

sia RECS

RTGS Extreme Contingency Service

sia RECS

RTGS Extreme Contingency Service

RTGS: a mission critical system

RTGS is a mission critical system: its resilience is one of the key objectives of Central Banks.

The RTGS system is the heart of the country economy and, as such, in case of a severe disaster, it should be taken back to operation as soon as possible.

Nowadays there's a consolidated certainty that a severe malfunction of financial systems can lead to dramatic consequences in the economy of a country. The unavailability of the payment system infrastructure for a long period can create additional turmoil in the financial sector making difficult for a Central Bank keeping the economy under control.

In case of major disaster (application failure due to a malicious attack, network failure on both primary and disaster recovery links, natural or accidental disaster, terroristic attack), the rapidity of restarting the financial system is crucial to limit the country economy downfall and restart the core business operations.

A major disaster can also involve 3rd site installation if within the country and it can jeopardise completely disaster recovery procedures.

All Central Banks have at least two sites (primary and disaster recovery

site) with a nearly real-time recovery architecture and some have a 3rd cold site in case of severe disaster. More and more Central Banks are taking into consideration the cost/benefit opportunity to have a 3rd disaster recovery site to be used in extreme contingency situation.

The main **characteristics** of such 3rd site solution must be:

- :: long distance from the primary and secondary sites preferably in a different country
- :: highly secure and reliable hosting premises
- :: quick recovery of basic RTGS functionalities
- :: functional flexibility of the RTGS service offered: from basic to full fledged RTGS system in case of a long service outage of the main sites
- :: affordable cost.

sia RECS

Looking to the possibility to be in a situation of a severe disaster there are two main topics a mission critical operator should take into consideration:

- :: **take a bigger picture:** a business continuity plan needs to look further than the immediate emergency, taking into account what will be required to get the business running

as soon as possible

- :: **distance is vital:** when a company has disaster recovery sites and alternative locations for its technology and people, these sites need to be a significant distance apart. In the case of any incident occurring that affects an entire suburb for an extended period, the business needs to ensure it is able to resume operations in a location that is not suffering the same problem. It is not only technology and buildings an Institution needs to take into consideration. People are crucial to the running of a company and there must be a mechanism in place to deal with injuries and general confusion in a disaster zone, as well as see that critical tasks are undertaken by alternative employees or by staff from a third-party service provider in a 3rd site.

The sia RTGS Extreme Contingency Service (sia RECS) has the objective to provide Central Banks with a RTGS contingency service that can function as 3rd site in case of severe disasters.

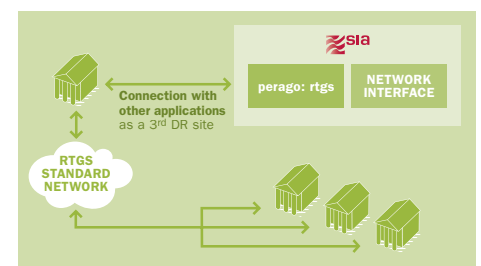
sia RECS is aiming to service the Central Banks facing a disaster covering with a wide number of possible scenarios

1. RTGS application unavailable or not working properly

The application is not working properly due to a malicious intervention or other application errors.

In this scenario it is assumed that the same problem is mirrored in the disaster recovery site causing the total disruption of the local RTGS operations.

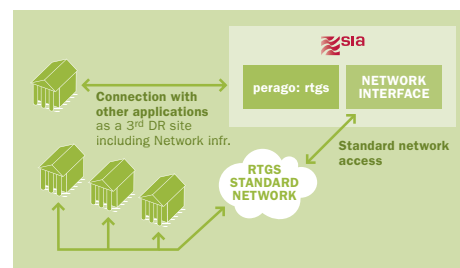
The other ancillary Central Bank's applications (like general ledger, collateral system, ...) as well as the other IT architecture components are still up and running.



