

DISASTER RECOVERY METHOD AND SYSTEM BASED ON REDUNDANT ARCHITECTURE

5 TECHNICAL FIELD

[0001] The present disclosure relates to the technical field of off-site disaster recovery, particularly to a disaster recovery method and system based on a redundant architecture.

BACKGROUND

10 [0002] In the field with stringent safety and reliability requirements, such as rail transit and nuclear power, failures in core service systems can lead to severe operational disruptions or even safety incidents. Therefore, the core service systems must be safeguard through disaster recovery and redundancy mechanisms.

[0003] Existing disaster recovery solutions predominantly employ single-point redundancy
15 or local backup approaches, which can provide basic system protection, but generally lacks unified management and coordinated control across multiple systems. In this way, it is difficult to achieve real-time synchronization of communication states and highly reliable failover, thereby failing to fully meet the stringent requirements for security, continuity, and redundancy protection in such systems.

20

SUMMARY

[0004] The present disclosure provides a disaster recovery method and system based on a redundant architecture, which can ensure service continuity and highly reliable switching when system failures or local disasters occur.

25 [0005] In a first aspect, some embodiments of the present disclosure provide a disaster recovery system based on a redundant architecture, and the disaster recovery system includes a third-party arbitration platform and a plurality of security subsystems. The third-party arbitration platform and the plurality of security subsystems are deployed at different geographic locations. Every two of the third-party arbitration platform and the plurality of
30 security subsystems are connected to each other via dual-channel communication. The plurality of security subsystems include a master-site-state security subsystem and at least one backup-site-state security subsystem and each include a plurality of computers. Every two of the plurality of computers are connected to each other via a dual-channel communication, and the

plurality of computers include a master-system-state computer and at least one backup-system-state computer. The master-system-state computer in the master-site-state security subsystem is configured to execute a host task and perform data synchronization operation on other computers in the disaster recovery system, so that at least one of the plurality of computers that
5 completes data synchronization is in a hot-backup state. In each platform cycle, the master-site-state security subsystem and the at least one backup-site-state security subsystem are configured to communicate with each other and monitor a communication status of each other. Under a condition that it is monitored that the communication status is abnormal, at least one of the master-site-state security subsystem or the at least one backup-site-state security
10 subsystem is configured to transmit an arbitration request to the third-party arbitration platform. The third-party arbitration platform is configured to, upon receiving the arbitration request, determine whether to switch the master-site-state security subsystem to an unavailable site state and switch one of the at least one backup-site-state security subsystem to a master site state, so that the master-system-state computer in the new master-site-state security subsystem takes
15 over and executes the host task after the switching.

[0006] In an embodiment of the first aspect, the master-site-state security subsystem is configured to transmit a master-site retention request to the at least one backup-site-state security subsystem and monitor an acknowledgment response from the at least one backup-site-state security subsystem, and transmit a first arbitration request to the third-party
20 arbitration platform under a condition that the master-site-state security subsystem fails to receive the acknowledgment response, the first arbitration request being configured to request the master-site-state security subsystem to maintain the master site state; and the at least one backup-site-state security subsystem each is configured to receive the master-site retention request transmitted from the master-site-state security subsystem, and transmit a second
25 arbitration request to the third-party arbitration platform under a condition that the backup-site-state security subsystem fails to receive the master-site retention request, the second arbitration request being configured to request the backup-site-state security subsystem to switch to the new master-site-state security subsystem.

[0007] In an embodiment of the first aspect, the third-party arbitration platform is
30 configured to: return a first arbitration response to the master-site-state security subsystem only upon receiving the first arbitration request, the first arbitration response being configured to confirm maintaining the master site state of the master-site-state security subsystem; upon receiving only the second arbitration request, return a second arbitration response to the at least

one backup-site-state security subsystem, the second arbitration response being configured to control one of the at least one backup-site-state security subsystem to switch to the new master-site-state security subsystem and authorize the master-system-state computer in the new master-site-state security subsystem to take over and execute the host task; and upon receiving
5 both the first arbitration request and the second arbitration request, process the first arbitration request and the second arbitration request sequentially in a sequence in which the first arbitration request and the second arbitration request are received.

[0008] In an embodiment of the first aspect, under a condition that the master-site-state security subsystem receives the first arbitration response and maintains to operate in the master
10 site state or the backup-site-state security subsystem receives the second arbitration response and switches to the new master-site-state security subsystem, the master-site-state security subsystem or the new master-site-state security subsystem is configured to: periodically transmit the master-site retention request to the third-party arbitration platform, monitor an acknowledgment response from the third-party arbitration platform, and maintain the master
15 site state upon receiving the acknowledgment response from the third-party arbitration platform; and the third-party arbitration platform is further configured to receive the master-site retention request transmitted from the master-site-state security subsystem or the new master-site-state security subsystem and return the acknowledgment response.

[0009] In an embodiment of the first aspect, a platform periodic operation primary-task, a
20 local master/backup voting task, and a master/backup site voting task are deployed on each of the plurality of computers in each of the plurality of security subsystems; the platform periodic operation primary-task is configured to simultaneously trigger the local master/backup voting task and the master/backup site voting task to be executed in each platform cycle; the local master/backup voting task is configured to perform local master-backup voting among the
25 plurality of computers in a same one of the plurality of security subsystems, and determine that each of the plurality of computers belongs to the master-system-state computer or one of the at least one backup-system-state computer to obtain a local master-backup voting result; the master/backup site voting task is configured to cause the master-site-state security subsystem and the at least one backup-site-state security subsystem to: communicate with each other in
30 each platform cycle, monitor the communication status of each other, and transmit the arbitration request to the third-party arbitration platform under a condition that it is monitored that the communication status is abnormal, so as to obtain a master-backup site voting result; and the platform periodic operation primary-task is configured to acquire the local master-

backup voting result from the local master/backup voting task, acquire the master-backup site voting result from the master/backup site voting task, cause a current computer that is determined as the master-system-state computer in the master-site-state security subsystem based on the local master-backup voting result and the master-backup site voting result, to
5 execute the host task, and perform data synchronization operation on other computers in the disaster recovery system, so that at least one of the other computers that completes data synchronization is in the hot-backup state.

[0010] In an embodiment of the first aspect, the plurality of computers in a same one of the plurality of security subsystems are further configured to: communicate with each other via the
10 local master/backup voting task to update their master-backup system states; and under a condition of abnormal communication, switch at least one of the plurality of computers in a master system state in the security subsystem to an unavailable state, and switch one of the plurality of computers in a backup system state in the security subsystem to the master system state.

[0011] In an embodiment of the first aspect, the plurality of computers in a same one of the plurality of security subsystems are further configured to: mutually transmit master-system promotion requests after successful self-checks; and among at least two of the plurality of computers that return response results for the master-system promotion requests from other computers, determine the master-system-state computer and the at least one backup-system-
20 state computer based on a first priority sequence.

[0012] In an embodiment of the first aspect, the plurality of security subsystems are further configured to: mutually transmit master-site promotion requests; and among at least two of the plurality of security subsystems that return response results for the master-site promotion requests from other security subsystems, determine the master-site-state security subsystem and the at least one backup-site-state security subsystem based on a second priority sequence.
25

[0013] In an embodiment of the first aspect, the disaster recovery system includes two security subsystems, and one of the two security subsystems is further configured to, under a condition that no response result for the master-site promotion request is received from the other one of the two security subsystems, transmit the master-site promotion request to the
30 third-party arbitration platform, receive a response result returned by the third-party arbitration platform, and switch to the master-site-state security subsystem.

[0014] In a second aspect, some embodiments of the present disclosure provide a disaster recovery method based on a redundant architecture, which is applicable to a disaster recovery

system. The disaster recovery system includes a third-party arbitration platform and a plurality of security subsystems. The third-party arbitration platform and the plurality of security subsystems are deployed at different geographic locations. Every two of the third-party arbitration platform and the plurality of security subsystems are connected to each other via a dual-channel communication. The plurality of security subsystems include a master-site-state security subsystem and at least one backup-site-state security subsystem and each include a plurality of computers. Every two of the plurality of computers are connected to each other via a dual-channel communication, and the plurality of computers include a master-system-state computer and at least one backup-system-state computer.

[0015] The disaster recovery method includes:

[0016] executing, by the master-system-state computer in the master-site-state security subsystem, a host task, and performing data synchronization operation on other computers in the disaster recovery system, so that at least one of the plurality of computers that completes data synchronization is in a hot-backup state;

[0017] in each platform cycle of the host task, communicating, by the master-site-state security subsystem and the at least one backup-site-state security subsystem, with each other and monitoring a communication status of each other;

[0018] under a condition that it is monitored that the communication status is abnormal, transmitting, by at least one of the master-site-state security subsystem or the at least one backup-site-state security subsystem, an arbitration request to the third-party arbitration platform; and

[0019] upon receiving the arbitration request, determining, by the third-party arbitration platform, whether to switch the master-site-state security subsystem to an unavailable site state, and switching one of the at least one backup-site-state security subsystem to a master site state, so that the master-system-state computer in the new master-site-state security subsystem takes over and executes the host task after the switching.

