CHAPTER 26.

SYSTEMIC RISKS CONTROL AS A DETERMINANT OF PAYMENT SYSTEMS DEVELOPMENT IN WB COUNTRIES[1]

Aleksandra BRADIĆ-MARTINOVIĆ[2]

Abstract

The payment systems have significant role in each economy. Large-value payment systems (LVPS) are essential part of financial market and represent its infrastructure. In this paper we tried to determine the impact of systemic risk in their functionality using the analysis of indicators for measuring the level of its development. As a basis for analysis we used methodology developed by Cirasino and Garcia (2008), representatives of Payment Systems Development Group (World Bank). In the first part each segment of LVPS indicator is analysed in order to establish connection between systemic risks and the level of LVPS development. The second part of paper contains empirical research for Serbia, Croatia, Bosnia and Herzegovina, Montenegro, Macedonia and Slovenia, because their payment systems share the same heritage. Cirasino and Garcia published their ranks, but we did detailed calculation within all criteria. This calculation provided deeper insight in the risk management of those countries. At the end of the paper the conclusion is given that there is a high dependence between LVPS development and systemic risk management. We also conclude that WB countries and Slovenia has solid systemic risk management in their LVPS.

Key words: *payment systems, LVPS, systemic risk management, WB countries*

INTRODUCTION

Payment system is one of the key elements of financial sector and indirectly of the real economy. Humphrey (1995) highlights the necessity for each country to

[1] This paper is a part of research projects numbers 47009 (European integrations and social and economic changes in Serbian economy on the way to the EU) and 179015 (Challenges and prospects of structural changes in Serbia: Strategic directions for economic development and harmonization with EU requirements), financed by the Ministry of Science and Technological Development of the Republic of Serbia..

[2] Aleksandra Bradić-Martinović, Institute of Economic Sciences Belgrade, Associate researcher

implement continuous improvement of the national payment system, as provided by progress of banking system, money market and economy.

Safe and efficient payment system has high importance in the development of economy, especially from the perspective of monetary policy and financial stability. In most countries central banks are LVSP providers and they monitor developments in the payment system in order to assess its impact on the demand for money, the influence of monetary policy transactions and the efficiency and stability of critically related financial markets (BIS-CPSS, 2006). Cirassino (2007) claims that the safe system is the *key element* for maintaining and promoting financial stability. The problems may arise if the system has poor design or technical and operational failures, because that condition can be generator for contagion and severe systemic disruptions in financial markets. Bech et al (2008) realize that the scope of problems is even more complex as a result of rapid technological changes and evolution of users needs (e-payments, m-payments). Those processes cause significant transformation of the payment systems infrastructure, procedures and risks. Central banks have become aware of these trends and they have taken an active role in payment systems development in last few decades, with the objective to provide solid base for overall financial system development.

Cirasino (2007) point out that payment systems have moved from the backroom to the boardroom of all financial institutions due to the recognition of the critical role which a solid functioning payment system plays in supporting the financial and real economies. From a broader perspective, a less than optimal use of payment instruments and/or inefficient or poorly designed systems to process these instruments may ultimately have an impact on systemic stability, economic development and growth.

Central part of each national payment systems is one or few (in highly developed countries) LVPS systems. This type of systems are mainly used for interbank payment instructions, which include settlement of interbank money market operations, the cash leg of securities trades and leg of foreign exchange trades. Large-value payment systems typically process a relatively small number of high-value and time-critical payments (ECB, www.ecb.int). The appearance of disorder in this area of economic infrastructure may have devastating consequences. The biggest problem of these systems relates to the possibility of generating and transmitting systemic disorders in a very short time (within one working day). Because of that, the development of real time gross settlement (RTGS) systems is response to the growing awareness of the need for sound risk management in large-value funds transfer systems. RTGS systems can offer a powerful mechanism for limiting settlement and systemic risks in the interbank settlement

process because they can effect final settlement of individual funds transfers on a continuous basis during the processing day. In addition, an RTGS system can contribute to the reduction of settlement risk in securities and foreign exchange transactions by facilitating the delivery versus payment (DVP) and payment versus payment mechanisms (World Bank, 2008).

