jUCMNav Report

http://www.softwareengineering.ca/jucmnav/

Title:	URNspec
Description:	
Author:	gunterm
Creation Date:	September 2, 2009 7:08:14 AM EDT
Modification Date:	September 19, 2009 12:03:46 AM EDT
Report Generation Date:	September 19, 2009 00:45:01 AM EDT
Specification Version:	183

Intentional Elements

1. Receive appropriate help in case of an incident in a timely fashion
2. Dispatch right number of resources to incidents in a timely fashion
3. Report incident
4. Handle incident efficiently
5. Report status and location without extra effort
6. Improved customer QoS metrics
7. Fast response time for mission execution
8. Ask witness only pertinent questions
9. Correctly identify location of incident
10. Assess required resources correctly
11. Assess severity and nature of incident correctly
12. Contact the closest resource location with available resources
13. Keep track of resource status
14. Low cost
15. Select the right missions based on past experience
16. Overall good performance of coordinator
17. Mission Request
18. Witness Report
19. Status Update
20. High skills of resources
21. High skills of coordinator
22. Resolve Crisis
23. Super Observer Mission
24. Rescue Mission
25. Helicopter Transport Mission
26. Remove Obstacle Mission
27. Capture Witness Report
28. Assign Internal Resources
29. Request External Resources
30. Coordinate response effectively
31. 2hrs of downtime every 30 days, failure recovery within 30sec [General Public]
32. Availability [Coordinator]
33. *
34. <<anytype>> Receive appropriate* || Improved customer*
35. <<anytype>> *
36. <<anytype>> * [2]
37. 2hrs of downtime every 30 days, failure recovery within 30sec [Government]
38. Availability [Resource]
39. <<anytype>> * [3]
40. 2hrs of downtime every 30 days, failure recovery within 30sec
41. Availability
42. Fast Recovery Time
43. Short Maintenance Time
44. Redundancy

45. Restrict access, authenticate users, encrypt communications [Government]
46. Security [Coordinator]
47. Security
48. Restrict access, authenticate users, encrypt communications
49. Improved customer*
50. Security of Terminal
51. Security of Host
52. Authentication
53. Identification
54. Access Control
55. Fingerprint
56. Password
57. Cardkey
58. Access Authorization
59. Encryption

Actors

1. General Public
2. Resource
3. Government
4. Coordinator
5. *

Strategy Legend

1:Existing System

2:New System

	Strategy Evaluations	
	1	2
Receive appropriate help in case of an incident in a timely fashion	-14	0
Dispatch right number of resources to incidents in a timely fashion	-14	31
Report incident	0	25
Handle incident efficiently	-14	0
Report status and location without extra effort	0	-25
Improved customer QoS metrics	-14	0
Fast response time for mission execution	-25	27

Ask witness only pertinent questions	0	25
Correctly identify location of incident	100	25
Assess required resources correctly	18	50
Assess severity and nature of incident correctly	75	0
Contact the closest resource location with available resources	23	62
Keep track of resource status	-25	-25
Low cost	0	0
Select the right missions based on past experience	-25	31

Overall good performance of coordinator	-14	0
Mission Request	-14	0
Witness Report	0	0
Status Update	0	-25
High skills of resources	-14	0
High skills of coordinator	-14	0
Resolve Crisis	0	100
Super Observer Mission	0	100
Rescue Mission	0	100
Helicopter Transport Mission	0	100
Remove Obstacle Mission	0	100
Capture Witness Report	0	100

Assign Internal Resources	0	100
Request External Resources	0	100
Coordinate response effectively	-25	25
2hrs of downtime every 30 days, failure recovery within 30sec [General Public]	0	0
Availability [Coordinator]	0	0
*	0	0
<<anytype>> Receive appropriate* || Improved customer*	0	0
<<anytype>> *	0	0
<<anytype>> * [2]	0	0
2hrs of downtime	0	0

every 30 days, failure recovery within 30sec [Government]		
Availability [Resource]	0	0
<<anytype>> * [3]	0	0
2hrs of downtime every 30 days, failure recovery within 30sec	0	0
Availability	0	0
Fast Recovery Time	0	0
Short Maintenance Time	0	0
Redundancy	0	0
Restrict access, authenticate users, encrypt communications [Government]	0	0

Security [Coordinator]	0	0
Security	0	0
Restrict access, authenticate users, encrypt communications	0	0
Improved customer*	0	0
Security of Terminal	0	0
Security of Host	0	0
Authentication	0	0
Identification	0	0
Access Control	0	0
Fingerprint	0	0
Password	0	0
Cardkey	0	0
Access Authorization	0	0
Encryption	0	0

