Ciências ULisboa | Informática

di.ciencias.ulisboa.pt

/difcul

Avaliação do Risco em Processos de Negócio

Ana Respício

Email: alrespicio@ciencias.ulisboa.pt

Web: http://di.ciencias.ulisboa.pt/~respicio/

Departamento de Informática & *CMAFIO*

Faculdade de Ciências, Universidade de Lisboa

Motivação

- A gestão de processos de negócio tem um papel fundamental nas organizações:
  - **modelação e simulação** dos processos de negócio;
  - **apoio à decisão** na optimização dos fluxos de trabalho, utilização de recursos, design de processos, e monitorização de processos.

- No contexto de **segurança informática**, a literatura apresenta um **gap** no que respeita à **modelação de processos de negócio** considerando **risco** de forma a poder realizar análises de cenários / simulações.

- Propõe-se uma metodologia para avaliar o risco e realizar análise de impacto no negócio (BIA).

Metodologia

- Modelar o processo de negócio incluindo nas atividades/ subprocessos informação sobre ameaças, vulnerabilidades, ativos, fiabilidade e risco.

Atividade
- Ameaças
- Vulnerabilidades
- Ativos
- Fiabilidade
- Risco (value at)

Metodologia

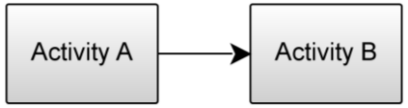
1. Modelar as atividades no processo de negócio;
2. Para cada atividade, identificar
   - componentes de risco: ameaças, vulnerabilidades, controlos;
   - fiabilidade; e
   - valor dos ativos.
3. Calcular a fiabilidade do processo (sub-processos);
4. Avaliar o risco do processo (e sub-processos);
5. Simulação e análise de cenários.

Fiabilidade e risco

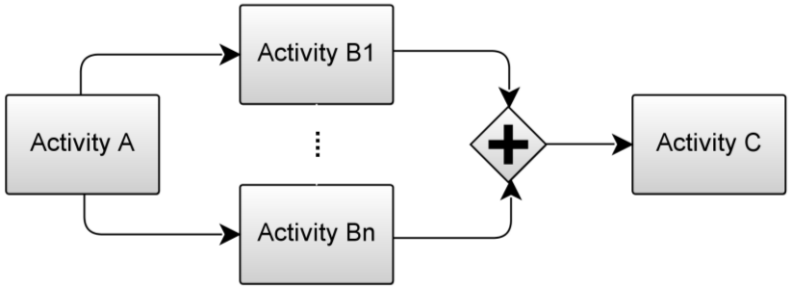
- Fiabilidade de uma atividade A, Fiabilidade(A) é a probabilidade de "não falha" dessa atividade.
- Calculamos a fiabilidade de processos de negócio BPMN (Respício and Domingos, 2015) usando o algoritmo Stochastic Workflow Reduction (Cardoso, 2002).
  - Folding do processo;

- Risco(A) = Valor(A) * (1-Fiabilidade(A)) (1 – Incerteza(A) - %Mitigação(A))

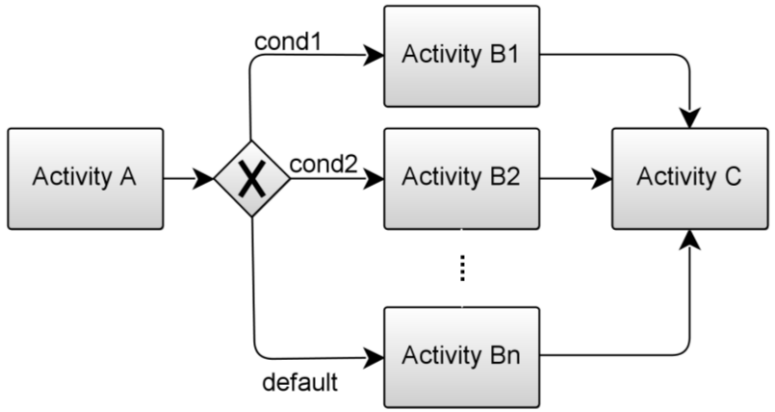
Bloco sequencial

Initial Block	Reduced Block	Reliability of the Reduced Block
		$R(AB) = R(A) * R(B)$