[0020] In a third aspect, some embodiments of the present disclosure provide a disaster recovery method based on a redundant architecture, which is applicable to a plurality of security subsystems in a disaster recovery system. The disaster recovery system further includes a third-party arbitration platform. The third-party arbitration platform and the plurality of security subsystems are deployed at different geographic locations. Every two of the third-party arbitration platform and the plurality of security subsystems are connected to each other via a dual-channel communication. The plurality of security subsystems include a master-site-

state security subsystem and at least one backup-site-state security subsystem and each include a plurality of computers. Every two of the plurality of computers are connected to each other via a dual-channel communication, and the plurality of computers include a master-system-state computer and at least one backup-system-state computer.

5 **[0021]** The disaster recovery method includes:

[0022] executing, by the master-system-state computer in the master-site-state security subsystem, a host task, and performing data synchronization operation on other computers in the disaster recovery system, so that at least one of the plurality of computers that completes data synchronization is in a hot-backup state; and

10 **[0023]** periodically communicating, by each of the plurality of security subsystems with other security subsystems, and monitoring communication status of other security subsystems, transmitting an arbitration request to the third-party arbitration platform under a condition that it is monitored that the communication status is abnormal, and based on a determination result of the third-party arbitration platform, maintaining a current master site state to operate, or
15 executing an operation of switching to a new master-site-state security subsystem so that the master-system-state computer in the new master-site-state security subsystem takes over and executes the host task after the switching.

[0024] In a fourth aspect, some embodiments of the present disclosure provide a disaster recovery method based on a redundant architecture, which is applicable to a third-party
20 arbitration platform in a disaster recovery system. The disaster recovery system further includes a plurality of security subsystems. The third-party arbitration platform and the plurality of security subsystems are deployed at different geographic locations. Every two of the third-party arbitration platform and the plurality of security subsystems are connected to each other via a dual-channel communication. The plurality of security subsystems include a master-site-state
25 security subsystem and at least one backup-site-state security subsystem and each include a plurality of computers. Every two of the plurality of computers are connected to each other via a dual-channel communication, and the plurality of computers include a master-system-state computer and at least one backup-system-state computer.

[0025] The disaster recovery method includes:

30 **[0026]** receiving an arbitration request transmitted from at least one of the plurality of security subsystems; and determining to maintain a master site state of a current master-site-state security subsystem, or determining to switch one of the at least one backup-site-state security subsystem to a new master-site-state security subsystem and authorizing the master-

system-state computer in the new master-site-state security subsystem state to take over and execute the host task after the switching; and

[0027] returning a determination result to the at least one of the plurality of security subsystems.

5 **[0028]** In a fifth aspect, some embodiments of the present disclosure provide an electronic device, and the electronic device includes a processor, and a memory storing computer program instructions. The processor is configured to read and execute the computer program instructions to implement any one of the methods of the second, third, or fourth aspect.

[0029] In a sixth aspect, some embodiments of the present disclosure provide a computer-readable storage medium. The computer-readable storage medium stores computer program instructions. When executed by a processor, the computer program instructions implement any one of the methods of the second, third, or fourth aspect.

[0030] In a seventh aspect, some embodiments of the present disclosure provide a computer program product. The computer program product includes a computer program. When
15 executed by a processor, the computer program implements any one of the methods of the second, third, or fourth aspect.

[0031] The technical solutions provided in the embodiments of the present disclosure bring at least the following beneficial effects.

[0032] According to the disaster recovery system based on the redundant architecture
20 provided in the embodiments of the present disclosure, the third-party arbitration platform and multiple security subsystems are deployed at different sites, a master-backup redundancy is provided at each of the security subsystem level and the computer level, and in combination with a unique arbitration mechanism of the third-party arbitration platform, rapid detection and seamless switching are achieved under cases of abnormal communication or equipment failures.
25 In this way, the operation security, the fault tolerance, and the service continuity are enhanced, thereby meeting disaster recovery requirements in scenarios with high security demands.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033] To more clearly illustrate the technical solutions of the embodiments of the present disclosure, the following provides a brief introduction to the drawings required for the
30 embodiments of the present disclosure.

[0034] Fig. 1 is an architecture schematic diagram of a disaster recovery system based on a redundant architecture provided in some embodiments of the present disclosure;

[0035] Fig. 2 is a flowchart of a disaster recovery method based on a redundant architecture provided in some embodiments of the present disclosure;

[0036] Fig. 3 is a flowchart of a disaster recovery method based on a redundant architecture provided in some embodiments of the present disclosure;

5 [0037] Fig. 4 is an interaction flowchart of task execution sequences provided in some embodiments of the present disclosure;

[0038] Fig. 5 is a flowchart of executing data and time synchronization provided in some embodiments of the present disclosure; and

[0039] Fig. 6 is a schematic diagram of a computer device provided in some embodiments
10 of the present disclosure.

DETAILED DESCRIPTION

[0040] To enable those skilled in the art to better understand the technical solutions of the present disclosure, the technical solutions in the embodiments of the present disclosure will be
15 described clearly and completely below with reference to the accompanying drawings. It should be understood that the specific embodiments described herein are intended only to explain the present disclosure and not to limit it. For those skilled in the art, the present disclosure can be implemented without some of the details described herein. The following description of the embodiments is provided only to facilitate a better understanding of the
20 present disclosure by illustrating examples thereof.

[0041] As described in the BACKGROUND section, implementing disaster recovery for critical equipments such as signal control systems is paramount in fields with extremely high safety and reliability requirements, such as rail transit and nuclear power.

[0042] Existing disaster recovery solutions lack coordinated management for a multi-site
25 deployment, synchronized communication status across systems, and highly reliable failover control, and thus struggle to fully meet the stringent requirements for safety, continuity, and redundancy protection demanded by systems like rail transit.

[0043] To address this technical problem, some embodiments of the present disclosure provide a disaster recovery method and system based on a redundant architecture. Specifically,
30 multi-level redundancy protection for safety systems is achieved by constructing a physically isolated and off-site redundant architecture. On such basis, device operational states are monitored in real time and determined consistency by employing communication status voting mechanisms in the same safety system and across systems, so that when there is a failure in

any redundant device, the failure is timely detected and then automatic switching to a functional redundant device is performed, ensuring the service continuity and the high operational reliability.

[0044] Fig. 1 is an architecture schematic diagram of a disaster recovery system based on a redundant architecture provided in an embodiment of the present disclosure. As shown in Fig. 1, the disaster recovery system 10 based on the redundant architecture includes a third-party arbitration platform 100 and multiple security subsystems 200.

[0045] It should first be noted that Fig. 1 and the subsequent embodiment descriptions merely illustrate an example where two security subsystems are provided. In practice, the architecture of the disaster recovery system 10 is not limited to such configuration and can include three, four, five, or even more security subsystems to accommodate requirements for varying system scales and different disaster recovery levels. It should be understood that increasing the number of security subsystems does not alter the fundamental principles of the redundancy architecture described herein but merely further enhances the reliability and the fault tolerance of the system.

[0046] The third-party arbitration platform 100 and the multiple security subsystems 200 are deployed at different geographic locations. That is, the third-party arbitration platform 100 and each security subsystem 200 are deployed at different geographic locations, and the multiple security subsystems 200 are deployed at multiple geographic locations different from each other. For example, as shown in Fig. 1, the third-party arbitration platform 200 is deployed at position C, the left security subsystem 200 is deployed at position A, and the right security subsystem 200 is deployed at position B. With such multiple-site deployment, when a catastrophic failure occurs in a region, subsystems in other regions remain operational, so that system-level multiple-location redundant protection is achieved, which significantly enhances overall disaster recovery capability and service continuity.

[0047] Additionally, as shown in Fig. 1, a dual-channel communication link is established between the third-party arbitration platform 100 and each security subsystem 200, and a dual-channel communication link is also established between every two security subsystems 200. For example, multiple security subsystems 200 can achieve communicated connection via multiple-location redundant fiber-optic links. The multiple-location redundant fiber-optic links can be designed as a dual-channel Ethernet communication. Such communication design can ensure timely and reliable information exchange among multiple security subsystems and the third-party arbitration platform.

[0048] According to their different control status, multiple security subsystems 200 can be divided into a master-site-state security subsystem 210 and a backup-site-state security subsystem 220. In the architecture diagram shown in Fig. 1, the left security subsystem serves as the master-site-state security subsystem 210, and the right security subsystem serves as the backup-site-state security subsystem 220.

[0049] The master-site-state security subsystem 210 is a security subsystem responsible for actual control and service processing tasks.

[0050] The backup-site-state security subsystem 220 is a security subsystem that remains in a backup or synchronous operating state and that is configured to take over services when failure occurs in the master-site-state security subsystem 210.

[0051] It should be noted that, for clarity, in the following text, the master-site-state security subsystem is referred to as a “master system”, and the backup-site-state security subsystem is referred to as a “backup system”.

[0052] It should be understood that during the operation of the disaster recovery system 10, only one master system 210 is provided, at least one backup system 220 is provided, and a communicated connection is maintained between the master system 210 and the backup system 220. In other words, a “one master and one backup” or “one master and multiple backups” architecture design is adopted at the security subsystem level, so that scenarios where double master systems operate in parallel are avoided, thereby preventing conflicts and security risks caused by inconsistent states of systems.

[0053] Furthermore, each security subsystem 200 internally includes multiple security computers.