Security - AoGRL

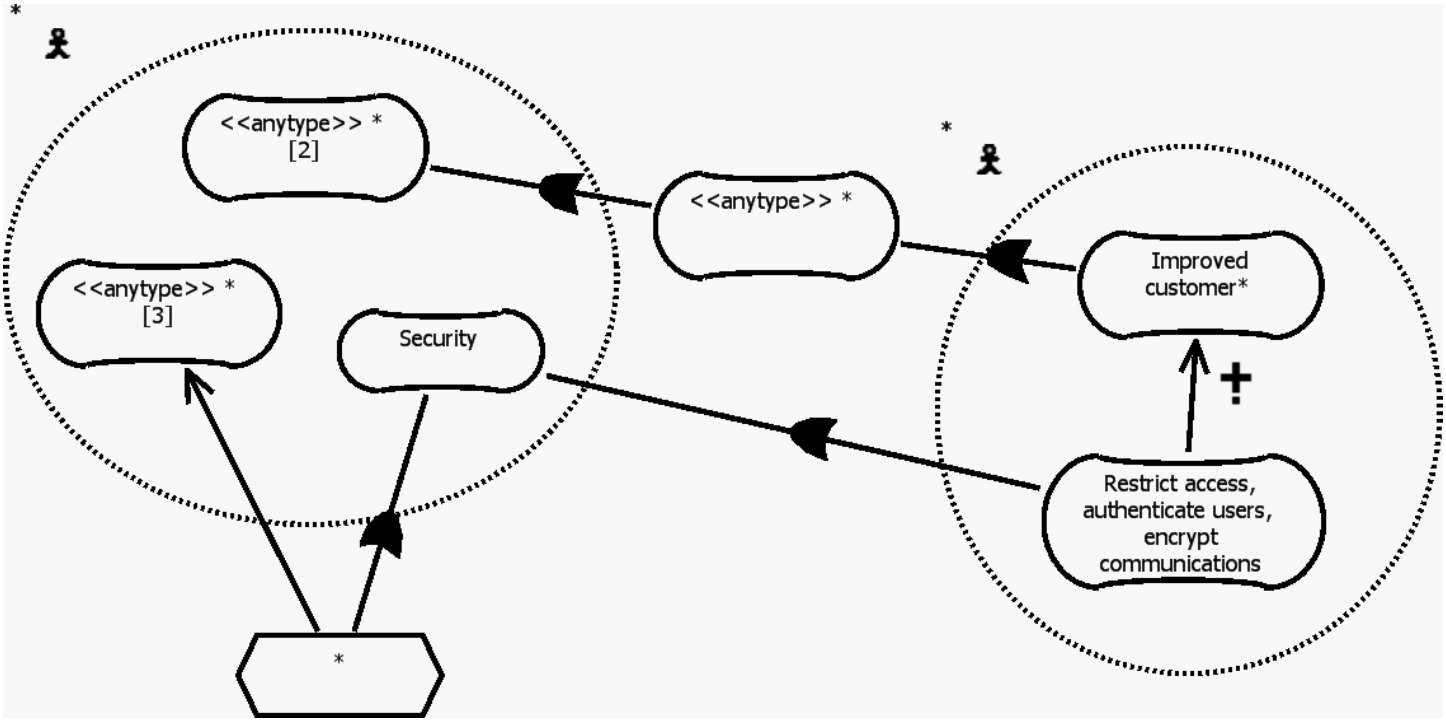

Figure 1 - Security - AoGRL

Security

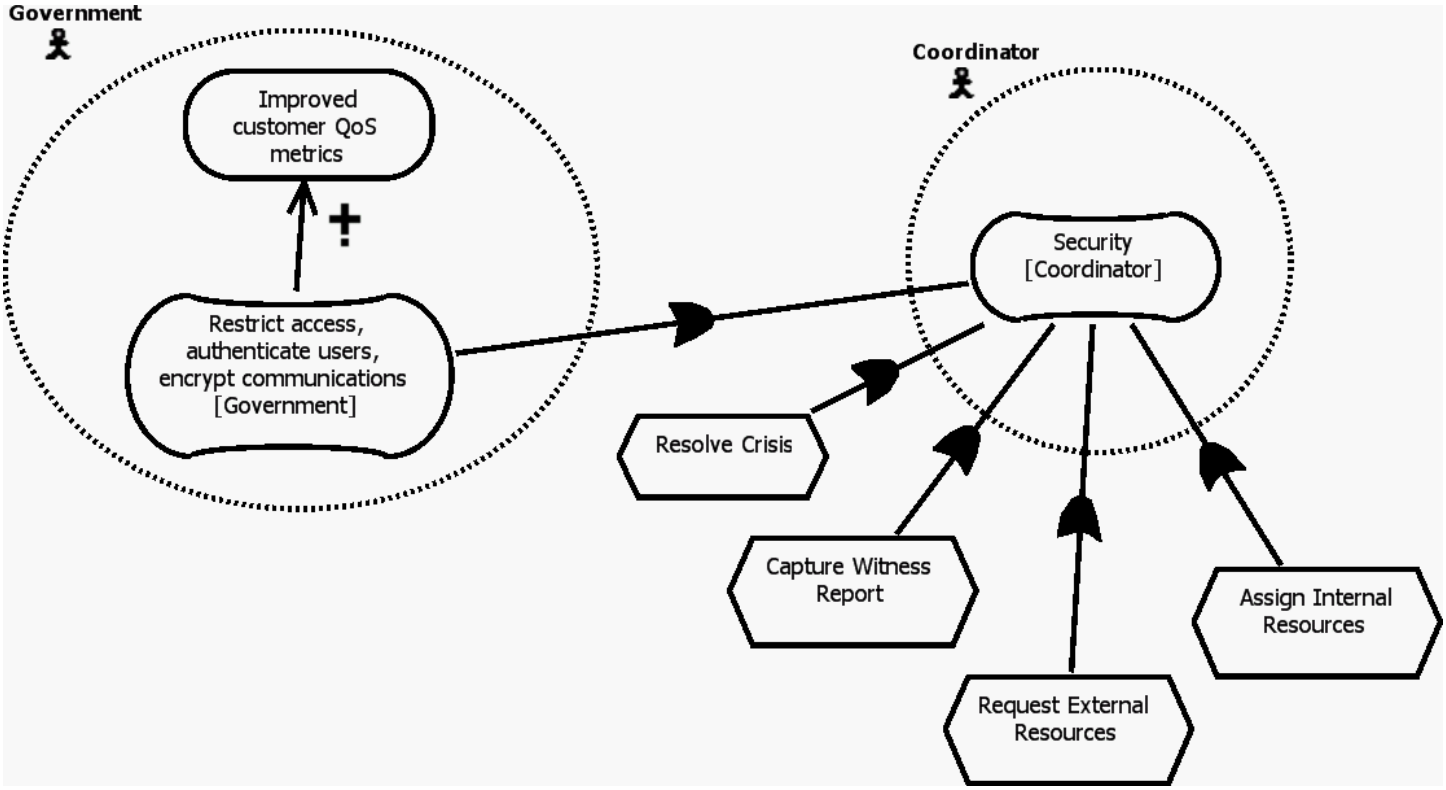