Bloco paralelo

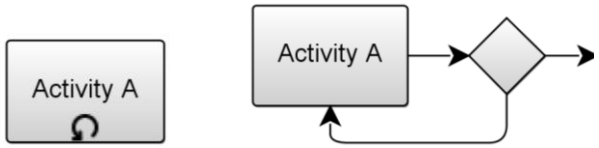
Initial Block	Reduced Block	Reliability of the Reduced Block
		$R(B1n) = \prod_{1 \le i \le n} R(Bi)$

Bloco condicional

Initial Block	Reduced Block	Reliability of Reduced Block
		$R(B1n) = \sum_{1 \le i \le n} p_i R(Bi)$

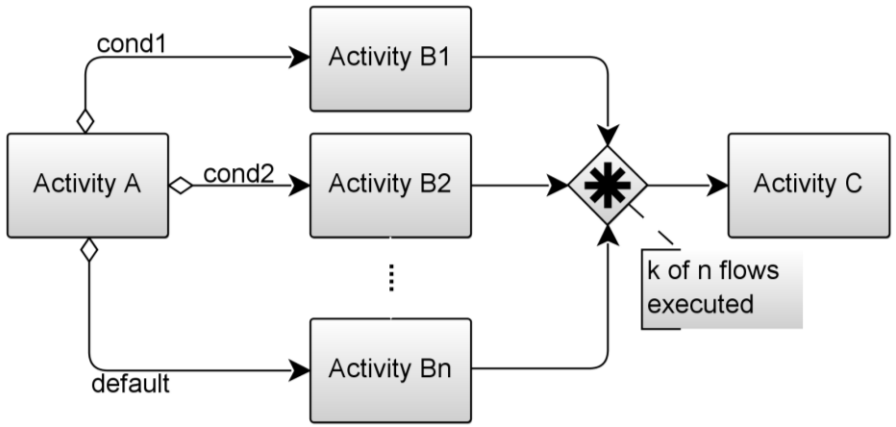
p_i is the probability of condition *condi*.

Bloco Loop

Initial Block	Reduced Block	Reliability of Reduced Block
		$R(A') = \frac{(1 - p)\,R(A)}{1 - pR(A)}$
		$R(A') = R(A)^k$

- p is the probability of executing the loop.
- k is the number of executions of a pre-determined loop.

Bloco fault tolerant

Initial Block	Reduced Block	Reliability of Reduced Block
		$$R(B1n) = \sum_{\substack{E_1=0,1 \\ \dots \\ E_n=0,1}} \phi\left(\sum_{i=1}^{n} E_i - k\right) * \prod_{\substack{i=1 \\ E_i=1}}^{n} R(Bi)$$

Where $E_i = \begin{cases} 1, \text{if } Bi \text{ executes} \\ 0, \text{otherwise} \end{cases}$ and $\phi(x) = \begin{cases} 1, \text{if } x \geq 0 \\ 0, \text{otherwise} \end{cases}$

