energy storage system, in: A. Arabkoohsar (Ed.), Mech. Energy Storage Technol., Academic Press, 2021, pp. 45–71, https://doi.org/10.1016/B978-0-12-820023-0.00003-1.

[32] A.G. Olabi, T. Wilberforce, M. Ramadan, M.A. Abdelkareem, A.H. Alami, Compressed air energy storage systems: components and operating parameters – a review, J. Energy Storage 34 (2021), 102000.

[33] M. Arbabzadeh, J.X. Johnson, G.A. Keoleian, P.G. Rasmussen, L.T. Thompson, Twelve principles for green energy storage in grid applications, Environ. Sci. Technol. 50 (2016) 1046–1055, https://doi.org/10.1021/acs.est.5b03867.

[34] E. Yao, H. Wang, L. Wang, G. Xi, F. Maréchal, Multi-objective optimization and exergoeconomic analysis of a combined cooling, heating and power based compressed air energy storage system, Energy Convers. Manag. 138 (2017) 199–209, https://doi.org/10.1016/J.ENCONMAN.2017.01.071.

[35] W. He, J. Wang, Optimal selection of air expansion machine in Compressed Air Energy Storage: a review, Renew. Sustain. Energy Rev. 87 (2018) 77–95.

[36] S. Mucci, A. Bischi, S. Briola, A. Baccioli, Small-scale adiabatic compressed air energy storage: control strategy analysis via dynamic modelling, Energy Convers. Manag. 243 (2021), 114358.

[37] G. Venkataramani, V. Ramalingam, K. Viswanathan, Harnessing free energy from nature for efficient operation of compressed air energy storage system and unlocking the potential of renewable power generation, Sci. Rep. 8 (2018) 9981, https://doi.org/10.1038/s41598-018-28025-5.

[38] Q. Zhou, D. Du, C. Lu, Q. He, W. Liu, A review of thermal energy storage in compressed air energy storage system, Energy 188 (2019), 115993, https://doi.org/10.1016/J.ENERGY.2019.115993.

[39] C. Guo, Y. Xu, X. Zhang, H. Guo, X. Zhou, C. Liu, W. Qin, W. Li, B. Dou, H. Chen, Performance analysis of compressed air energy storage systems considering dynamic characteristics of compressed air storage, Energy 135 (2017) 876–888, https://doi.org/10.1016/J.ENERGY.2017.06.145.

[40] I. Arsie, V. Marano, M. Moran, G. Rizzo, G. Savino, Optimal management of a wind/CAES power plant by means of neural network wind speed forecast, in: Eur. Wind Energy Conf. Exhib. Eur. Wind Energy Assoc. (EWEA), 2007. Milan, May.

[41] H. Guo, Y. Xu, Y. Zhang, C. Guo, J. Sun, X. Zhang, W. Li, H. Chen, Off-design performance and operation strategy of expansion process in compressed air energy systems, Int. J. Energy Res. 43 (2019) 475–490, https://doi.org/10.1002/er.4284.

[42] H. Guo, Y. Xu, X. Zhang, Q. Liang, S. Wang, H. Chen, Dynamic characteristics and control of supercritical compressed air energy storage systems, Appl. Energy 283 (2021), 116294.

[43] M. Rausand, Reliability of Safety-Critical Systems: Theory and Applications, John Wiley & Sons, 2014.

[44] Q. Xu, Y. Wu, W. Zheng, Y. Gong, S. Dubljevic, Modelling and Dynamic Safety Control of Compressed Air Energy Storage System, Available SSRN 4037429. (n. d.).

[45] C. Yang, W. Jing, J.J.K. Daemen, G. Zhang, C. Du, Analysis of major risks associated with hydrocarbon storage caverns in bedded salt rock, Reliab. Eng. Syst. Saf. 113 (2013) 94–111.

[46] N. Zhang, L. Ma, M. Wang, Q. Zhang, J. Li, P. Fan, Comprehensive risk evaluation of underground energy storage caverns in bedded rock salt, J. Loss Prev. Process. Ind. 45 (2017) 264–276.

[47] K. Kazaras, T. Kontogiannis, K. Kirytopoulos, Proactive assessment of breaches of safety constraints and causal organizational breakdowns in complex systems: a joint STAMP-VSM framework for safety assessment, Saf. Sci. 62 (2014), https://doi.org/10.1016/j.ssci.2013.08.013.

[48] K. Wróbel, J. Montewka, P. Kujala, Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels, Reliab. Eng. Syst. Saf. 178 (2018), https://doi.org/10.1016/j.ress.2018.05.019.

[49] T. Bjerga, T. Aven, E. Zio, Uncertainty treatment in risk analysis of complex systems: the cases of STAMP and FRAM, Reliab. Eng. Syst. Saf. 156 (2016), https://doi.org/10.1016/j.ress.2016.08.004.

[50] H. Kim, O.I. Haugen, B. Rokseth, M.A. Lundteigen, Comparison of hazardous scenarios for different ship autonomy types using systems-theoretic process analysis, in: Proc. 29th Eur. Saf. Reliab. Conf. (ESREL). 22–26 Sept. 2019, Hann. Ger., 2019.

[51] M. Ali, A. Ul-Hamid, L.M. Alhems, A. Saeed, Review of common failures in heat exchangers – Part I: mechanical and elevated temperature failures, Eng. Fail. Anal. 109 (2020), 104396.

[52] ISO 19859, Gas Turbine Applications — Requirements for Power Generation, 2016.

[53] IEC 61508, Functional Safety of Electrical/electronic/programmable Electronic Safety-Related Systems, 2010.