In her speech, Tumpel-Gugerell (2010) pointed out that analysis conducted after the crisis showed that payment and settlement systems have functioned well during the recent crisis and have contributed to prevent worse outcomes, continuous work on further strengthening and harmonizing payment and settlement systems will enhance the resilience of the financial system. More harmonized and integrated payment and settlement systems increase the efficiency of financial markets and ultimately lead to cost savings and welfare gains for the overall economy, these efficiency gains will free up more liquidity and capital for the financial industry.

Total disruptions of payments systems are extremely rare events, so we do not have much historical data on how payment systems react to a disruption. As we already stated even in the recent financial crisis the payment systems have functioned without serious disruptions. One of the most well known operational disruptions in the interbank payment system is the attacks on the world trade centre in New York on September 11, 2001. The massive damage on property and communication systems made it more difficult or even impossible for some banks to execute payments to other banks. The impact of such a disruption can have effects beyond the immediate counter parties of the banks disrupted by the shock. In extreme cases it might even disrupt the whole financial system (Heijmans, 2009).

ANALYTICAL FRAMEWORK

Risk is a phenomenon present in each area of business and also is characterized by the operations of payment systems. In general, no matters of the cause, payment system's risks are consequence of inability to complete the initiated payment transaction, i.e. to reach the state of finality (Kahn and Roberds, 1998). Seemingly technical problem can have far-reaching effects on payment system functioning, but in extreme situation on the whole economy.

Scmitz and Puhr (2009) and Khandelwar (2007) share the state that the payment systems risks are directly determined by the participants, type of settlement systems, technology in use and the role of providers. The level of risk is additionally amplified by the security market transactions, because of their influence in global volume of transactions.

Introduction of information and communication technology is a basis of significant changes in the way of payment systems functioning. As a result of that process some risks reduced, the other modified, but some new risks arise, as well. The crucial invention which caused general reduction of risks level was introducing of RTGS systems. The main feature of this type of systems is that they can process payment transactions in real time and decrease the overall level of risks.

The payment systems risks can be divided into credit risk, unwinding risk, liquidity risk and operational risk. The group which comprises credit, liquidity and unwinding risks is known as settlement risk group (Dale, 1998). All presented risks have one common feature, they can trigger systemic disturbance. The initial disturbance itself can e.g. be severe liquidity problems or insolvency of bank and its cases varied. The initial problem may become systemic when it transfers to other participants of the payment system, or even of the financial system (Galos and Soramaki, 2005).

Other participants of the financial system may suffer the initial disturbance which then becomes systemic (a systemic event). A systemic event may decrease the confidence in participants of the financial sector and thus result in "investor panics" when creditors withdraw their claims. A systemic event may appear as credit losses and/or liquidity problems and may cause other banks to become insolvent or illiquid. A disturbance of systemic nature may affect the performance of the financial markets which may become weak due to that and eventually negatively affect the economy as a whole (De Bandt and Hartmann, 2000).

Credit risk is the risk of loss as a consequence of a participant's inability to meet its payment obligation. The credit risk can arise between the moment when payment transaction entered in the system and the moment of execution. Galos and Soramaki (2005) observe that RTGS system provides instant finality throughout the business day and reduce the risk that settlement will not occur. DNS system settles the account at the end of the day, so the probability of credit risk failure is much higher. That is the main reason why most of the countries decide to upgrade their national payment system, implementing the RTGS solution.

Unwinding risk is another settlement risk and it arises because the payment instruction released to receivers may be revoked, or unwound. Unwinding risk is characteristic only for DNS systems, in the situation of settlement errors, because it is not technically possible in RTGS systems. Compare to credit risk, unwinding risk is very difficult to measure, and even more difficult to manage. Management

of this type of risk must include group agreement, which provide that each participant in the system have insight in credit ability of other participants.

Liquidity risk is participant's inability to carry the payment obligation or more of them, in time, due to cash flow short fall or insufficient funds. Liquidity in the moment of settlement is crucial for payment system and its participants. Khandelwal (2007) implies that the bank can have solid financial condition, but be unable to fulfil its obligation because of system failure. The liquidity risk is more typical for RTGS systems. In that type of system the participant need more funds for settlement during the whole business day. As an example of liquidity risk we can observe the situation explained in Financial Stability Paper (Bank of England, 2009). They point out events that have crystallised in recent years in UK payment systems. "On 15 September 2008, Lehman Brothers was places in administration. Lehman Brother's default occurred after some intraday funding via the self-collateralising repo mechanism had been undertaken by CREST settlement banks. This demonstrates the importance of settlement banks ensuring adequate liquidity management planning for client default".