[0054] It should be noted that Fig. 1 and the subsequent embodiments merely illustrate an example where two security computers. In practice, three, four, five, or even more security computers can also be deployed in each security subsystem to accommodate requirements for different system scales and different disaster recovery levels. It should be understood that increasing the number of the security computers does not alter the fundamental principles of the redundancy architecture described herein, but rather further enhances the computational redundancy and the fault tolerance in the subsystem.

[0055] In an embodiment, two security computers deployed in each security subsystem form a 2oo2 (Two-out-of-Two) architecture.

[0056] Furthermore, as shown in Fig. 1, a dual-channel communication link is established between every two of multiple security computers in a same security subsystem. For example,

the security computers in a same subsystem achieve communicated connection through dual-channel Ethernet communication and dual-channel RS-422 (serial differential communication standard 422) communication. It should be understood that the dual-channel RS-422 communication can be replaced with any other communication method, such as hardware
5 pulses. Such design can ensures data exchange while achieving effective monitoring and control of communication status, thereby enhancing the stability and the reliability of internal subsystem communication.

[0057] According to their different control status, multiple security computers in each security subsystem 200 can be divided into a master-system-state computer and a backup-
10 system-state computer.

[0058] A master-system-state computer is a security computer responsible for master computation and control tasks in the security subsystem.

[0059] A backup-system-state computer is a security computer that is in a backup or synchronized state and that is configured to take over tasks when there is a failure in the master-
15 system-state computer.

[0060] It should be noted, for clarity, in the following description, the master-system-state computer is referred to as a “master computer”, and the backup-system-state computer is referred to as a “backup computer”.

[0061] It should be understood that during operation of the disaster recovery system 10, each security subsystem 200 includes only one master computer and is provided with at least
20 one backup computer. In other words, the “one master and one backup” or “one master and multiple backups” architecture design is also adopted at the security computer level, so that a scenario where double master computers operate concurrently is avoided, thereby avoiding logical conflicts caused by master computers in a same subsystem competing for control.

[0062] Correspondingly, the master system 210 includes a master computer 211 and a backup computer 212, and the backup system 220 includes a master computer 221 and a backup
25 computer 222. The local computer-level redundancy configuration can further enhance the stability and the fault tolerance of an individual subsystem, and forms a complement with a remote system-level redundancy to establish a multi-level disaster recovery protection
30 mechanism.

[0063] It should be understood that, in some embodiments, the roles of the master system and the backup system, as well as the master computer and the backup computer, can be preset and fixed during system deployment. In some embodiments, multiple security subsystems and

their security computers have the same functions and status at an initial state without preset role distinctions. In this case, through communication interaction and state determination mechanisms during a system initialization phase, the master system and the backup system, as well as the master computer and the backup computer, can be automatically negotiated to be differentiated, which achieves flexible role assignment and redundancy control.

[0064] After determining the master system and the backup systems in the disaster recovery system 10, as well as the master computer and the backup computer in each security subsystem via the aforementioned methods, the following describes a function of each component when the disaster recovery system 10 is in an operating state.

[0065] The master computer 211 of the master system 210 is configured to execute a host task and perform data synchronization operation on other security computers in the disaster recovery system 10, so that at least one of the plurality of computers that completes data synchronization is in a hot-backup state.

[0066] In other words, the master-system-state computer 211 in the master-site-state security subsystem 210 is configured to execute the host task and perform data synchronization operation on the other security computers in the disaster recovery system 10, so that at least one of the multiple computers that completes data synchronization is in the hot-backup state.

[0067] The host task refers to core control, computation, or service processing task undertaken by the master-system-state computer 211 in the master-site-state security subsystem 210.

[0068] In an embodiment, the master computer 211 of the master system 210 is also configured to perform time synchronization operations on other computers in the disaster recovery system 10. The security computer completing time synchronization and data synchronization switches to the hot-backup state, so as to rapidly take over the host task when there is a failure in the master computer 211.

[0069] A possible implementation of the above embodiment includes the following steps. During a power-up initialization phase, the master computer 211 of the master system 210 first initiates time synchronization communication, to drive other computers to complete time calibration with the master computer 211; after completing power-up time synchronization, the disaster recovery system 10 enters a periodic operation phase where the master computer 211 and other computers periodically perform clock deviation assessment and time synchronization processing. After completing time synchronization, the backup computers other than the master computer 211 periodically transmit time synchronization completion marks to the master

computer 211; and the master computer 211 determines whether to initiate data follow-up requests to corresponding backup computers based on their completion marks. Backup computers upgrade to the hot-backup state upon completing data follow-up synchronization. Upon detecting that a certain backup computer has successfully transitioned to the hot-backup state, the master computer 211 disables continuous data follow-up function of the backup computer to reduce system load and maintain state stability.

[0070] With the above mechanism, the master computer 211 of the master system 210 not only executes core task but also ensures that the backup computers maintain highly consistent operational state with the master computer via time and data synchronization, so that the backup computers have the takeover capability at any time, thereby achieving rapid and reliable disaster recovery switching.

[0071] In each platform cycle, the master system 210 and the backup system 220 are configured to communicate with each other and monitor a communication status of each other. Upon monitoring that the communication status of the other is abnormal, the master system 210 and/or the backup system 220 is configured to transmit an arbitration request to the third-party arbitration platform 100.

[0072] That is, in each platform cycle, the master-site-state security subsystem 210 and the backup-site-state security subsystem 220 are configured to communicate with each other and monitor a communication status of each other. Upon monitoring that the communication status of the other is abnormal, the master-site-state security subsystem 210 and/or the backup-site-state security subsystem 220 are configured to transmit the arbitration request to the third-party arbitration platform 100.

[0073] The arbitration request refers to a message initiated by either party when communication between security subsystems becomes abnormal or their states become inconsistent, requesting the third-party arbitration platform 100 to determine a master/backup identity.

[0074] It should be understood that the purpose of communication between systems is to confirm whether the other is in a normal operating state. Upon monitoring an anomaly, a central arbitration is requested in time through the third-party arbitration platform to avoid confusion between master and backup roles caused by both parties simultaneously losing their decision-making capabilities.

[0075] For example, the arbitration request from the master system 210 can be transmitted by the master computer 211 or the backup computer 212, while the arbitration request from the

backup system 220 is transmitted by the master computer 221.

[0076] In an embodiment, the master system 210 is configured to transmit a master-site retention request to the backup system 220 and monitor an acknowledgment response of the backup system 220. Under a condition that the master system 210 fails to receive the
5 acknowledgment response, the master system 210 transmits a first arbitration request to the third-party arbitration platform 100.

[0077] That is, the master-site-state security subsystem 210 is configured to transmit the master-site retention request to the backup-site-state security subsystem 220 and monitor an acknowledgment response from the backup-site-state security subsystem 220. Under a
10 condition that the master-site-state security subsystem 210 fails to receive the acknowledgment response, the master-site-state security subsystem 210 transmits the first arbitration request to the third-party arbitration platform 100.

[0078] Correspondingly, the backup system 220 is configured to periodically receive the master-site retention request transmitted from the master system 210. Under a condition that
15 the backup system 220 fails to receive the master-site retention request, the backup system 220 transmits a second arbitration request to the third-party arbitration platform 100.

[0079] That is, the backup-site-state security subsystem 220 is configured to receive the master-site retention request transmitted from the master-site-state security subsystem 210. Under a condition that the backup-site-state security subsystem 220 fails to receive the master-
20 site retention request, the backup-site-state security subsystem 220 transmits the second arbitration request to the third-party arbitration platform 100.

[0080] The master-site retention request is a message transmitted from the master-site-state security subsystem 210 for indicating that it is in a normal operating state and requesting continued maintenance of the master site state.

[0081] The first arbitration request is used to request the maintenance of both the master site state and normal operation of the master-site-state security subsystem 210.

[0082] The second arbitration request is used to request switching the backup-site-state security subsystem 220 to a new master-site-state security subsystem.

[0083] In this embodiment, a complete communication and arbitration process is as follows.

[0084] The master system 210 transmits the master-site retention request to the backup
30 system 220; upon receiving the master-site retention request, the backup system 220 returns an acknowledgment response permitting the maintenance of the master site state; and after receiving the acknowledgment response from the backup system 220, the master system 210

maintains its own master site state;

[0085] when failing to receive the acknowledgment response, the master system 210 considers that the backup system 220 may have a failure or the communication link is abnormal, and in this case, the master system 210 transmits the first arbitration request to the third-party arbitration platform 100 to request maintenance of its master site state; and

[0086] under a condition that the backup system 220 fails to receive the master-site retention request, the backup system 220 considers that the master system 210 may have a failure or the communication link is abnormal, and in this case, the backup system 220 transmits the second arbitration request to the third-party arbitration platform 100 to request itself or another backup system to be promoted to a new master system.

[0087] Exemplarily, under a condition that the disaster recovery system 10 includes only one backup system 220, the second arbitration request from the backup system 220 is to request that it be switched to the new master system; and under a condition that the disaster recovery system 10 includes multiple backup systems 220, the second arbitration request is to request that the master system be switched, and the third-party arbitration platform 100 selects an optimal backup system among the multiple backup systems 220 according to a preset evaluation mechanism to switch the optimal backup system to the new master system.