2. RTGS Application and Central Bank's Network Infrastructure Gateways unavailable

The RTGS system and the Central Bank's Network Infrastructures Gateways (Swift or VPN) are not working properly (both production and disaster recovery). In this scenario it is assumed that the same problem is mirrored in the disaster recovery site causing the total disruption of the local RTGS operations and the Central Bank Swift Gateways.

The other ancillary Central Bank's applications as well as the other IT architecture components are still up and running.

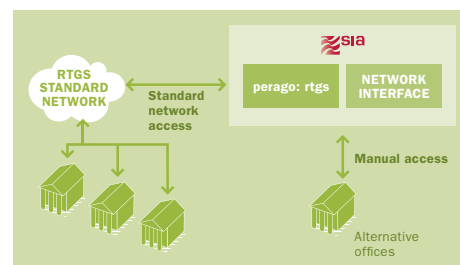


3. Central Bank's IT premises unavailable (including/excluding offices)

Central Bank's IT premises (production and disaster recovery) have been heavily damaged by a natural/accidental disaster or by an intentional attack.

In this scenario it is assumed that both primary and secondary site are no more available possibly including the entire premises.

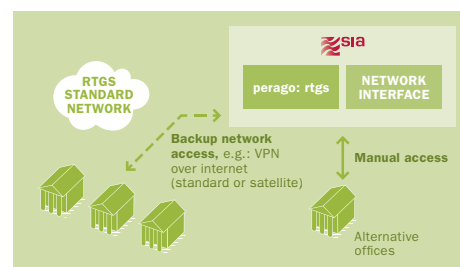
Every component outside the Central Bank (network, participant's sites) is still working.



4. Central Bank's IT premises and Network unavailable

Central Bank's IT premises (production and disaster recovery) and the network have been heavily damaged by a natural/accidental disaster or by an intentional attack. In this scenario it is assumed that Central Bank's primary and secondary site and the domestic network are no more available.

Every component at Participant's site are still working.

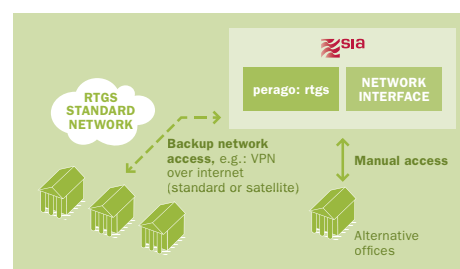


5. Central Bank's premises and some commercial banks' premises unavailable

A disaster destroys part of the main city. In this scenario it's assumed that most of the national financial infrastructure is not more available including:

- :: both Central Bank's primary and secondary site
- :: participant bank's head quarters
- :: domestic networks

Only some Central Bank's personnel and participant's disaster recovery offices in other regions are still operational. The sia RECS features will vary depending on the scenario the Central Bank is aiming to address.



sia RECS Main features

Knowledge

the fact that sia RECS is based on current SIA capabilities is strongly reducing the risk for the Central Bank to entrust SIA for the 3rd site management.

SIA is currently both an RTGS product and mission critical service leading provider. It has a well established Swift Service Bureau, a Swift like European VPN with 100% SLA, and a dedicated Central Bank's help desk currently in operation

Service Flexibility

Capability to adapt to diverse Central Bank business continuity requirements with different SLA's (i.e. few hours recovery time; few days time to normality) thanks to the advanced data center and help desk processes

Functional Flexibility

Availability of basic RTGS functions as well as sophisticated ones; scenario driven synchronisation level (i.e. system configuration, static data, participant settlement position and payment message alignment); STP and web participant and/or central bank access

Reliability

Strong HW, SW, network building and process reliability

Pricing

Flexible and affordable prices sia RECS is based on the state of the art perago:rtgs solution hosted at the highly secure and highly reliable SIA datacenter.

In addition, sia RECS will use the 24x7 SIA-Help desk service for Central Banks, a dedicated and experienced team of people that is already supporting live RTGS customers.

SIA S.p.A.
Via Francesco Gonin, 36 - 20147 Milano
Tel. +39.02.6084.1
info@sia.eu
www.sia.eu

