Enhancing the resilience of the Bank of England's Real-Time Gross Settlement infrastructure

By Ed Kelsey and Simon Rickenbach of the Bank's Market Services Division.[1]

- The Bank of England operates the United Kingdom's Real-Time Gross Settlement (RTGS) infrastructure for the settlement of the main electronic sterling payment systems. This infrastructure plays a vital role in the safe functioning of the UK financial system, and therefore in maintaining financial stability.
- The Bank continuously seeks to improve the resilience of its infrastructure. Recently, enhancement of the resilience of payment infrastructure has become a higher priority for central banks.
- The Bank, together with other central banks, worked with SWIFT to develop a new RTGS contingency infrastructure with which to settle payments should the principal infrastructure become unavailable. The Bank is the first central bank to adopt this contingency solution.

Introduction

Electronic payments and central banks

The ability to make electronic payments underpins the functioning of a modern economy. In the United Kingdom over 98% of sterling payments by value are made electronically. Such payments are used by individuals to buy goods, by companies to pay salaries, by the government to pay for public services, and by banks to make transfers to one another.

In the United Kingdom, electronic payments can be made through a number of payment systems, such as CHAPS — the United Kingdom's same-day, high-value payment system — or the Faster Payments Service, which allows retail payments to be made throughout the day, all year round. At their most basic level, all payment systems involve the transfer of funds from one entity to another.

The range of IT infrastructure that supports these payment systems must be highly resilient, since an infrastructure failure could greatly inhibit — or remove entirely — the ability of individuals and firms to make their payments. This would have severe consequences for economic activity.

In the United Kingdom, the Bank of England provides critical functionality through its role as a 'settlement agent' to allow direct participants in payment systems to settle their interbank payment obligations in central bank money.[2] The Bank operates the Real-Time Gross Settlement (RTGS) infrastructure that acts as the accounting database for participants in the main sterling payment systems. The RTGS infrastructure also holds the central bank reserves balances for the banking sector.[3]

The Bank's RTGS infrastructure accommodates two models of interbank settlement. The first is RTGS, where payment instructions are exchanged and settled in real time on a gross basis throughout the business day. CHAPS uses this model. The second is the periodic settlement of net obligations at the end of a 'clearing cycle', known as deferred net settlement (DNS). Retail payment systems, such as Bacs and Faster Payments, use this model. The disadvantage of the DNS model is that it leaves obligations owed to the recipient bank unfulfilled until settlement occurs. This could result in a loss if the paying bank were to default before net settlement had been completed. This risk can be mitigated by, for example, requiring banks to collateralise these exposures — as occurs in the Bacs and Faster Payments systems.

(1) The authors would like to thank Robert Maclean for his help in producing this article.
(2) Dent and Dison (2012) describe this in detail.
(3) As of July 2014, the approximate value of reserves was £300 billion. See the *Bankstats* page (data file A1.1.1), available at www.bankofengland.co.uk/statistics/Pages/bankstats/default.aspx.

The importance of RTGS to the UK economy

RTGS infrastructure performs a role in the settlement of the vast majority of electronic payments made by the UK population. The Bank, therefore, provides this service as part of its financial stability objective. The Bank seeks to make its infrastructure as reliable as possible, targeting RTGS availability of 99.95% of its defined operating hours. It has achieved 100% availability for the past four years.

As the provider of the infrastructure for CHAPS payment processing, the Bank's financial stability objective is aligned with the objectives of CHAPS as a payment system. Since 2012, the internationally agreed 'Principles for financial market infrastructures' have set out the standards which are considered best practice for high-value payment systems and their critical suppliers. These principles include the expectation that a critical service provider's disaster recovery plans should support 'the timely resumption of critical services in the event of an outage'.(1)

To ensure that payments can continue to be settled safely and efficiently the Bank, like other central banks, continuously seeks to improve the resilience of its RTGS infrastructure against outright failures. In February 2014, the Bank introduced the 'Market Infrastructure Resiliency Service' (MIRS) as an additional contingency infrastructure that could be used in the event of a failure of its principal RTGS infrastructure. This ensures that banks can continue to settle CHAPS payments in the event of a disruption without resorting to a DNS model. MIRS also facilitates the net interbank settlement of the retail schemes.

This short article explains this recent improvement in the resilience of RTGS infrastructure. The article begins by explaining the drivers behind the need for improved contingency, before evaluating the key requirements defined by the central bank community for a contingency RTGS infrastructure, which resulted in the development of MIRS.