Exemplo de aplicação

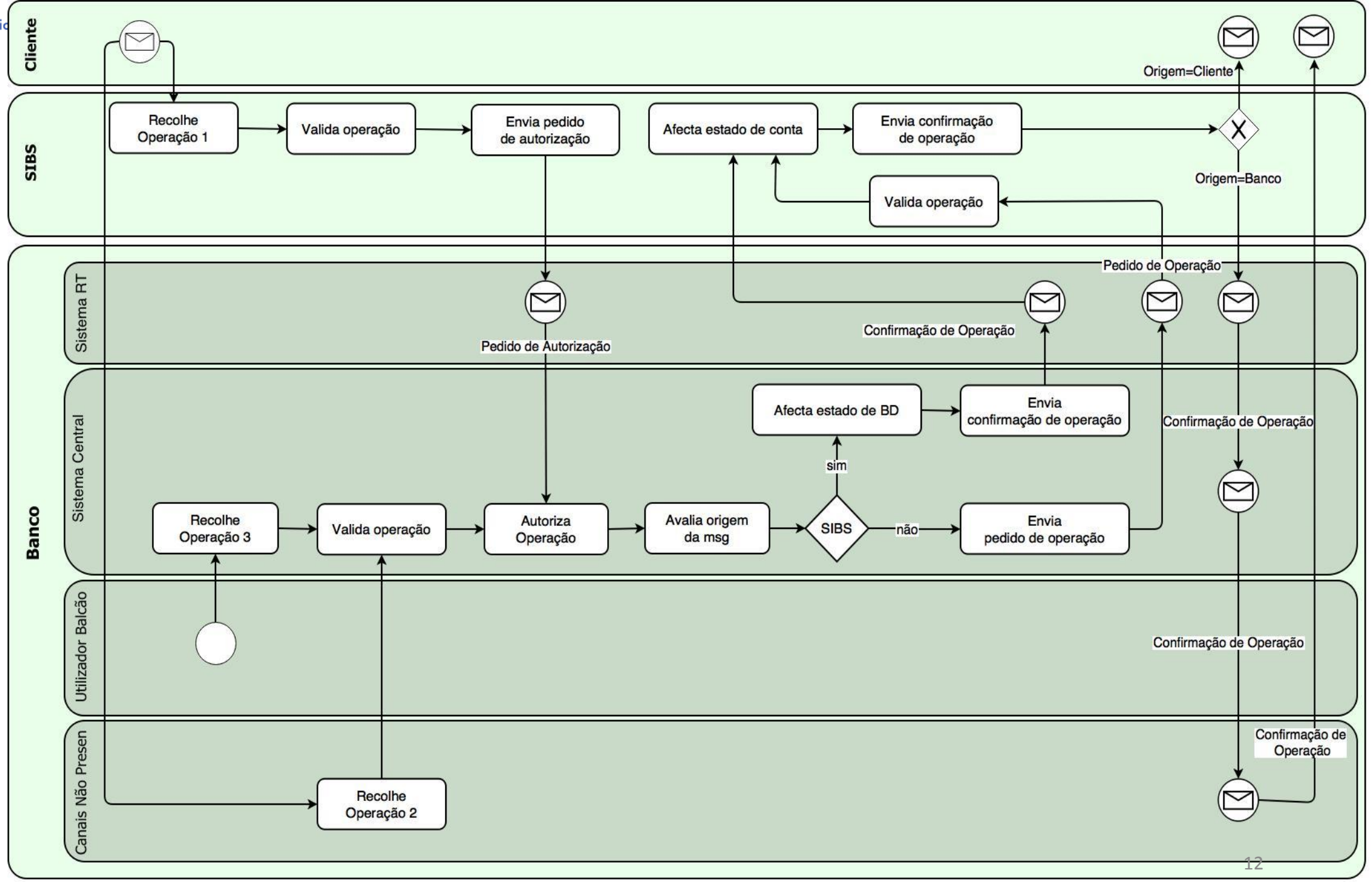
Ferramenta Quanto

Análise de Risco associado