The liquidity risk can be minimize or even eliminate, in the system where all participants hold enough fund in transactional account. Fund can be cash or reserve, but the essential is that they can be used for settlement. The main problem is that holding funds in transactional account is expensive for banks, because these funds do not bring income. If we observe this problem form the banks' focus, the costs of total risk elimination is too high. Jinesku (2006) pointed out that in RTGS systems each participant is exposed to the risk from any other participant. Illiquidity of one participant can cause the illiquidity of other, who counts for that fund as a guarantee of liquidity of its own. Unlike the RTGS system, where liquidity risk can arise during the whole business day, in DNS system it can happened only in the settlement cycle (one or more, per the day).

The specific source of settlement risk can be found in cross-border transactions, which connect several payment systems in different countries, currencies and time zones. Additional problem is that those transactions are large value. In literature (Shirreff, 1996) the most known example of credit cross-border risk is Herstatt event, when Bankhaus Herstatt in Cologne was shut down by the German banking supervisors, in 1974. The closure, at 3.30 pm German time, left all of Herstatt's dollar foreign exchange transactions half completed in New York, where it was still only 10.30 am. The panic caused, even by that small number of failed payments, resulted in dislocation and gridlock in the foreign exchange markets. Eisenbeis (1997) points out more recent example from 1991, when the Bank of Credit and Commerce International (BCCI) has been closed. The Industrial Bank of Japan had paid 44 billion yen into BCCI's branch in Tokyo, for which payment

was to be received in New York from BCCI's New York branch. When BCCI was closed, the dollar portion of the transaction was never completed, and Industrial Bank of Japan became a creditor for $30 million. The name of that risk is *herstatt risk*.

Operational risk arises as potential outcomes of operational events. Norman et al. (2009) provide an explanation of operational events, which are consists of: human aspect (errors as a result of insufficient experience, non-compliance procedures and policies, and fraud affinity), technical aspect (errors in the model of transaction processing or lack of appropriate instruments for risk measurement), process management aspect (lack of adequate report, monitoring and decision procedures. poor data processing and bad process control), and information technology aspect (it is connected with imperfection of information systems that are not identified in time). We can find lot of examples for operational risks events, but we will point the case of "double failure of the firewalls surrounding the RTGS processor on 7 July 2008 in UK payment system. When the main firewall at the secondary site, from where RTGS was running at the time, was unable to start due to a power failure, the backup firewall should have taken over, but it was unable to do so. This was subsequently found to be due to a lack of synchronisation between the two firewalls. On the day, the procedures for 'failing over' RTGS to the primary site, where the firewalls were operating correctly, worked well, but RTGS was unavailable in total for over 200 minutes" (Bank of England, 2008).

Today one of the main goals of most system provider (i.e. central banks) is to minimize systemic risks. For settlement risks they obtain risks reduction by increasing the liquidity held by the participants in the system. Most countries have implemented the RTGS system in their large value payment systems aimed at reduction of systemic risk. RTGS systems significantly decrease the level of settlement risks, despite the high price for keeping the liquidity reserves. Dhumale (1999) observes that current design issues in RTGS systems vary by different countries but two aspects which are commonly discussed for better risk management are policies for central banks granting intraday credit and establishing queuing systems. Intraday credits transfer credit risk from participants to the central bank, but the best situation is when high quality collateral is required. The other solution is that the source or liquidity is opening balances and funds received from other participants during the day, or their reserve requirements during the day, or credit lines between banks. The additional solution for risk reduction is payment order which goes into a queue for later processing.

McPhail (2003) suggest that in the case of operational risk most popular solution for risk reduction is outsource. But, when it is concerned of central bank's LVPS, that is not an option, because they are essential part of the financial infrastructure and are often unique. The other solution is risk control. For human error central bank must provide internal controls, for data and ICT infrastructure provider must have routine procedures for periodical data back-ups, tapes and other storage media which are kept in sites other than the main processing site, back-up servers which are deployed at the main processing site, a fully equipped alternate processing site, documented a formal business continuity plan which include procedures for crisis management and information dissemination, regularly tested.