Why central banks require contingency for their RTGS infrastructures

The Bank operates its principal RTGS infrastructure from two sites in the London region. If the live site should become unavailable, RTGS can continue to operate from the standby site. The standby site duplicates the hardware and software of the live site and operators are present to control the system from both sites throughout each business day. Transactions between RTGS accounts applied to the live database are automatically copied to the standby database at the other location in real time.

However, it is conceivable that both sites could become unavailable at the same time. Environmental factors leading to an inability to physically operate at a site, or IT hardware failures, could cause two simultaneous but unrelated problems. Alternatively, and perhaps more likely, there could be a software failure which creates a single problem that affects both sites. Such an event resulted in a six-hour service interruption to the Bank's RTGS infrastructure on 12 February 2007. More recently, public authorities and commercial institutions have needed to consider the risks to their systems arising from an external cyber attack.

While the loss of both sites is very unlikely, it would have a severe impact due to the critical role of the RTGS infrastructure in the safe functioning of the UK financial system. For this reason, continually developing improved resilience, including contingency procedures, is an important feature of any central bank's role in the provision of RTGS infrastructure.

Since the introduction of the Bank's RTGS infrastructure in 1996, and prior to adopting MIRS, a dual site failure would have caused an inability to settle CHAPS payments individually and in real time. Instead, the contingency solution was to settle the net obligations between banks arising in CHAPS at the end of the day, using a DNS model.(2)

In those circumstances, as settlement of payment obligations would not have occurred in real time, CHAPS direct participants would have incurred the **credit risk** associated with settling under an uncollateralised DNS model. Furthermore, there would have been significant **operational risk**, as it would have been difficult to establish exactly which payments had been processed at the point of failure.

Drivers for the Bank to improve its contingency

The Bank had been aware of the benefits of mitigating these risks, but three key factors have emerged over the past five years that have led to a renewed focus to address them through improving RTGS infrastructure contingency procedures:

(i) Central banks have become more concerned with identifying and mitigating tail risks to financial stability. The financial crisis highlighted the need to address the risks of low probability, but high-impact, events. Had the Bank's RTGS infrastructure faltered during a significant market stress event, such as the failure of Lehman Brothers, the crisis could have been greatly exacerbated.(3) As a result there has been a drive from the Bank to address latent risks, such as those associated with the RTGS infrastructure contingency procedures.

(1) See Annex F3 available at www.bis.org/publ/cpss101a.pdf.
(2) The retail payment systems already settle using a DNS model, so do not require a sophisticated contingency solution.
(3) See Salmon (2011).

(ii) The Bank believes that the threat landscape facing payment infrastructure has worsened in recent years and the Bank needs to be proactive in combating emerging threats to infrastructure. One example of a risk that has been identified as becoming increasingly prevalent and sophisticated is cyber crime.(1) As Greg Medcraft, Chairman of the Board of the International Organization of Securities Commissions (IOSCO), recently remarked: 'Cyber crime has a huge potential impact on markets'.(2) The heightened risk of a failure of a principal infrastructure has caused an increase in demand for contingency solutions.

(iii) The operational risk of settling net obligations via the CHAPS settlement contingency solution increased with the introduction of the RTGS infrastructure's Liquidity Saving Mechanism (LSM) in 2013.(3) While the LSM has been successful in reducing banks' liquidity costs, it has introduced a small period between the point that most CHAPS payments are submitted to the RTGS infrastructure and when they are definitively settled.(4) This means that, in the event of an interruption to the service, it may not be possible to identify whether or not settlement had occurred for a payment caught between these two points in the payment process. In turn the impact of switching from using the principal infrastructure to the contingency solution increased.

The Bank was not alone in undertaking this analysis: other central banks had also become increasingly aware of their own drivers for improving their RTGS contingency solutions. Over the past five years, central banks have begun to investigate options for more sophisticated resilience solutions that could be invoked in the event of a dual site failure, which would address these risks.

One option that the Bank considered as a potential contingency solution was to construct a third RTGS site. As a public sector institution, the Bank seeks to provide value for money in fulfilling its objectives. The Bank weighs up the effectiveness of its contingency solutions against the risks it faces. It was concluded that developing a third site would have been too costly compared with the benefits it would bring; and furthermore that it may not offer the full risk-reduction benefits that were sought.