[0088] With the above configuration, the disaster recovery system 10 may achieve real-time status verification and anomaly detection between the master system and the backup system during operation, and under a condition that there is abnormal communication or an equipment failure, the disaster recovery system 10 completes master-backup switching rapidly and reliably with the third-party arbitration platform 100. Such mechanism not only avoids a scenario where there are double master systems or the system lacks master control, but also ensures the consistency and the high reliability during this switching process, thereby significantly enhancing the fault tolerance and the service continuity of the system in critical scenarios.

[0089] The third-party arbitration platform 100 is configured to, upon receiving the arbitration request, determine whether to switch the master system 210 to an unavailable site state according to the arbitration request, and switch one of the backup systems 220 to a new master system, so that the master computer in the new master system takes over and executes the host task after the switch is completed.

[0090] In other words, the third-party arbitration platform 100 is configured to, upon receiving the arbitration request, determine whether to switch the master-site-state security

subsystem 210 to the unavailable site state according to the arbitration request, and switch one of the backup-site-state security subsystems 220 to the master site state, so that the master-system-state computer in the new master-site-state security subsystem takes over and executes the host task after the switch is completed.

5 **[0091]** Depending on different types of arbitration requests and different transmitter, in an embodiment, a processing logic of the third-party arbitration platform 100 includes the following steps.

10 **[0092]** Under a condition that the third-party arbitration platform 100 receives only the first arbitration request, the third-party arbitration platform 100 determines that the current master system 210 is operating normally, and confirms that the master system 210 continues operating. In an implementation, under a condition that only the first arbitration request is received, the first arbitration response is returned to the master-site-state security subsystem 210. The first arbitration response is configured to confirm that the master-site-state security subsystem 210 maintains the master site state.

15 **[0093]** Under a condition that the third-party arbitration platform 100 receives only the second arbitration request, the third-party arbitration platform 100 determines that the master system 210 may have a failure or there is abnormal communication, one of the backup systems 220 is controlled to switch to a new master system, and the master computer in the new master system is authorized to take over the host task. In an implementation, a second arbitration response is returned to the backup-site-state security subsystem 220. The second arbitration response is configured to control one of the backup-site-state security subsystems 220 to switch to a new master-site-state security subsystem and authorize the master-state computer in the new master-site-state security subsystem to take over and execute the host task.

25 **[0094]** Under a condition that the third-party arbitration platform 100 receives both the first arbitration request and the second arbitration request, the third-party arbitration platform 100 sequentially processes the first arbitration request and the second arbitration request in a sequence in which the first arbitration request and the second arbitration request are received.

30 **[0095]** It should be understood that the third-party arbitration platform 100 internally pre-configures an arbitration algorithm. With a serial processing mechanism for arbitration information, the arbitration algorithm ensures that there is only one master system at any one moment. Specifically, when the third-party arbitration platform 100 receives the arbitration requests from both the master system 210 and the backup system 220, the third-party arbitration platform 100 processes these arbitration requests according to the sequence in which these

arbitration requests are received, and responds to the earlier request in priority, so as to avoid “double master systems” to guarantee the uniqueness of the arbitration result.

[0096] With the design in the above embodiment, the third-party arbitration platform 100 can flexibly adjudicate arbitration requests of different origins and types. The third-party arbitration platform 100 can not only maintain the status of the current master control when the master system 210 is operating normally, but also switch the backup system 220 to a new master system in time when there is a failure in the master system 210 or there is abnormal communication. Furthermore, the third-party arbitration platform 100 ensures arbitration uniqueness through sequential processing mechanism when there are conflicting requests. In this way, risks of “double master systems” or loss of master control are effectively avoided, which ensures the reliability and service continuity during system switching.

[0097] According to the disaster recovery system based on the redundant architecture provided in the present disclosure, the third-party arbitration platform and multiple security subsystems are deployed at different sites, redundancy is provided at both the security subsystem level and the security computer level, and in combination with a unique arbitration mechanism of the third-party arbitration platform, rapid detection and seamless switching are achieved in cases of abnormal communication or equipment failures. This system not only guarantees the uniqueness of master/backup identity and the high reliability during switching but also maintains the backup computer in the hot-backup state through data synchronization, thereby achieving timely service takeover when there is a failure in the master computer. In this way, the overall system enhances the operation security, fault tolerance, and service continuity, thereby meeting the disaster recovery requirements in scenarios with high security demands.

[0098] In an embodiment, when the master-site-state security subsystem 210 receives the first arbitration response and maintains the master site state to operate, or when the backup-site-state security subsystem 220 receives the second arbitration response and switches to the new master-site-state security subsystem, the master-site-state security subsystem 210 or the new master-site-state security subsystem is configured to: periodically transmit the master-site retention request to the third-party arbitration platform 100, monitor the acknowledgment response from the third-party arbitration platform, and maintain the master site state upon receiving the acknowledgment response; and the third-party arbitration platform 100 is configured to receive the master-site retention request transmitted from the master-site-state security subsystem or the new master-site-state security subsystem, and return the

acknowledgment response.

[0099] According to such design in this embodiment, when there is a system abnormality, the third-party arbitration platform 100 can communicate with the security subsystem currently in the master site state, and continuous maintenance of the master site state is guaranteed through periodic interactions of retention request and acknowledgment response; meanwhile, after the master-backup switching, the new master-site-state security subsystem can also maintain master site state confirmation with the third-party arbitration platform through the same interaction mechanism, so as to avoid loss of the master site state or inconsistencies in the master state and the backup state due to abnormality, enhancing the operation stability and the reliability of the system.

[00100] In an embodiment, the master computer and the backup computer in each security subsystem are connected to each other via dual-channel communication. For example, the security computers in a same security subsystem achieve four-line communication connections via a data line and a control signal line.

[00101] It can be understood that during the operating process of the disaster recovery system 10, the computers in each security subsystem also communicate with each other to confirm whether the other is in a normal operating state. Upon detecting an abnormality, switching between the master computer and the backup computer can be completed in time, thereby preventing task interruptions caused by a single point failure.

[00102] Accordingly, in an embodiment, functions of parts in the security subsystem during communication include:

[00103] the master computer in each security subsystem is configured to transmit a master-system retention request to the backup computer in the same security subsystem and receive an acknowledgment response returned by the backup computer; and

[00104] the backup computer in each security subsystem is configured to monitor the master-system retention request transmitted from the master computer in the same security subsystem, return an acknowledgment response to the master computer upon receiving the master-system retention request, and switch to the master computer and take over an execution task of the original master computer it when the backup computer fails to receive the master-system retention request.

[00105] The master-system retention request is a message transmitted from the computer currently in the master system state and configured to declare its master computer identity and maintain its master system state.

[00106] At the local security subsystem level, rapid disaster recovery in the security subsystem is achieved through periodic communication between the master computer and the backup computer and an autonomous switching mechanism. When the master computer operates normally, the master-system retention request and the acknowledgment response form a stable communication link, ensuring the master computer status is not misjudged; and when there is an abnormality in the master computer or the communication link is disconnected, the backup computer can swiftly take over tasks, preventing system pauses or service interruption, thereby significantly enhancing the reliability and the fault tolerance of the disaster recovery system. As mentioned in the above embodiments, the role assignments between the master system and the backup system, and the master computer and the backup computer, can be preset during disaster recovery system deployment or can be automatically negotiated and distinguished through communication interactions and state determination mechanisms.

[00107] It can be understood that automatically negotiating master/backup roles via communication interaction avoids limitations inherent in manual configuration, providing the system with greater adaptability and flexibility across diverse deployment environments. Accordingly, the present disclosure proposes a mechanism for automatically completing role election during an initialization phase of the disaster recovery system. Under this mechanism, the function of each part is as follows. In an embodiment, multiple computers in the same security subsystem are configured to: after successful self-check, mutually transmit master-system promotion requests; and among at least two of the multiple computers that return response results for the master-system promotion requests from other computers, determine the master-system-state computer and the backup-system-state computer based on a first priority sequence.

[00108] The master-system promotion request is a communication request transmitted from a security computer and configured to vie for the master system state during an initialization process of the disaster recovery system.

[00109] The first priority sequence is a preset comparison basis configured to resolve situations where multiple security computers each meet a candidate condition for the master computer.

[00110] Exemplarily, the first priority sequence can be preset based on information such as a hardware serial number, a power-on sequence, or configuration parameters, which is not limited in the present disclosure.

[00111] That is, during the initialization phase of the disaster recovery system, multiple

security computers in each secure subsystem mutually transmit the master-system promotion requests; and among computers returning responses, the computer with the highest priority is determined as a master computer according to the first priority sequence, and other computers are determined as backup computers.

5 **[00112]** Exemplarily, status of security computers that fail to transmit the master-system promotion requests or return responses is marked as unavailable to prevent abnormal nodes from interfering the election result.

10 **[00113]** With reference to an example, it is supposed that only two security computers are deployed in a security subsystem, which are designated as computer A and computer B. After this subsystem is powered on, arbitration is completed relying on four-line communication between two local computers:

15 **[00114]** under a condition that the computer A and the computer B are powered on simultaneously and each keep a normal communication, since the computer A has a higher master promotion priority by default, the computer A serves as a master computer, and the computer B serves as a backup computer;

20 **[00115]** under a condition that only the computer A is powered on and the four-line communication times out, it is determined that the computer B is offline and the computer A is directly upgraded to the master computer;

25 **[00116]** under a condition that only computer B is powered on and the four-line communication times out, it is determined that the computer A is offline and the computer B is directly upgraded to the master computer;

30 **[00117]** under a condition that the computer B is already operating as the master computer the computer B periodically broadcasts master computer maintenance information; and then when the computer A is subsequently powered on and receives this information, the computer A automatically enters a backup state, while the computer B maintains its master computer status; and

35 **[00118]** under a condition that the computer A is already operating as the master computer, when the computer B is powered on, the computer B automatically enters the backup state.