a Quebras de Serviço

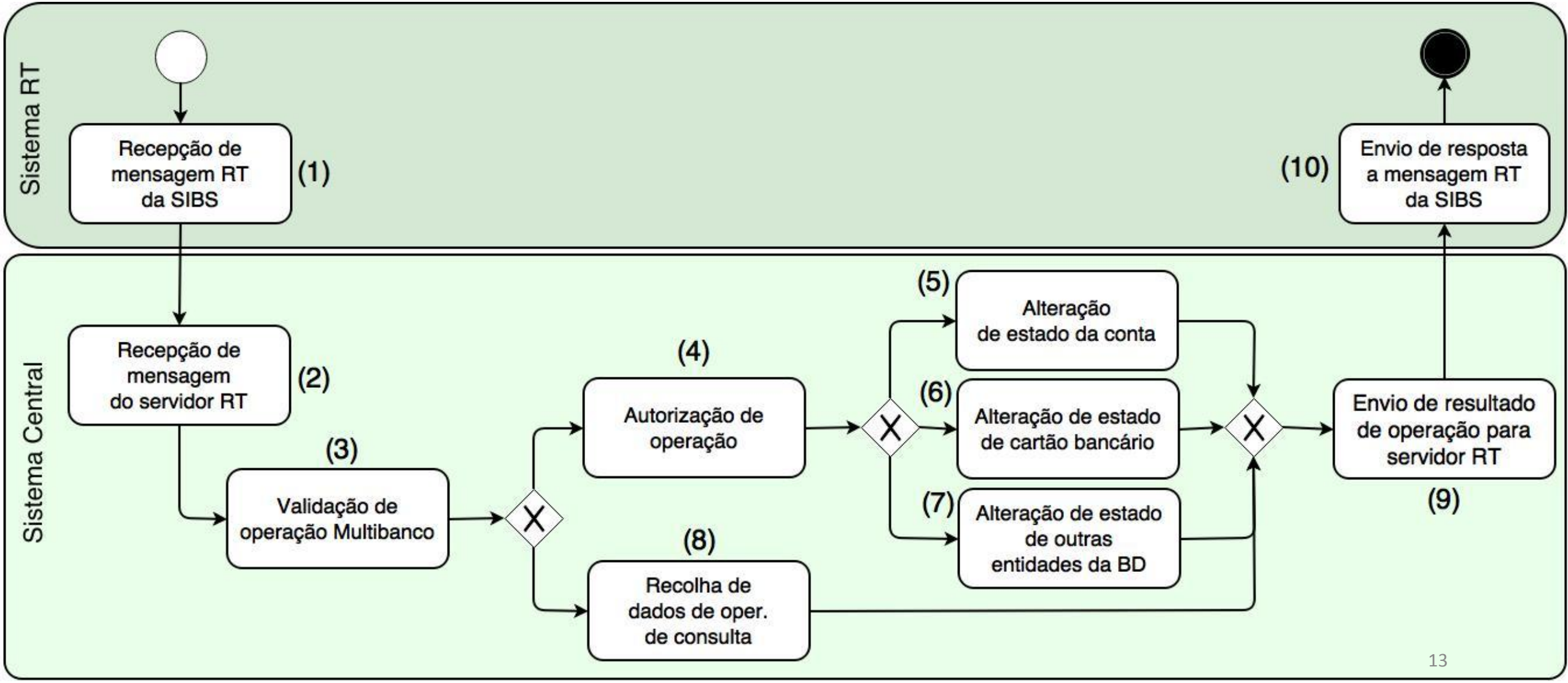
No contexto de um processo no setor bancário