After establishing the relationship between financial market, payment systems and systemic risks in those systems, we can set the core hypothesis that the appropriate approach to risk management is necessary to achieve a high degree of LVPS development.

Institutional reaction in the field of payment systems risk is included in the document published by Bank for International Settlement (BIS) entitled Core Principles for Systematically Important Payment Systems (Core Principles for SIPS). The Core Principles are intended for use as universal guidelines to encourage the design and operation of safer and more efficient SIPS worldwide (BIS, 2001). They present public policy objectives, safe and efficiency in SIPS.
Based on Core Principles for SIPS, Cirasino and Garcia (2003) developed an indicator for measuring the LVPS level of development. They used Core Principles as a list of criteria that must be fulfilling by the LVPS. In the next part of this paper we will describe the structure of LVPS indicator in purpose to explore in which extent the risk reduction is important determinant of development level.

Based on the World Bank's Global Payment Systems Survey 2008, the document "Measuring Payment Systems Development" presents a measurement methodology and related outcomes for four areas of the national payments system: i) Legal and Regulatory Framework; ii) **Large-Value Funds Transfer Systems;** iii) Retail Payment Systems; and, iv) Payment system Oversight Function and Cooperation.

DATA AND METHODOLOGY

The scoring for LVPS is based on system design and key policy decisions that affect the safety, soundness and efficiency of the system. For RTGS systems, the Core Principles that are scored in explicit form are CP III, CP VII, CP VIII, CP IX and CP X (Cirasino and Garcia, 2003).

First component of indicator measure the liquidity risk, which is cover with the questions about main sources of liquidity during the day, mechanism which is apply in the case of insufficient balance on participant's account, and the pricing policy. Pricing policy is important because it is better to send payment instructions earlier in the morning, to avoid potential problems at the end of the business day, or before closing hour. The questions about liquidity risks are:

LIQUIDITY RISKS

1. What are the main sources of liquidity during the day?

a.	Opening balances and funds received from other participants during the day
b.	Participants can use a part of their reserve requirements during the day
c.	Participants can use all their reserve requirements balance during the day
d.	Lines of credit between banks
e.	The RTGS operator allows current account overdrafts
f.	The RTGS operator grants credit, either in the form of a loan or a repo
g.	Other

Scoring:

If answers b) or c) ***and*** *e) or f)*	then give a 3
If answers b) or c) ***or*** *e) or f) only*	then give a 1.5
If answer d) combined with either b), c), e) or f)	then give a 1.5
Otherwise	then give a 0

2. If a participant does not have enough balance (and/or credit) in its current account with the RTGS operator to process new payments, what mechanism becomes applicable?

a.	The payment order is rejected immediately
b.	The payment order goes into a queue for later processing

Scoring:

If answer b)	then give a 1.5
Otherwise	then give a 0

3. Is the pricing policy used to incentivate the smooth flow of payments through the system during the day e.g. with differentiated charges based on the time of the day in which payment orders are processed, to promote

participants begin sending their orders early in the operational day? (indicate YES or NO)

Scoring

If YES	then give a 1.5
If NO	then give a 0

Additional question is about credit risk, but that question is applicable in the case when the RTGS operator allows current account overdrafts or grants credit. Otherwise, there is no need to answer question 2.1. But if operator allows liquidity extension, it is very important to provide proper collateral mechanism.

CREDIT RISKS FOR OPERATOR/INTRADAY LIQUIDITY PROVIDER

4. *How does the RTGS operator manage the credit risk that may arise as a result of applying some of the mechanisms discussed in the previous question?*

a.	High quality collateral is required in all cases
b.	Collateral is required in all cases, but collateral does not always have suitable quality
c.	Current account overdrafts/credit is limited, but no collateralization is required
d.	There are no limits or collateralization requirements for account overdrafts/ credit

Note: this is necessarily linked to item 1.1 under Liquidity Risks (answers e) and f)). Therefore, scoring system here uses subtraction mechanism, and combination of 1.1 and 2.1 cannot be negative.

Scoring

If answer a)	then give 0
If answer b) or c)	then give a -1.5 (subtract)
If answer d)	then give -3 (subtract)

Very important group of questions cover the main source of operational risks, ITC infrastructure failures. Those questions indicate the most important procedures and equipment which are necessary for safe functioning of LVPS.