40 **[00119]** It can be seen from the above that this embodiment achieves automatic negotiation and rapid confirmation of the master computer and the backup computer through the communication interactions and the priority rules between the local computers, which not only reduces the complexity of manual configuration and human intervention but also avoids double master computer conflict or ambiguous role assignment. In this way, the reliability and the

consistency of system initialization are ensured, thereby laying the foundation for the stable operation of the disaster recovery system.

[00120] In an embodiment, the multiple security subsystems are further configured to: mutually transmit master-site promotion requests; and among at least two of the multiple security subsystems that return response results for the master-site promotion requests from other security subsystems, determine the master-site-state security subsystem and the backup-site-state security subsystem based on a second priority sequence.

[00121] The master-site promotion request refers to a communication request transmitted from a security subsystem and configured to vie for the master site state during the initialization process of the disaster recovery system.

[00122] The second priority sequence refers to a basis for comparison and adjudication when multiple security subsystems each meet a candidate condition for the master system.

[00123] Exemplarily, the second priority sequence can be set based on method of deployment site priority of the subsystems, hardware configuration parameters, power-on sequence, or operational maintenance policies, which is not limited in the present disclosure.

[00124] That is, during the initialization phase of the disaster recovery system, security subsystems mutually transmit master-site promotion request; and among at least two of the multiple security subsystems that return response results, the security subsystem with the highest priority is determined as the master system according to the second priority sequence, and other security subsystems are determined as the backup systems.

[00125] Furthermore, taking cases of abnormal communication into account, in an embodiment, multiple security subsystems are also configured to transmit the master-site promotion requests to the third-party arbitration platform under a condition that they do not receive a response result from other security subsystems.

[00126] Correspondingly, the third-party arbitration platform is also configured to compare priorities of the security subsystems corresponding to these requests based on the second priority sequence upon receiving the master-site promotion requests, determine the security subsystem with the highest priority as the master system, and determine the other security subsystems as the backup systems.

[00127] With such design, even in a scenario of cross-region communication failures or a scenario where some subsystems cannot return responses, the third-party arbitration platform can provide unified adjudication, which ensures that there is always only one master system in the system and avoids problems of “double masters” or “no master”. Consequently, the

robustness and the reliability of the disaster recovery system in a complex network environment are significantly enhanced.

[00128] With reference to an example, it is supposed that two security subsystems respectively located at sites A and B are deployed in the disaster recovery system, these
5 subsystems at two different sites perform master-backup voting via dedicated redundant optical fiber:

[00129] in a default case, the subsystem at site A has a right to be promoted to the master system in priority, and transmits the master-site promotion request to the subsystem at site B through an inter-site redundant optical fiber; under a condition that the subsystem at site B is
10 powered on and receives the request, the subsystem at site B returns a response permitting the master-site promotion; and under a condition that both the request and the response are successful, the subsystem at site A becomes the master system, and the subsystem at site B switches to the backup system;

[00130] under a condition that the subsystem at site B is already in a master state, the
15 subsystem at site B periodically broadcasts its master-system state, the subsystem at site A automatically switches to the backup system upon receiving the broadcast, and the subsystem at site B maintains the master site status;

[00131] under a condition that there is completely abnormal communication between two sites, site A and site B simultaneously initiate the master-site promotion request to the third-
20 party arbitration platform at site C, and according to the arbitration algorithm, the third-party arbitration platform permits only one subsystem to be promoted to the master system and the other subsystem to switch to the backup system; and

[00132] under a condition that only site A fails to receive a response from site B, the subsystem at site A requests the third-party arbitration platform at site C to be promoted to the
25 master system, and under a condition that the arbitration succeeds, the subsystem at site A becomes the master system, and the subsystem at site B switches to the backup system.

[00133] It can be seen from the above contents, this embodiment achieves automatic master-backup differentiation across regions by introducing a cross-security-subsystem master election mechanism during the initialization phase of the disaster recovery system, in
30 combination with the second priority sequence and the decision-making capability of the third-party arbitration, so as to avoid a scenario of “double masters” or “no master” caused by a race condition, thereby ensuring determinism during the initialization process of the system and the high reliability during operation.

[00134] The following describes a disaster recovery method based on a redundant architecture provided in the present disclosure with reference to the embodiments.

[00135] Fig. 2 illustrates a disaster recovery method based on a redundant architecture provided in some embodiments of the present disclosure, applicable to the disaster recovery system 10 based on the redundant architecture provided by the present disclosure. As shown in Fig. 2, the disaster recovery method can include following steps.

[00136] In step S1, the master-site-state security subsystem 210 and the backup-site-state security subsystem 220 periodically communicate with each other and monitor the communication status of each other.

[00137] The master system 210 periodically transmits the master-site retention request to the backup system 220, and the backup system 220 returns an acknowledgment response permitting maintenance of the master site state upon receiving the master-site retention request; and the master system 210 maintains operation in the master site state upon receiving the acknowledgment response from the backup system 220.

[00138] In step S2, under a condition that it is monitored that the communication status is abnormal, the master-site-state security subsystem 210 and/or the backup-site-state security subsystem 220 is configured to transmit an arbitration request to the third-party arbitration platform 100.

[00139] The abnormal communication status includes failure to receive request/response and reception timeouts.

[00140] Under a condition that the master system 210 fails to receive the acknowledgment response, the master system 210 considers the backup system 220 may have a failure or the communication link is abnormal, and in this case, the master system 210 transmits a first arbitration request to the third-party arbitration platform 100 to request maintenance of the master site state.

[00141] Under a condition that the backup system 220 fails to receive a master system retention request, the backup system 220 considers that the master system 210 may have a failure or the communication link is abnormal, and in this case, the backup system 220 transmits a second arbitration request to the third-party arbitration platform 100 to request that it or another backup system be promoted to a new master system.

[00142] In step S3, the master-system-state computer 211 in the master-site-state security subsystem 210 executes a host task and perform data synchronization operations on other computers in the disaster recovery system 10, so that at least one computer that completes data

synchronization is in the hot-backup state.

[00143] In step S4, the third-party arbitration platform 100 determines, based on the arbitration request, whether to switch the master-site-state security subsystem 210 to an unavailable site state, and switch one of the at least one backup-site-state security subsystem
5 220 to the master site state, so that the master-system-state computer in the new master-site-state security subsystem takes over and executes the host task.

[00144] The disaster recovery method provided by this embodiment achieves real-time monitoring of each other's status through a periodic communication between the master system and the backup system. When a communication abnormality or a failure occurs, the security
10 subsystem can transmit the arbitration request to the third-party arbitration platform in time, so as to ensure the accuracy of a determination and switching of the master site state. Simultaneously, while executing the host task, the master system performs data synchronization with other computers in the backup system or in the disaster recovery system to keep them in the hot-backup state, so that rapid switching to a new master system is achieved
15 to make the new master system to continue to execute the task upon there is a failure in the master system, thereby enhancing the reliability, the fault tolerance, and the service continuity of the system in overall.

[00145] Some embodiments of the present disclosure provide a disaster recovery method based on a redundant architecture, applicable to multiple security subsystems in a disaster
20 recovery system. A method flow can include the following steps:

[00146] executing, by the master computer 211 in the master system 210, a host task and performing data synchronization operations on other computers in the disaster recovery system
10 so that at least one computer that completes data synchronization is in the hot-backup state;

[00147] establishing, by each security subsystem 200, periodic communication with other
25 security subsystems, and monitor communication status of other security subsystems; and

[00148] under a condition that it is monitored that the communication status is abnormal, transmitting an arbitration request to the third-party arbitration platform 100; and

[00149] according to the determination result of the third-party arbitration platform 100, either maintaining the current master site state to operate or executing an operation of switching
30 to the new master-site-state security subsystem, and after the switching is completed, taking over and executing, by the master-system-state computer in the new master-site-state security subsystem, the host task.

[00150] With the method provided in the embodiments of the present disclosure, when the

master system is operating normally, the master system can continuously process the host task and maintain data synchronization to keep other computers be in the hot-backup state, so as to ensure the takeover capability at any time. On such basis, periodic communication is established between security subsystems to monitor the communication status. Under a condition that there is an abnormality, the security subsystem transmits the arbitration request to the third-party arbitration platform in time, and the third-party arbitration platform uniformly determines whether to execute a master-backup switchover, so as to avoid system paralysis caused by a single point failure or a misjudgment.

[00151] Some embodiments of the present disclosure provide a disaster recovery method based on a redundant architecture, applicable to a third-party arbitration platform 100 in a disaster recovery system. The method flow can include the following steps:

[00152] receiving an arbitration request transmitted from at least one security subsystem, determining to maintain the master site state of a current master-site-state security subsystem or to switch one of the backup-site-state security subsystems to a new master-site-state security subsystem, and authorizing the master-system-state computer in the new master-site-state security subsystem to take over and execute the host task; and

[00153] returning the determination result to at least one security subsystem.