Developing a contingency solution that meets the requirements of RTGS infrastructure providers

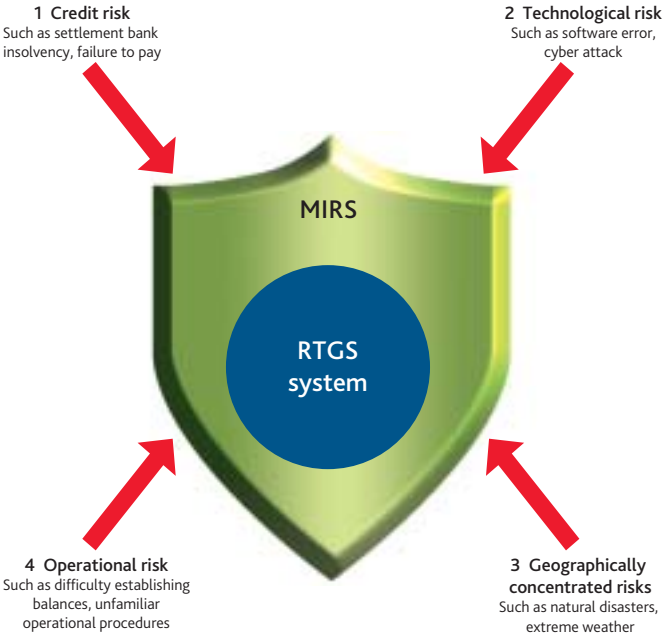
In order to transfer funds via a payment system, banks must use a standardised communication system. Many payment systems internationally, including in the United Kingdom, use a messaging service provided by a company called SWIFT.

From 2009, the Bank worked with SWIFT to identify the potential for an improved resilience model for an RTGS system.

Working in close co-operation with other central banks, a set of characteristics that would be required of an improved contingency system (that would be compatible with differing RTGS infrastructures) was identified.

The solution, which has been developed by SWIFT in conjunction with the central bank community, including the Bank, is the Market Infrastructure Resiliency Service (MIRS). It utilises SWIFT's position as communications network provider for many high-value payments systems internationally. MIRS is a basic RTGS contingency infrastructure that performs interbank settlement of payment obligations based on the information contained in SWIFT payment messages. MIRS meets the five main requirements discussed by central banks, which are detailed below. The first four of these relate to risks that an effective contingency system should mitigate and are summarised in **Figure 1**.

Figure 1 The risks that MIRS seeks to mitigate



Requirement 1: reducing credit risk by settling payments in real time

The first requirement was for the contingency system to settle payments in real time with certainty and without credit risk. This ensures that obligations between banks are extinguished

(1) For more information, see page 14 of Bank of England (2013).
(2) See www.ft.com/cms/s/0/82519604-2b8f-11e4-a03c-00144feabdc0.html?siteedition=uk#axzz3C8zZ0MS0.
(3) This was implemented to give banks the opportunity to reduce their CHAPS intraday liquidity requirements. See Davey and Gray (2014).
(4) The average CHAPS payment takes around seven and a half minutes between submission and settlement across the RTGS infrastructure.

immediately, rather than building up until net settlement at the end of the business day. If activated, MIRS acts as an accounting platform that allows any new SWIFT payment messages sent by banks to be processed in real time, facilitating continuous settlement of high-value payments. Once the problem affecting the principal sites had been resolved, the account balances would be taken from MIRS and applied back to the principal infrastructure.

To facilitate the continuous settlement of obligations in real time it is desirable for a contingency to have the ability to process peak quantities of payments. MIRS has the capacity to process more than the peak CHAPS volume processing requirement of 300,000 payments in three hours.

Requirement 2: reducing technological risk

Operating infrastructure at multiple sites using the same IT software and hardware does not protect against technological risks as a defect in one area would be replicated across sites, making it vulnerable to the same risks. As outlined above, the Bank has experienced this type of technological vulnerability in the past. Analysis of cyber security suggests that a technologically independent contingency solution can mitigate this cyber vulnerability.(1)

MIRS is run on an independent IT platform with different software suppliers and underlying programming from the principal infrastructure. This means that it is unlikely that the same software error that caused the principal RTGS infrastructure to fail would prevent settlement in MIRS.

Requirement 3: reducing geographically concentrated risks

Some localised disruptions — such as those resulting from unexpected extreme weather conditions, natural disasters, terrorist activity or power failures — could be on a large enough scale to affect both of a central bank's sites simultaneously. MIRS is hosted from SWIFT's sites, which are geographically remote from the sites operated by most central banks, mitigating the risk of geographical concentration.