RESILIENCE AND BUSINESS CONTINUITY

5. Resilience and Business Continuity

a.	Routine procedures are in place for periodical data back-ups
b.	Tapes and other storage media are kept in sites other than the main processing site
c.	Back-up servers have been deployed at the main processing site
d.	A fully equipped alternate processing site exists
e.	The RTGS operator has documented a formal business continuity plan
f.	Business continuity arrangements include procedures for crisis management and information dissemination
g.	Business continuity arrangements are regularly tested

Scoring:

If all of the above, or all exept c)	6
If answers d) ***through*** *g)*	6
If all of the above, except d)	4
If answers a) ***through*** *e), even without c)*	4
*If answers a)****through*** *c)and e)*	3
If answers d)and e)	3
*If answers a)****through*** *c)*	2
If only a) and b) or none	0

Efficiency of the payment process and in this case in connection with Central Security Depository systems is directly related with the risk. Less time for transaction execution, it is less likely the adverse event to happen.

EFFICIENCY – Integration of the RTGS with other key settlement systems

6. Central Bank-operated securities registry or CSD – The CSD has a real-time interface with the RTGS (if applicable)? *(indicate YES or NO)*

Scoring:

If YES to any of the two questions above	2
Oherwise	0

Safety and protection of the payment system depends of reliability of its participants and they are usually credit institutions. The Payment Services Directive (PSD, 2007/64/EC) is a regulatory document in EU which regulate payment systems, services and participants (providers), with objective (among others) to increase pan-European competition allowing non-banks to be a providers in payment systems. In new circumstances it is very important to provide rigid access rules and policies. Otherwise, the payment system can be very vulnerable and exposed to settlement risk.

ACCESS RULES AND POLICIES

7. *RTGS access rules and policies*.

a.	There is an explicit access/exclusion policy for the RTGS system
b.	Access to the RTGS is granted on the basis of institutional standing (i.e. whether the applicant is a bank, or some other specific type of financial institution
c.	Access to the RTGS is granted on the basis of the fulfillment of a set of objective criteria to ensure a safe and sound operation of the system (e.g. capital requirements, technological capacity, internal risk controls, appropriate management, etc)
d.	Formal rules or arrangements are in place to allow the RTGS operator to exclude a system participant in a timely fashion

Scoring

If all of the above, or all except b)	4
If all of the above exept c) or d)	3
If answers a) and c)	3
If answers a) and b)	2
If answers b) and d) or c) i d)	1
Otherwise	0

Finally, the system is more efficient and less risk exposed if there is explicit organizational part of system which can address all participants' needs and solve problems connected with them.

SYSTEM GOVERNANCE

8. Is there a specific RTGS User's Group in place for the RTGS operator to better address participants' needs? (indicate YES or NO)

Scoring

If YES, and score for this sub-component so far is 14 or more	then give a 2
If YES, and score for this sub-component is less than 14	then give a 1
If NO, and score for this sub-component so far is 14 or more	then give a 1
If NO	then give a 0

After scoring, the level of LVPS development can be determined following the next scheme:

Actual Score	Level of Development
>10-12	High
>7-10	Medium High
>3-7	Medium Low
0-3	Low

Notes: Maximum Score: 12 points; Minimum Score: 0 points.

The structure of LVPS indicator implies that the risk management is key determinant of its development. The Q1 and Q2 have strongpoint in CP III - The system should have clearly defined procedures for the *management of credit risks and liquidity risks*, which specify the respective responsibilities of the system operator and the participants and which provide *appropriate incentives to manage and contain those risks*. The Q3 is directly connected to CP VII - The system should ensure a *high degree of security and operational reliability* and should have contingency arrangements for timely completion of daily processing. The Q4 is connected to CP VIII - The system should provide a means of making payments which is *practical for its users and efficient for the economy*, which is in broader sense connected with risk, as we already explained. Questions Q5 and Q6 have strongpoint in CPs IX and X – The system should have objective and publicly disclosed criteria for participation, which permit fair and open access; and The system's governance arrangements should be effective, accountable and transparent.