[00154] With the method provided in the embodiments of the present disclosure, after receiving the arbitration request from the security subsystem, the third-party arbitration platform performs centralized master/backup determination and returns the result to each security subsystem, achieving unified arbitration for maintaining the master system or switching of the backup system.

[00155] Fig. 3 illustrates a flowchart of a disaster recovery method based on a redundant architecture provided in some embodiments of the present disclosure.

[00156] It should be understood that the execution entities of solutions of the present disclosure include the master system 210, the backup system 220, and the third-party arbitration platform 100. The master system 210 and the backup system 220 maintain communicated connection through periodic interactions, and the third-party arbitration platform 100 serves as a unified determination and scheduling center and is configured to arbitrate and switch master/backup identity in scenarios of abnormal communication or failures.

[00157] It should also be understood that this embodiment primarily describes the communication verification process between the master system 210 and the backup system 220, as well as the arbitration processing and master/backup switching procedures when there is an

abnormality.

[00158] As shown in Fig. 3, the method can include the following steps.

[00159] In step S10, the master system 210 actively transmits a master-site retention request to the backup system 220.

5 **[00160]** In step S20, after receiving the master-site retention request, the backup system 220 transmits an acknowledgment response.

[00161] In step S21, under a condition that the backup system 220 fails to receive the master-site retention request or the receiving is timeout, it is regarded that the master system 210 is offline, transmits no response to the master system 210, and transmits a second arbitration request to the third-party arbitration platform 100.

[00162] In step S30, after receiving the acknowledgment response, the master system 210 maintains its master site state and continues normal operation.

[00163] In step S31, under a condition that the master system 210 fails to receive the acknowledgment response, the master system 210 transmits a first arbitration request to the third-party arbitration platform 100.

[00164] In step S40, according to a serial processing principle, the third-party arbitration platform 100 processes received arbitration requests in a sequence in which the requests are received.

20 **[00165]** In step S41, under a condition that the third-party arbitration platform 100 first receives the first arbitration request, the third-party arbitration platform 100 returns a response of maintaining the master site state.

[00166] In step S42, under a condition that the third-party arbitration platform 100 first receives the second arbitration request, the third-party arbitration platform 100 returns a response of switching to the new master system.

25 **[00167]** In step S50, after receiving the response of maintaining the master site system, the master system 210 continues operating in its current master site state.

[00168] For example, after maintaining normal operation, the master system 210 establishes periodic arbitration communication with the third-party arbitration platform 100 to maintain its master site state to continue operating without being interfered, and the backup system 220 switches to an unavailable state or an offline state.

30 **[00169]** In step S60, after receiving the response of switching to the new master system, the backup system 220 is upgraded to the master system, and the master take is taken over and executed by its master computer.

[00170] For example, after being upgraded to the master system, the backup system 220 maintains the master site state through periodic arbitration communication with the third-party arbitration platform 100 without being interfered, and the original master system 210 switches to an unavailable state or an offline state.

5 **[00171]** With the above embodiments, the present disclosure maintains stable operation of the master system during normal communication between the master system and the backup system, and under a condition that there is abnormal communication or a failure, the master system or the backup system initiates the arbitration request to the third-party arbitration platform in time, and the third-party arbitration platform makes centralized determination and
10 issues the results according to an information serial processing principle. In this way, conflicts and inconsistencies that may be caused by independent judgment of a signal subsystem are avoided, ensuring the timeliness, fairness, and consistency of the master-backup switching. Meanwhile, the new master system after switching seamlessly takes over the host task, significantly enhancing the reliability, the fault tolerance, and the service continuity of the
15 disaster recovery system in failure scenarios.

[00172] In an embodiment, a platform periodic operation primary-task, a local master/backup voting task, and a master/backup site voting task are deployed on each computer in each security subsystem.

[00173] The platform periodic operation primary-task is configured to simultaneously
20 trigger the local master/backup voting task and the master/backup site voting task to be executed in each platform cycle.

[00174] The local master/backup voting task is configured to perform local master-backup voting among multiple computers in a same security subsystem, and determine that each computer belongs to the master-system-state computer or the backup-system-state computer to
25 obtain a local master-backup voting result.

[00175] It should be understood that in the local master/backup voting task, multiple computers in the same security subsystem are configured to:

[00176] communicate with each other via the local master/backup voting task to update their master-backup system states; and

30 **[00177]** under a condition of abnormal communication, switch at least one computer in a master system state in the security subsystem to an unavailable state, and switch at least one computer in a backup system state in the security subsystem to the master system state.

[00178] Specifically, the functions performed by the master-system-state computer and the

backup-system-state computer in the local master/backup voting task refer to the communication process in the security subsystem described in the preceding embodiments, that is, the master-backup voting solution between the computers in the subsystem through the “master-system retention request”, which will not be repeated herein.

5 **[00179]** The master/backup site voting task is configured to cause the master-site-state security subsystem and the backup-site-state security subsystem to: communicate with each other in each platform cycle, monitor the communication status of each other, and transmit the arbitration request to the third-party arbitration platform under a condition that it is monitored that the communication status is abnormal, so as to obtain a master-backup site voting result.

10 **[00180]** It should be understood that the functions performed by the security subsystem in the master site state, the security subsystem in the backup site state, and the third-party arbitration platform in the master/backup site voting task refer to the preceding embodiments, that is, the master-backup voting solution between the security subsystems through the “master-site retention request”, which will not be repeated herein.

15 **[00181]** The platform periodic operation primary-task is configured to acquire the local master-backup voting result from the local master/backup voting task, acquire the master-backup site voting result from the master/backup site voting task, cause a current computer that is determined as the master-system-state computer in the master site state based on the local master-backup voting result and the master-backup site voting result, to execute the host task,
20 and perform data synchronization operation on other computers in the disaster recovery system, so that at least one of the other computers that completes data synchronization is in the hot-backup state.

25 **[00182]** In this embodiment, the platform periodic operation primary-task is uniformly deployed on all computers and synchronously trigger the local master/backup voting task and the master/backup site voting task in each platform cycle, so that the determination of master-backup relationships and state confirmation can be completed simultaneously in and across subsystems, thereby ensuring timely detection of and initiation of arbitration under abnormal conditions to guarantee the correctness and consistency of the master-backup switching. Furthermore, when the current computer is determined to as the master-system computer in the
30 master site state according to the voting result, this computer can immediately take over the host task and perform data synchronization on other computers, so as to place relevant computers into the hot-backup state to achieve rapid takeover and seamless disaster recovery switching, thereby enhancing the reliability and the fault tolerance of the system.

[00183] Fig. 4 is an interaction flowchart of task execution sequences provided in some embodiments of the present disclosure.

[00184] It can be seen from Fig. 4, during operation of the disaster recovery system in this embodiment, the disaster recovery system executes the platform periodic operation primary-task (300 ms), the local master/backup voting task (50 ms), and the master/backup site voting task (50 ms). At the start of each system cycle, the platform periodic operation primary-task triggers these three tasks to be executed in parallel. During this period, the computers interact through periodic status information, voting information, and arbitration request/response messages (REQ_MASTER/RES_ALLOWED) to achieve cross-computer and cross-system consistency and fault tolerance.

[00185] Specifically, upon reaching the cycle start point, the platform periodic operation primary-task triggers all three tasks to operate simultaneously. During this process, the master computer and the backup computer in the master system periodically and actively transmit status information to communicate with each other. Additionally, the master system and the backup system exchange status messages to maintain consistency. On the third-party arbitration platform, the master computer in the master system periodically reports and transmits a master control request (REQ_MASTER), and the backup computer or other system computers response (RES_ALLOWED). If conditions are met, the master computer is permitted to continue as a master controller. If an abnormality is detected, the arbitration mechanism can switch the master role and the backup role. It should be noted that the communication verification and abnormal arbitration steps for the master system and the backup system have been introduced in detail in the embodiments shown in Fig. 3 and Fig. 4. The corresponding sections in Fig. 4 will not be repeated herein and can refer to the aforementioned embodiments to understand their specific implementation methods and operation flows.

[00186] It can be seen from Fig. 4, the operational logic of the disaster recovery system in this embodiment is divided into different micro-cycles, i.e., input micro-cycle, application micro-cycle, output micro-cycle, and idle micro-cycle.

[00187] During the input micro-cycle, communication data reception and I/O data collection are completed; master-backup synchronization is performed on the collected input data to ensure data consistency between the master system and the backup system; and security protocol parsing is performed on input data, thereby providing a reliable data source for the application micro-cycle.

[00188] During the application micro-cycle, application logic processing is executed based

on data provided in the phase of the input micro-cycle, which includes performing, by an application software, corresponding logical operations on the input data, transmitting the processed output data to a platform software in queue format, and performing secure protocol packaging on output data to ensure transmission security.

5 **[00189]** During the output micro-cycle, whether to output data outside is determined according to a master-backup state, which includes: acquiring a master-backup system information of a current computer from the master-backup voting task, acquiring the master-backup state of the current computer from the local master/backup voting task, outputting data outside under a condition that the current computer is a master computer in the master system,
10 and not outputting data outside under a condition that the computer is not the master computer in the master system, thereby ensuring consistency and security of the disaster recovery system.