Ricardo Oliveira, 2015

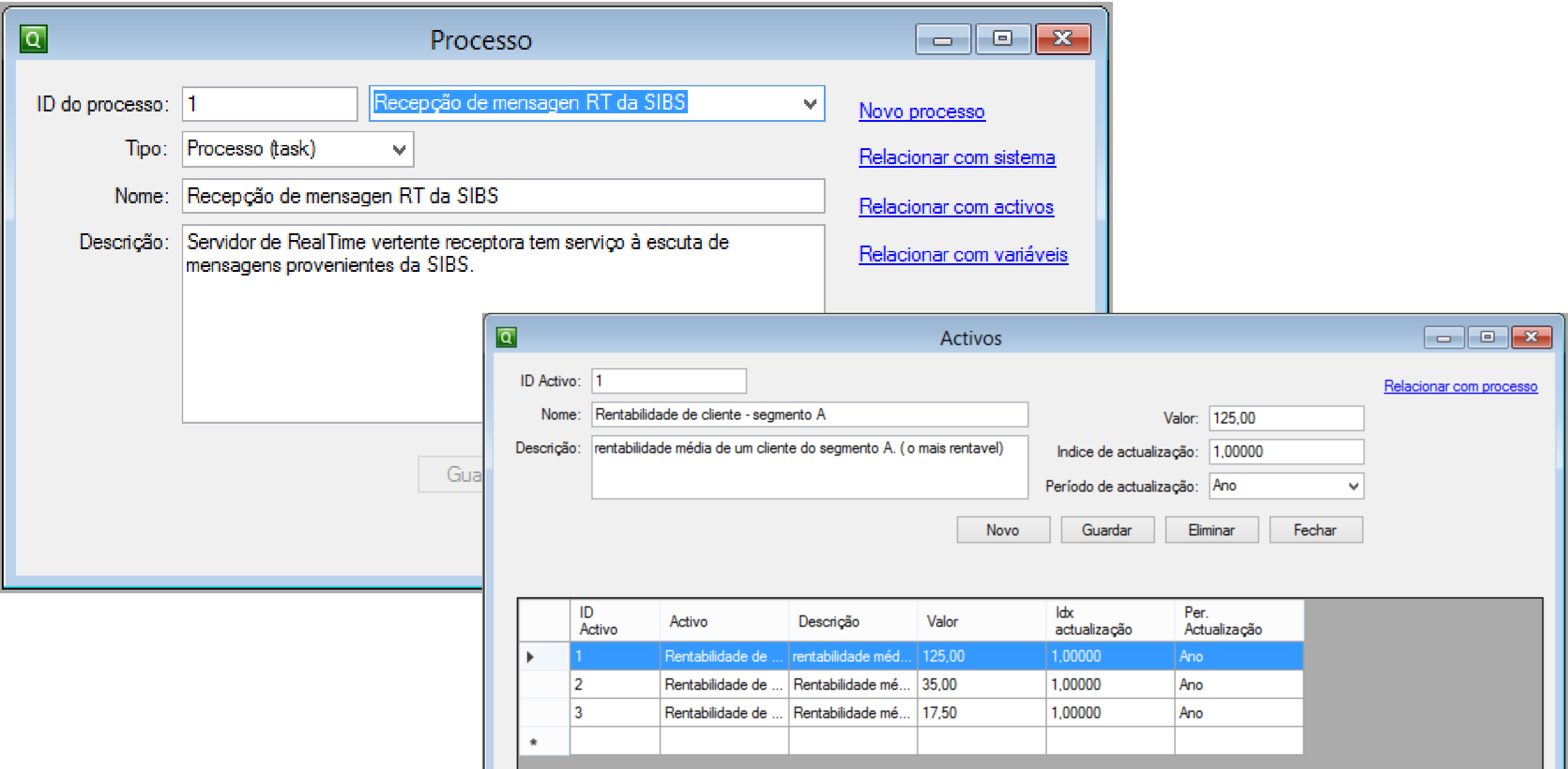
Sistema MB componente real-time



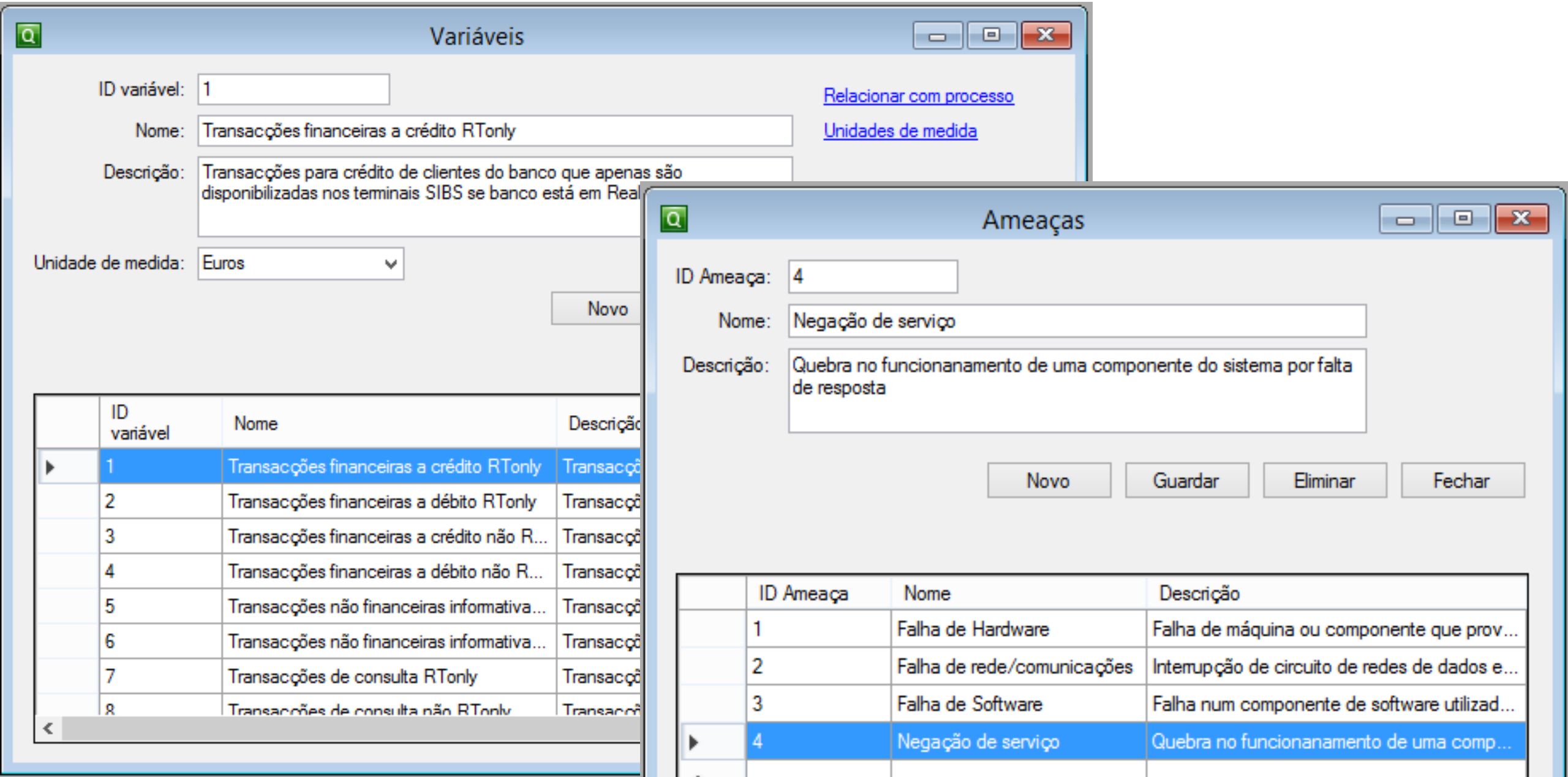
Operações MB Real-Time – vertente recetora



Aplicação Quanto – Introdução do modelo/dados



Aplicação Quanto – Introdução do modelo/dados



Simulação de falha

Risco Relativo

#	Sistema	ID proc.	Processo	Ameaça	Valor activos	Valor gerado no processo	Prob. falha (%)	Mitigação (%)	Custo de falha acrescido	Risco base	Risco relativo
4	Multibanco verte...	4	Autorização de O...	Negação de serv...	177,50	522 048,11	0,200	40,000	11 014,96	1 044,45	731,12
5	Multibanco verte...	8	Recolha de dado...	Negação de serv...	177,50	3 391 675,88	0,200	40,000	0,00	6 783,71	4 748,59
6	Multibanco verte...	5	Afecta estado de...	Negação de serv...	177,50	521 320,55	0,200	40,000	11 014,96	1 043,00	730,10
7	Multibanco verte...	6	Afectação do est...	Negação de serv...	177,50	1 479,44	0,200	40,000	0,00	3,31	2,32
8	Multibanco verte...	7	Afectação do est...	Negação de serv...	177,50	1 092,98	0,200	40,000	0,00	2,54	1,78
9	Multibanco verte...	9	Envio de resultad...	Negação de serv...	177,50	3 913 723,99	0,200	40,000	11 014,96	7 827,80	5 479,46
10	Multibanco verte...	10	Envio de resposa...	Negação de serv...	177,50	3 913 723,99	10,000	40,000	11 014,96	391 390,15	273 973,10
								Total	**77 104,72**	**1 198 703,06**	**839 092,13**