In the research part of this paper we did the calculation of the indicator with data obtained from WB countries (Serbia, Croatia, Bosnia and Herzegovina and

Macedonia, together with Slovenia), responses to the Global Payment System Survey carried by the PSDG (2008) in 2007 and 2008. The Survey data was not complete, because Montenegro did not send the fulfil Questionnaire. We provide essential answers with direct support from Central bank of Montenegro, National Payment Operations Department for 2010. In order to achieve the same time frame in the Questionnaire, we provide additional answers for other WB countries, in cooperation with their central banks.

Cirasino and Garcia (2008) paper contain a table with all 142 examined countries, and their ranks. We used top down approach and reconstructed of all answers with scoring, in order to find the strength, weaknesses and risk exposure of the LVPS systems in WB countries and Slovenia.

RESULTS

On the basis of our data we constructed the following table. All WB countries and Slovenia are presented in the table, with individually results for each question. The table include the Sub row, because of the conditional scoring for Q. 6.1.

	SRB	**HRV**	**BIH**	**MNE**	**MKD**	**SVN**
Liquidity risks						
1.1	3	3	3	1.5	3	1.5
1.2	1.5	1.5	1.5	1.5	1.5	1.5
1.3	1.5	1.5	1.5	1.5	1.5	0
Credit risks						
2.1	0	0	0	0	0	0
Operational risks						
3.1	6	6	6	4	0	6
Efficiency						
4.1	2	2	2	0	2	2
Access rules and policies						
5.1	3	3	4	4	2	4
Sub	17	17	18	12.5	10	15
System governance						
6.1	1	1	2	0	1	2
Score	**18**	**18**	**20**	**12.5**	**11**	**17**
Rank	**1**	**1**	**1**	**2**	**2**	**1**

The results points out that Serbia, Croatia, Bosnia and Herzegovina, and Slovenia have LVPS systems with High level of development, while Macedonia and Montenegro have systems with Medium High level of development.

The highest score in the region of WB countries has Bosnian RTGS, with maximum 20 points. This system (official name: RTGS) has the full protection of liquidity risk. As a *liquidity extension* the participants can use opening balances and funds received from other participants during the day and all their reserve requirements balance during the day. They also can use lines of credit between banks. RTGS operator allows current account overdraft and grants credit, either in form of loan or repo. The system has a queue for latter processing in case a participant does not have enough balance/credit in its current account to process payments. The RTGS operator use pricing policy to incentivize the smooth flow of payments through the system during the day. Because of ability to overdraft and take a credit, participants must provide high quality colateral.

The operational risk is extremely well managed because RTGS has routine procedures for periodical data back-ups, tapes and another storage media which are kept in sites other then the main processing site and back-up servers which have been deployed at the main processing site. It also has a fully equipped alternate processing site and documented a formal business continuity plan. The business continuity arrangements include procedures for crisis management and information dissemination and those arrangements are regularly tested. From 2011 in BiH there is a real-time interface between RTGS operator and Central Securities Depository (CSD).

Serbia (official name: RTGS) and Croatia (official name: HSVP) have high developed LVSP, only 2 points below the highest possible level, exactly the same shortcoming. The systems enable opening balances and funds received from other participants during the day and RTGS operator allows current account overdrafts, as sources of liquidity. In Croatia participants can use a part of their reserve requirements during the day and in Serbia participants can use. In Croatia the RTGS operator allows current account overdrafts, and in Serbia the RTGS operator grants credit, either in form of loan or a repo. The both systems also have technical ability to enable queue for latter processing, in case when participant does not have enough balance/credit in its current account with RTGS operator. Finally, liquidity risk is minimized in these systems with pricing policy which incentivize the smooth flow of payments through the system during the day. Solutions for *liquidity extension* in Croatia and Serbia present the higher standard. According to methodology the *credit risk* exposure in the system is high if the RTGS operator allows overdrafts or loan without proper collateral. In these two counties the RTGS operator requires high quality collateral in all cases, and as a result of that, the credit risk is minimized.

The *operational risk* in Croatian and Serbian payment system is also managed well, and received high score (see all about routines and continuity plan in BiH

part). The systems are *efficient*, because the RTGS operator have real-time interface with CSD.