[00190] The idle micro-cycle is primarily configured to maintain synchronization and status update of double computers, which includes completing periodic time synchronization of double computers; mutually transmitting, by two computers, the master-backup state of the
15 current system and related information of the master and backup computers; completing master-backup state switching based on received information; upgrading the backup computer to the master computer under a condition that at least three lines of the four-line communication each are disconnected, and entering a follow-up state under a condition the case where at least three lines of the four-line communication each are disconnected does not occur; updating a
20 master-backup follow-up state of the current computer and notifying the platform periodic operation primary-task; and setting an operating cycle of the idle micro-cycle to 50 ms.

[00191] With this embodiment, communication status detection and data synchronization of double computers can be completed during the input micro-cycle and the idle micro-cycle, so as to ensure data consistency between the master system and the backup system. Furthermore,
25 in cases of abnormal communication or voting failures, the master system, the backup system, and the third-party arbitration platform jointly determine the master control identity, thereby avoiding conflicts caused by a single point failure. In addition, the backup computer is rapidly upgraded to the master computer and takes over the tasks through a master-backup switching and the determination of the third-party arbitration platform, so as to ensure continuous
30 operation of the system, thereby enhancing the reliability, the fault tolerance, and the service continuity of the disaster recovery system and achieving high availability and security of the master system and the backup system.

[00192] Fig. 5 is a flowchart of executing data and time synchronization provided in some

embodiments of the present disclosure.

[00193] At the start of the host task cycle, the master computer in the master system actively transmits a 1588 time synchronization request (SYNC_1588 message) to the master computer in the non-master system. Apart in a dashed-line box in Fig. 5 presents a standard 1588 precision time protocol (PTP) message exchange process. The master computer in the non-master system employs a two synchronization method, i.e., twice message exchanges and timestamp comparisons, which can precisely estimate and correct clock errors to maintain high-precision synchronization with the master computer in the master system. The process briefly includes: transmitting, by the master computer in the master system, a synchronization message (SYNC) at time T1; recording, by the master computer in the non-master system, a reception time T2 upon receiving this message; then transmitting, by the master computer in the master system, a follow-up message (Follow_Up) carrying a precise transmission time T1; actively transmitting, by the master computer in the non-master system, a delay request message (Delay_Req) to the master computer in the master system at a local time T3; recording, by the master computer in the master system, a time T4 upon receiving Delay_Req, and transmitting a delay response message (Delay_Resp) to inform the master computer in the non-master system of T4; and calculating, by the master computer in the non-master system, a round-trip delay and an offset of its local clock relative to the master computer using the four timestamps (T1, T2, T3, T4), and adjusting its local clock according to the round-trip delay and the offset to achieve alignment.

[00194] The master computers in the non-master systems include the backup computer in the master system (the computer B at site A), the master computer in the backup system (the master computer A at site B), and the backup computer in the backup system (the computer B at site B). After receiving a time synchronization request, the master computers in the non-master systems sequentially performs offset calculation, delay compensation, and time calibration operations to correct their local clocks, so that their local clocks is in consistency with the master computer in the master system. After completing time synchronization, the master computers in the non-master systems return completion flags and enter a time synchronization completed state.

[00195] After one master computer in the non-master system completes time synchronization, the master computer in the master system periodically issues data synchronization instructions to this computer via a user datagram protocol (UDP) channel. As shown in the figure, the master computer in the master system generates a cycle start flag

(T_cycleStart) at the beginning of its own cycle and transmits a data synchronization message through the UDP channel to the master computer in the non-master system and the message includes a start flag for the current cycle, and status information. After receiving the UDP broadcast message, the master computer in the non-master system updates its local cycle counter based on the T_cycleStart information in the UDP broadcast message, and have a same data processing rhythm with the master computer in the master system. Under a condition that there is data abnormality, detection is performed through a CRC verification mechanism. Through periodic UDP broadcasts, the master computer in the master system ensures that the master computer in the non-master system perform computation at a same cycle start point, thereby achieving synchronization in data processing and task scheduling. After receiving the data synchronization instruction, the computer enters a data follow-up state in which comparison and update of status data and task data are executed to progressively transit itself into the hot-backup state. Once the master computer in the non-master system confirms that this computer has completed data synchronization and successfully entered the hot-backup state, the master computer in the non-master system rejects the data follow-up request from this computer, so as to avoid repeated synchronization, thereby enhancing the communication and processing efficiency of the system.

[00196] With this embodiment, precise time synchronization and data synchronization are achieved, ensuring that the clock of the master computer in the non-master system keeps consistent with the master computer in the master system in the host task cycle. In this way, a reliable time reference is provided for subsequent data synchronization. During the data synchronization phase, each master computer in the non-master system achieves a smooth transition from the follow-up state to the hot-backup state by progressively comparing and updating status data and task data, ensuring data consistency between the master system and the backup system. Meanwhile, the master computer in the master system stops issuing synchronization request after confirming that the data synchronization is complete, so as to avoid repeated operations, thereby enhancing the communication efficiency and processing performance of the system.

[00197] Fig. 6 illustrates a hardware schematic diagram of an electronic device provided in some embodiments of the present disclosure.

[00198] The electronic device can include a processor 7001 and a memory 7002 storing computer program instructions.

[00199] Specifically, the processor 7001 can include a central processing unit (CPU), an

application specific integrated circuit (ASIC), or one or more integrated circuits configured to implement one or more embodiments of the present disclosure.

[00200] The memory 7002 can include a large-capacity storage device for data or instructions. For example, without limitation, the memory 7002 can include a hard disk drive (HDD), a floppy disk drive, a flash memory, an optical disk, a magneto-optical disk, a magnetic tape, or a universal serial bus (USB) drive, or a combination of two or more of the above. In an embodiment, the memory 7002 can include removable or non-removable (or fixed) media, or the memory 7002 can be non-volatile solid-state memory. The memory 7002 can be located inside or outside an integrated network gateway disaster recovery device.

[00201] In an example, the memory 7002 can be a read only memory (ROM). In an example, the ROM can be a mask-programmed ROM, a programmable ROM (PROM), an erasable PROM (EPROM), an electrically erasable PROM (EEPROM), an electrically alterable ROM (EAROM), a flash memory, or a combination of two or more of the above.

[00202] The processor 7001 implements the disaster recovery method based on the redundant architecture shown in the embodiments of Fig. 2 by reading and executing the computer program instructions stored in the memory 7002.

[00203] In an example, the electronic device can include a communication interface 7003 and a bus 7004. As shown in Fig. 6, the processor 7001, the memory 7002, and the communication interface 7003 are connected to each other via the bus 7004 to communicate with each other.

[00204] The communication interface 7003 is primarily configured to realize communication between various modules, devices, units, and/or equipments in the embodiments of the present disclosure.

[00205] The Bus 7004 includes a hardware, a software, or both and couples components of online data traffic metering equipment. For example, but not limited to, the bus can include an accelerated graphics port (AGP) or other graphics bus, an extended industry standard architecture (EISA) bus, a front side bus (FSB), a hyper transport (HT) interconnect, an industry standard architecture (ISA) bus, an unlimited bandwidth interconnect, a low pin count (LPC) bus, a memory bus, a micro channel architecture (MCA) bus, a peripheral component interconnect (PCI) bus, a PCI-express (PCI-X) bus, a serial advanced technology attachment (SATA) bus, a video electronics standards association local bus (VLB), or other suitable buses, or combinations of two or more of the above. Where appropriate, the bus 7004 can include one or more buses. Although specific buses are described and illustrated in the embodiments of the

present disclosure, any suitable bus or interconnect is taken into account.

[00206] In addition, in conjunction with the disaster recovery method based on the redundant architecture described in the above embodiments, some embodiments of the present disclosure can provide a computer storage medium to implement the method. The computer storage medium stores computer program instructions, and when executed by a processor, the computer program instructions implement any of the disaster recovery methods based on the redundant architecture described in the above embodiments.

[00207] The present disclosure also provides a computer program product including computer programs, which when executed by a processor, implement any of the disaster recovery methods based on the redundant architecture described in the above embodiments.

[00208] It should be clear that the present disclosure is not limited to the specific configurations and processing described above and illustrated in the figures. For the sake of brevity, detailed descriptions of known methods have been omitted herein. In the above embodiments, several specific steps are described and illustrated as examples. However, the method process of the present disclosure is not limited to the described and illustrated specific steps. Those skilled in the art, upon understanding the spirit of the present disclosure, can make various changes, modifications, and additions, or alter the order of the steps.

[00209] The functional blocks illustrated in the above structural block diagram can be implemented as hardware, software, firmware, or a combination thereof. When implemented as hardware, it can be, for example, an electronic circuit, an application specific integrated circuit (ASIC), appropriate firmware, a plug-in, a function card, etc. When implemented as software, the elements of the present disclosure are programs or code segments used to perform the required tasks. The programs or code segments can be stored on a machine-readable medium or transmitted on a transmission medium or communication link via data signals carried by a carrier. "Machine-readable medium" can include any medium capable of storing or transmitting information. Examples of machine-readable medium include electronic circuits, semiconductor memory devices, read-only memory (ROM), flash memory, erasable read only memory (EROM), floppy disks, compact disc read-only memory (CD-ROM), optical discs, hard disks, fiber optic media, radio frequency (RF) links, and the like. Code segments can be downloaded via computer networks such as the Internet or intranets.