Evolução Temporal do Impacto

#	Sistema	ID proc.	Processo	Ameaça	1 hora	2 horas	3 horas	4 horas	5 horas	1 dia	2 dias	3 dias	4 dias	5 dias
1	Multibanco verte...	1	Recepção de me...	Negação de serv...	2 485,12	8 992,88	24 572,10	49 812,70	75 127,48	280 963,28	560 218,25	900 292,51	1 185 863,55	1 467 275,39
2	Multibanco verte...	2	Recepção de ms...	Negação de serv...	2 485,12	8 992,88	24 572,10	49 812,70	75 127,48	280 963,28	560 218,25	900 292,51	1 185 863,55	1 467 275,39
3	Multibanco verte...	3	Validação de ope...	Negação de serv...	49,70	179,86	491,44	996,25	1 502,55	5 619,27	11 204,36	18 005,85	23 717,27	29 345,51
4	Multibanco verte...	4	Autorização de O...	Negação de serv...	2,72	9,17	33,82	78,90	133,94	840,21	1 721,87	3 437,11	4 205,18	4 960,07
5	Multibanco verte...	8	Recolha de dado...	Negação de serv...	46,98	170,69	457,63	917,35	1 368,61	4 779,05	9 482,50	14 568,74	19 512,09	24 385,44
6	Multibanco verte...	5	Afecta estado de...	Negação de serv...	2,61	8,96	33,62	78,84	133,72	839,20	1 722,08	3 438,74	4 207,78	4 965,21
7	Multibanco verte...	6	Afectação do est...	Negação de serv...	0,14	0,28	0,42	0,56	0,83	2,07	2,06	2,03	2,15	2,12
8	Multibanco verte...	7	Afectação do est...	Negação de serv...	0,00	0,00	0,00	0,00	0,14	1,53	3,06	4,87	6,54	7,51

Perda Esperada

#	Sistema	ID proc.	Processo	Ameaça	SLE	ARO	ALE
1	Multibanco verte...	1	Recepção de me...	Negação de serv...	273 973,10	12	3 287 677,25
2	Multibanco verte...	2	Recepção de ms...	Negação de serv...	273 973,10	12	3 287 677,25
3	Multibanco verte...	3	Validação de ope...	Negação de serv...	5 479,46	4	21 917,85
4	Multibanco verte...	4	Autorização de O...	Negação de serv...	731,12	4	2 924,46
5	Multibanco verte...	8	Recolha de dado...	Negação de serv...	4 748,59	4	18 994,38
6	Multibanco verte...	5	Afecta estado de...	Negação de serv...	730,10	4	2 920,39
7	Multibanco verte...	6	Afectação do est...	Negação de serv...	2,32	4	9,28

Processos Criticos

Tipo Criticidade	1º Processo	2º Processo	3º Processo
1	1	2	10
2	1	2	10
3	1	2	3
4	1	2	10
5	4	10	0
6	9	10	0

Legenda:

1 - Risco Base
2 - Risco Relativo
3 - Valor
4 - Probabil. de Falha
5 - Nº processos dependentes
6 - Nº processos condicionadores

Análise de falha

Perda Relativa

	ID proc	Processo	Ameaça	Valor activos	Valor gerado no processo	Custo Adic.	Valor activos ant.	Valor gerado no proc. ant.	Custo Adic. ant.	Valor activos dep.	Valor gerad no proc. dep.	Custo Adic. dep.	Variação
	4	Autorização de O...	Negação de serv...	177,50	279 458,90	42 707,55	177,50	493 702,98	15 207,57	177,50	450 040,29	20 061,87	-217 485,57
	5	Afecta estado de...	Negação de serv...	177,50	279 678,87	42 707,55	177,50	495 238,76	15 207,57	177,50	452 010,90	20 061,87	-219 018,79
	6	Afectação do est...	Negação de serv...	177,50	-7,38	0,00	177,50	-19,50	0,00	177,50	85,30	0,00	-40,28
	7	Afectação do est...	Negação de serv...	177,50	1 391,06	0,00	177,50	1 788,52	0,00	177,50	1 291,70	0,00	-149,05
	9	Envio de resultad...	Negação de serv...	177,50	2 301 663,80	42 707,55	177,50	3 787 786,80	15 207,57	177,50	3 502 014,71	20 061,87	-1 368 309,79
	10	Envio de resposa...	Negação de serv...	177,50	2 301 663,80	42 707,55	177,50	3 787 786,80	15 207,57	177,50	3 502 014,71	20 061,87	-1 368 309,79
			Total	**1 065,00**	**5 163 849,05**	**170 830,20**	**1 065,00**	**8 566 284,36**	**60 830,28**	**1 065,00**	**7 907 457,61**	**80 247,48**	**-3 173 313,26**