Small shortcoming in the systems can be found in the part of access and rules policies. The both systems have explicit access/exclusion policy. Also, access to the RTGS is granted on the basis of institutional standing (i.e. whether the applicant is a bank or some other specific type of financial institution) and formal rules of arrangements are in place to allow the RTGS operator to exclude a system participant in a timely fashion. For maximum grade, the systems need to have access to the RTGS granted on the basis of the fulfilment of a set of objective criteria to ensure a safe and sound operation of the system (e.g. capital requirements, technological capacity, internal risk controls, appropriate management, etc.).

Finally, both systems do not have a specific user group in place for the RTGS operator to better address participants' needs, but they receive 1 point because the previous sub score is more than 14, so the efficiency and risk control are estimated as high, despite this deficiency.

Slovenian payment system (official name: TARGET2-Slovenia) has only 1 point less than the previous. In this system the imperfection in *liquidity risk* can be found in lack of liquidity extension in form of overdraft. In this systems participant can use credit (either in form of loan or a repo), opening balances and funds received from other participants during the day and part of their reserve requirements during the day. The system has queue for latter processing in case when participant does not have enough balance/credit in its current RTGS account, but the operator do not use pricing policy to incentivize the smooth flow of payments through the system during the day. *Credit risk* is covered by high quality collateral[3].

The *operational risk* management is highly rated because Slovenian LVPS has all requested elements (see Croatia and Serbia). *Efficiency* in the system is high, because of existence a real-time interface between CSD and RTGS operator. Access rules and policies are according with the highest standard. there is an explicit access/exclusion policy for the RTGS system, access to the RTGS is granted on the basis of institutional standing (i.e. whether the applicant is a bank, or some other specific type of financial institution), access to the RTGS is also granted on the basis of the fulfilment of a set of objective criteria to ensure a safe

[3] In the new methodology (2010) this answer is slightly changed, so the precise expression is *suitable collateral*. The explanation is: "In this context, suitable collateral should be interpreted as being liquid should a default occur. It also implies that the value of such collateral is marked to market on a daily basis and haircuts applied where appropriate."

and sound operation of the system (e.g. capital requirements, technological capacity, internal risk controls, appropriate management, etc) and formal rules or arrangements are in place to allow the RTGS operator to exclude a system participant in a timely fashion. All these conditions for participants provide the best score for Slovenia. The final question has also maximum score because the Slovenian central bank has specific RTGS Users' Group in place to better address participants' needs.

Montenegro has LVPS (official name: RTGS) with medium high level of development (12.5/20). The *liquidity extension* is based on opening balances and funds received from the participants during the day and participant can use a part of their reserve requirements during the day. The better solution requires lines of credit between banks, the ability of RTGS operator to allow current account overdrafts or to grant a credit (either in form of loan or a repo). The system has queue for latter processing in case when participant does not have enough balance/credit in its current RTGS account, and the RTGS operator use pricing policy to incentivize the smooth flow of payments through the system during the day. Because of inability to grant a credit or overdraft there is no *credit risk* in the system.

Montenegrin payment system has the most required procedure for system recovery. The only shortage is lack of procedures for crisis management and information dissemination in business plan. The problem also exists in the area of efficiency, because there is no real-time interface between CSD and RTGS operator.

Access and policy rules are fully improved and consist of high standard requirements (see Slovenia). The additional shortage is absence of specific RTGS Users' Group in place to better address participants' needs.

In WB region Macedonia has the lowest score for LVPS development (11/20), but its RTGS system (official name: MIPS) is in middle high category. Macedonian payment system has high scored *liquidity management* procedures, because participants can use opening balances and funds received from other participants during the day or all their reserve requirements balance during the day and RTGS operator grants credit, either in the form of a loan or repo. This is optimal combination of liquidity extension. The system also has technical ability to enable queue for latter processing, in case when participant does not have enough balance/credit in its current account with RTGS operator. Finally, liquidity risk is minimized in the systems with pricing policy which incentivize the smooth flow of payments through the system during the day. As a solution for *credit risk*

exposure in case when RTGS operator grants credits, system requires collateral of high quality.

The main problem in Macedonian LVPS is *operational risks*. The system has only routine procedures in place for periodical data back-ups and back-up servers have been deployed at the main processing site. This part of LVPS indicator receives 0 points. The operator (Macedonian central bank) need to implement tapes and another storage media which are kept in sites other then the main processing site, fully equipped alternate processing site and documented a formal business continuity plan. The business continuity arrangements have to include procedures for crisis management and information dissemination and those arrangements are regularly tested. The operational risks management is the reason for low scoring of Macedonian payment system.