While MIRS might mitigate the risk of a dual site failure, it does rely on SWIFT's IT platform. However, there is no direct link between a failure of RTGS infrastructure at both of a central bank's sites, and an outage that would affect SWIFT's ability to host MIRS.

Requirement 4: reducing operational risk

The fourth requirement sought by central banks from a contingency solution was the minimisation of exposure to operational risk. This was deemed to be required in three areas.

First, in establishing the participants' exact balances at the point of failure. New payments cannot be made if there is uncertainty about account balances, as a bank may not have sufficient funds available to settle any further transactions. MIRS overcomes this problem by reconstructing the exact account balance at the point of failure — mitigating the increase in risk described in the previous section that relates to the temporary queuing of payments in the LSM. This functionality relies on the central bank's RTGS system sending MIRS a snapshot of each bank's settlement account balance at regular intervals throughout the business day so that MIRS has a remotely stored record with which to start reconstructing the balances. Then, in the event that it is invoked, MIRS takes the most recent balances that are known with certainty and applies all of the payment message confirmations that have been received since that point.

Second, operational risk arises when banks utilise processes that are unfamiliar to them. MIRS mitigates this risk by processing standard SWIFT messages, so the way that payments are processed by banks does not materially change.

Third, while developing an improved contingency solution may involve outsourcing the infrastructure that RTGS is operated on, most central banks would not be comfortable outsourcing the actual operation of their RTGS infrastructure, as this could introduce operational risk. To address this concern, MIRS allows central banks to remain in control of their RTGS infrastructure even when it is invoked.

Requirement 5: simplicity of design

To cater for all aspects of the various bespoke national RTGS systems would have made MIRS unfeasible, increasing the complexity and costs and introducing operational risk. MIRS was deliberately designed to be a simple RTGS system, and consequently it does not support all of the bespoke functions of individual central banks' RTGS infrastructures. To take one example, it does not replicate the Bank's RTGS LSM.

This is because MIRS is designed to provide an alternative to a principal RTGS infrastructure in the event of a worst-case scenario. It addresses the financial stability risks of banks being unable to settle their high-value payment obligations with certainty, providing the necessary basic functionality but without the additional cost and complexity of all the other functions of their RTGS infrastructure.

MIRS and the Bank of England

MIRS has been developed by SWIFT in conjunction with the central bank community, including the Bank, in order to fulfil these requirements.

In February 2014, the Bank became the first central bank to adopt MIRS as its contingency RTGS infrastructure. It concluded that MIRS provides a significantly improved level of resilience at a much lower cost than other potential

(1) See Goldman (2010).

contingency options considered. Other central banks are working towards a similar adoption of MIRS as their alternative contingency system.

Conclusion

The importance of payment systems in maintaining financial stability fosters a need for central banks to continuously improve the infrastructure that facilitates these payments.

The Bank of England's RTGS system has always had a high degree of operational resilience. Although the Bank hopes to never have to invoke its contingency RTGS infrastructure, MIRS has further improved the Bank's ability to continue safe and efficient settlement of payments under a range of extreme adverse scenarios.

References

Bank of England (2013), *Payment Systems Oversight Report 2012*, available at www.bankofengland.co.uk/publications/Documents/psor/psor2012.pdf.

Davey, N and Gray, D (2014), 'How has the Liquidity Saving Mechanism reduced banks' intraday liquidity costs in CHAPS?', *Bank of England Quarterly Bulletin*, Vol. 54, No. 2, pages 180–89, available at www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q207.pdf.

Dent, A and Dison, W (2012), 'The Bank of England's Real-Time Gross Settlement infrastructure', *Bank of England Quarterly Bulletin*, Vol. 52, No. 3, pages 234–43, available at www.bankofengland.co.uk/publications/Documents/quarterlybulletin/qb120304.pdf.

Goldman, H (2010), 'Building secure, resilient architectures for cyber mission assurance', Secure and Resilient Cyber Architectures Conference, The MITRE Corporation, McLean, VA, October, available at www.mitre.org/sites/default/files/pdf/10_3301.pdf.

Salmon, C (2011), 'The case for more CHAPS settlement banks', available at www.bankofengland.co.uk/publications/Documents/speeches/2011/speech508.pdf.