Evolução Temporal da Perda

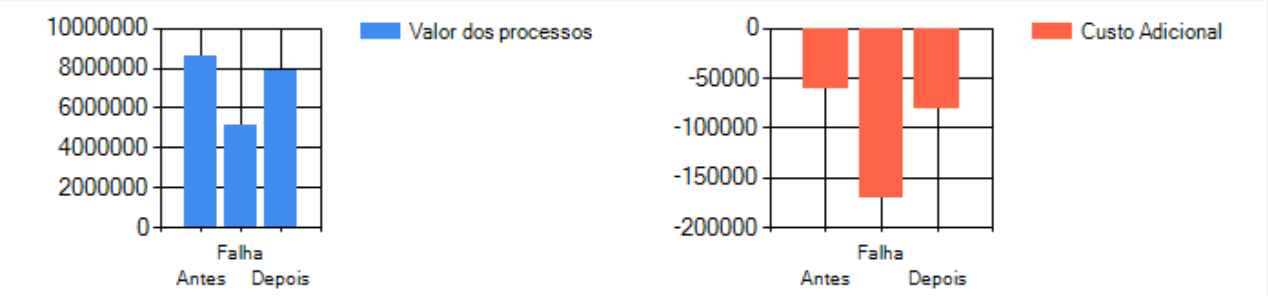
#	ID processo	Processo	Ameaça	Variação 1h	Variação 2h	Variação 3h	Variação 4h	Variação 5h	Variação 1d	Variação 2d	Variação 3d	Variação 4d	Variaç
1	4	Autorização de O...	Negação de serv...	-35 858,93	-35 779,11	-35 729,99	-35 877,67	-35 930,25	-174 554,84	-64 339,22	26 911,03	-250 328,16	
2	5	Afecta estado de...	Negação de serv...	-35 858,93	-35 779,11	-35 729,99	-35 877,67	-35 933,50	-176 064,92	-64 934,17	26 386,32	-250 830,26	
3	6	Afectação do est...	Negação de serv...	0,00	0,00	0,00	0,00	0,00	-40,28	57,66	7,07	0,81	
4	7	Afectação do est...	Negação de serv...	0,00	0,00	0,00	0,00	0,00	-149,05	-248,42	99,37	49,67	
5	9	Envio de resultad...	Negação de serv...	-30 698,17	-30 321,20	-29 081,18	-29 130,83	-31 319,09	-1 330 391,32	-735 133,97	-874 254,62	-63 798,24	
6	10	Envio de resposa...	Negação de serv...	-30 698,17	-30 321,20	-29 081,18	-29 130,83	-31 319,09	-1 330 391,32	-735 133,97	-874 254,62	-63 798,24	

Processos Criticos

Tipo Criticidade	1º Processo	2º Processo	3º Processo
1	9	10	0
3	9	10	0
5	4	5	6
6	9	0	0

Legenda:

1 - Valor de Perda
3 - Valor de processo
5 - Nº processos dependentes
6 - Nº processos condicionadores



Conclusões

- Proposta de metodologia para avaliação do risco (SI) em processos de negócio e análise de impacto no negócio.
- Aplicação num ambiente de suporte à tomada de decisão permitindo realizar simulações e análise de cenários.
- Resultados:
  - impacto no design, implementação e monitorização dos processos,
  - identificação de atividades críticas, afetação de recursos, implementação de controlos,
  - negociação de SLAs.
- Ongoing work: extensão para BPMN.

Obrigada.

Questões?