There is a real-time interface between RTGS operator and CSD. Lower score is caused also by the state of access and rules policies. The Macedonia has access to the RTGS is granted on the basis of institutional standing (i.e. whether the applicant is a bank, or some other specific type of financial institution) and formal rules or arrangements to allow the RTGS operator to exclude a system participant in a timely fashion. The highest score would be received if the system has explicit access/exclusion policy and access to the RTGS is granted on the basis of the fulfilment of a set of objective criteria to ensure a safe and sound operation of the system (e.g. capital requirements, technological capacity, internal risk controls, appropriate management, etc). Finally, there is a specific RTGS Users' Group in place to better address participants' needs.

CONCLUSIONS AND RECOMMENDATIONS

In conclusion we can emphasize two points. First point is related to the structure of LVPS indicator. After insight of its consisting component we can conclude that the main part of it is measuring of liquidity, credit and operational risks in one word – systemic risks, together with efficiency. It is obvious that the systemic risk management is the essential part of large value payment system development.

The other point is related to the research done in the WB countries and Slovenia. The results show that the systemic risk management is a high-level, so their national payment systems have good scores and belong to high or medium high developed systems. This is very important conclusion for WB countries in their efforts in EU integrations. Our recommendations for those countries are to improve their systems and avoid unnecessary risk exposure.

References

[1] Bank of England, (2008), Payment Systems Oversight Report 2008

[2] Bech M.L, Preisig C, Soramaki K (2008) Global Trends in Large-Value Payment Systems, *FRBNY Economic Policy Review*, September 2008

[3] BIS, (2001), Core Principles for Systematically Important Payment Systems, www.bis.org/publ/cpss43.pdf

[4] Dale R. (1998) Risk Management and Public Policy in Payment, Clearing and Settlement Systems, *International Finance 1:2*

[5] De Bandt, O, Hartmann, P. (2000) *Systemic Risk: A Survey*, Working Paper no. 35, ECB

[6] Dhumale, R. (1999), Systemic Risk in International Settlement, ESRC Centre for Business Research, University of Cambridge, Working Paper No. 152

[7] Eisenbeis, R.A, (1997), International Settlements: A New Source of Systemic Risk, Federal Reserve Bank of Atlanta, *Economic Review*, second quarter 1997

[8] Galos, P, Soramaki, K. (2005), Systemic Risk in Alternative Payment System Designs, ECB, Working Paper Series, no. 508

[9] Jinescu, G.B. (2006), By-pass FIFO Queue Mechanism for Liquidity Risk Management in Electronic Payments of System, *Economy Informatics*, 1-4/2006

[10] Kahn C.M, W. Roberds (1998), Payment System and Banking Incentives, *The Review of Financial Studies*, vol. 11, no. 4

[11] Khandelwal, S., (2007), Risks in Large Value Payment Systems, *Journal of Internet Banking and Commerce*, vol. 12, no. 1

[12] McPhail, K. (2003), Managing Operational Risk in Payment, Clearing, and Settlement Systems, Working Paper, Bank of Canada

[13] Norman, B, Brieley, P, Gibbard, P, Mason, A, Meldrum, A. (2009), A Risk-based Methodology for Payment System Oversight, Bank of England, Financial Stability Paper no. 6

[14] Schmitz, S.W, Puhr, C. (2009), Structure and Stability in Payment Networks – A Panel Data Analysis of ARTIS Simulations (http://ssrn.com/abstract=1400883)

[15] Shirreff, D. (1996), The Fears that dares to speak its name, *Euromoney*, Issue 329

[16] Tempel-Gugerell, G. - www.financialregulationforum.com/wpmember/payment-and-settlement-integration-in-europe-5178/ (*Speech by Gertrude Tumpel-Gugerell, ECB, at the 13th Frankfurt Euro Finance Week, 15 November 2010)*

[17] Worl Bank, PSDG, (2008) Payment Systems Worlwide, A Snapshot, Country-by-Contry answers

[18] World Bank, PSDG (2008), Payment Systems Worldwide – Snapshot, 2008.