[00210] The flowcharts and/or block diagrams of the methods, apparatus (systems), and computer program products according to the embodiments of the present disclosure described above illustrate various aspects of the present disclosure. It should be understood that each box

in the flowcharts and/or block diagrams, as well as combinations of boxes in the flowcharts and/or block diagrams, can be implemented by computer program instructions. These computer program instructions can be provided to a processor of a general-purpose computer, a dedicated computer, or other programmable data processing apparatus to produce a machine, so that the instruction executed by the processor of the computer or other programmable data processing apparatus can realize the functions/actions specified in one or more boxes of the flowchart and/or block diagram. Such processor can be, but is not limited to, a general-purpose processor, a dedicated processor, a special application processor, or a field programmable logic circuit. It is also understood that each block in the block diagram and/or flowchart, as well as combinations of blocks in the block diagram and/or flowchart, can also be implemented by dedicated hardware performing the specified function or action, or by a combination of dedicated hardware and computer instructions.

[00211] The foregoing describes specific embodiments of the present disclosure. Those skilled in the art can clearly appreciate that, for the sake of description and brevity, the specific operational processes of the systems, modules, and units described above can refer to the corresponding processes in the preceding method embodiments and are not repeated herein. It should be understood that the protection scope of the present disclosure is not limited to the above. Any person skilled in the art can readily conceive various equivalent modifications or replacements in the scope of the disclosed technology, and such modifications or replacements should fall within the protection scope of the present disclosure.

What is claimed is:

1. A disaster recovery system based on a redundant architecture, comprising:
a third-party arbitration platform; and
a plurality of security subsystems,

5 wherein the third-party arbitration platform and the plurality of security subsystems are deployed at different geographic locations;

every two of the third-party arbitration platform and the plurality of security subsystems are connected to each other via dual-channel communication;

the plurality of security subsystems comprise a master-site-state security subsystem and
10 at least one backup-site-state security subsystem and each comprise a plurality of computers, every two of the plurality of computers being connected to each other via a dual-channel communication, and the plurality of computers comprising a master-system-state computer and at least one backup-system-state computer;

the master-system-state computer in the master-site-state security subsystem is configured
15 to execute a host task and perform data synchronization operation on other computers in the disaster recovery system, so that at least one of the plurality of computers that completes data synchronization is in a hot-backup state;

in each platform cycle, the master-site-state security subsystem and the at least one backup-site-state security subsystem are configured to communicate with each other and
20 monitor a communication status of each other;

under a condition that it is monitored that the communication status is abnormal, at least one of the master-site-state security subsystem or the at least one backup-site-state security subsystem is configured to transmit an arbitration request to the third-party arbitration platform;
and

25 the third-party arbitration platform is configured to, upon receiving the arbitration request, determine whether to switch the master-site-state security subsystem to an unavailable site state and switch one of the at least one backup-site-state security subsystem to a master site state, so that the master-system-state computer in the new master-site-state security subsystem takes over and executes the host task after the switching.

30 2. The disaster recovery system according to claim 1, wherein

the master-site-state security subsystem is configured to transmit a master-site retention request to the at least one backup-site-state security subsystem and monitor an

acknowledgment response from the at least one backup-site-state security subsystem, and transmit a first arbitration request to the third-party arbitration platform under a condition that the master-site-state security subsystem fails to receive the acknowledgment response, the first arbitration request being configured to request the master-site-state security subsystem to maintain the master site state; and

the at least one backup-site-state security subsystem each is configured to receive the master-site retention request transmitted from the master-site-state security subsystem, and transmit a second arbitration request to the third-party arbitration platform under a condition that the backup-site-state security subsystem fails to receive the master-site retention request, the second arbitration request being configured to request the backup-site-state security subsystem to switch to the new master-site-state security subsystem.

3. The disaster recovery system according to claim 2, wherein the third-party arbitration platform is configured to:

return a first arbitration response to the master-site-state security subsystem only upon receiving the first arbitration request, the first arbitration response being configured to confirm maintaining the master site state of the master-site-state security subsystem;

upon receiving only the second arbitration request, return a second arbitration response to the at least one backup-site-state security subsystem, the second arbitration response being configured to control one of the at least one backup-site-state security subsystem to switch to the new master-site-state security subsystem and authorize the master-system-state computer in the new master-site-state security subsystem to take over and execute the host task; and

upon receiving both the first arbitration request and the second arbitration request, process the first arbitration request and the second arbitration request sequentially in a sequence in which the first arbitration request and the second arbitration request are received.

4. The disaster recovery system according to claim 3, wherein under a condition that the master-site-state security subsystem receives the first arbitration response and maintains to operate in the master site state or the backup-site-state security subsystem receives the second arbitration response and switches to the new master-site-state security subsystem,

the master-site-state security subsystem or the new master-site-state security subsystem is configured to: periodically transmit the master-site retention request to the third-party arbitration platform, monitor an acknowledgment response from the third-party arbitration

platform, and maintain the master site state upon receiving the acknowledgment response from the third-party arbitration platform; and

the third-party arbitration platform is further configured to receive the master-site retention request transmitted from the master-site-state security subsystem or the new master-site-state security subsystem and return the acknowledgment response.

5. The disaster recovery system according to any one of claims 1 to 4, wherein

a platform periodic operation primary-task, a local master/backup voting task, and a master/backup site voting task are deployed on each of the plurality of computers in each of the plurality of security subsystems;

the platform periodic operation primary-task is configured to simultaneously trigger the local master/backup voting task and the master/backup site voting task to be executed in each platform cycle;

the local master/backup voting task is configured to perform local master-backup voting among the plurality of computers in a same one of the plurality of security subsystems, and determine that each of the plurality of computers belongs to the master-system-state computer or one of the at least one backup-system-state computer to obtain a local master-backup voting result;

the master/backup site voting task is configured to cause the master-site-state security subsystem and the at least one backup-site-state security subsystem to: communicate with each other in each platform cycle, monitor the communication status of each other, and transmit the arbitration request to the third-party arbitration platform under a condition that it is monitored that the communication status is abnormal, so as to obtain a master-backup site voting result; and

the platform periodic operation primary-task is configured to acquire the local master-backup voting result from the local master/backup voting task, acquire the master-backup site voting result from the master/backup site voting task, cause a current computer that is determined as the master-system-state computer in the master-site-state security subsystem based on the local master-backup voting result and the master-backup site voting result, to execute the host task, and perform data synchronization operation on other computers in the disaster recovery system, so that at least one of the other computers that completes data synchronization is in the hot-backup state.

6. The disaster recovery system according to claim 5, wherein the plurality of computers in a same one of the plurality of security subsystems are further configured to:

communicate with each other via the local master/backup voting task to update their master-backup system states; and

5 under a condition of abnormal communication, switch at least one of the plurality of computers in a master system state in the security subsystem to an unavailable state, and switch one of the plurality of computers in a backup system state in the security subsystem to the master system state.

10 7. The disaster recovery system according to any one of claims 1 to 4, wherein the plurality of computers in a same one of the plurality of security subsystems are further configured to:

mutually transmit master-system promotion requests after successful self-checks; and

among at least two of the plurality of computers that return response results for the master-system promotion requests from other computers, determine the master-system-state computer
15 and the at least one backup-system-state computer based on a first priority sequence.

8. The disaster recovery system according to any one of claims 1 to 4, wherein the plurality of security subsystems are further configured to:

mutually transmit master-site promotion requests; and

20 among at least two of the plurality of security subsystems that return response results for the master-site promotion requests from other security subsystems, determine the master-site-state security subsystem and the at least one backup-site-state security subsystem based on a second priority sequence.

25 9. The disaster recovery system according to claim 8, wherein

the disaster recovery system comprises two security subsystems, and

one of the two security subsystems is further configured to, under a condition that no response result for the master-site promotion request is received from the other one of the two security subsystems, transmit the master-site promotion request to the third-party arbitration
30 platform, receive a response result returned by the third-party arbitration platform, and switch to the master-site-state security subsystem.

10. A disaster recovery method based on a redundant architecture, applicable to a disaster recovery system, wherein

the disaster recovery system comprises a third-party arbitration platform and a plurality of security subsystems, wherein the third-party arbitration platform and the plurality of security subsystems are deployed at different geographic locations; every two of the third-party arbitration platform and the plurality of security subsystems are connected to each other via a dual-channel communication; the plurality of security subsystems comprise a master-site-state security subsystem and at least one backup-site-state security subsystem and each comprise a plurality of computers, every two of the plurality of computers being connected to each other via a dual-channel communication, and the plurality of computers comprising a master-system-state computer and at least one backup-system-state computer; and

the disaster recovery method comprises:

executing, by the master-system-state computer in the master-site-state security subsystem, a host task, and performing data synchronization operation on other computers in the disaster recovery system, so that at least one of the plurality of computers that completes data synchronization is in a hot-backup state;

in each platform cycle of the host task, communicating, by the master-site-state security subsystem and the at least one backup-site-state security subsystem, with each other and monitoring a communication status of each other;

under a condition that it is monitored that the communication status is abnormal, transmitting, by at least one of the master-site-state security subsystem or the at least one backup-site-state security subsystem, an arbitration request to the third-party arbitration platform; and

upon receiving the arbitration request, determining, by the third-party arbitration platform, whether to switch the master-site-state security subsystem to an unavailable site state, and switching one of the at least one backup-site-state security subsystem to a master site state, so that the master-system-state computer in the new master-site-state security subsystem takes over and executes the host task after the switching.