Figure 2 - Security

Availability - General

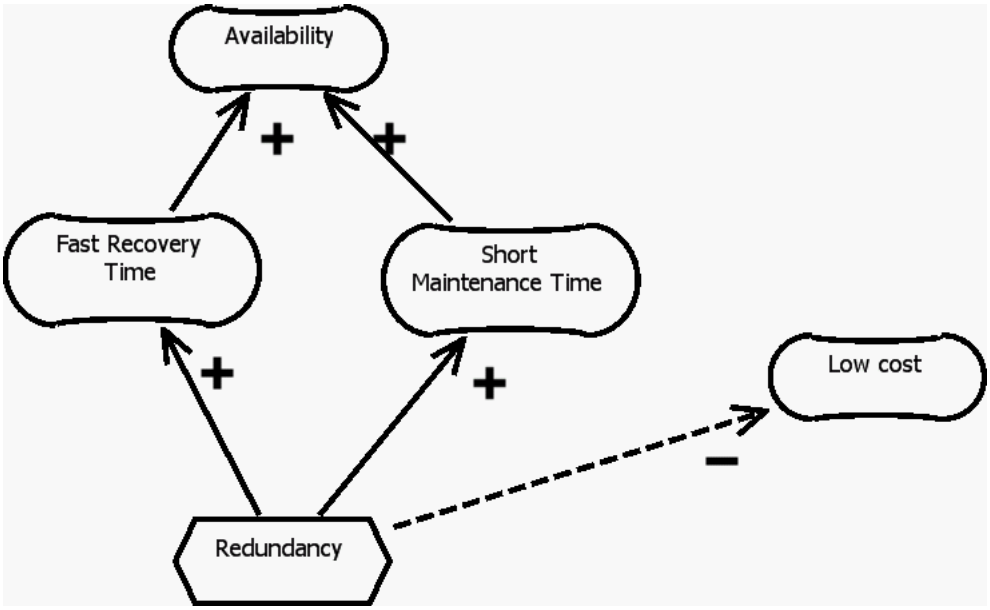

Figure 3 - Availability - General

Security - General

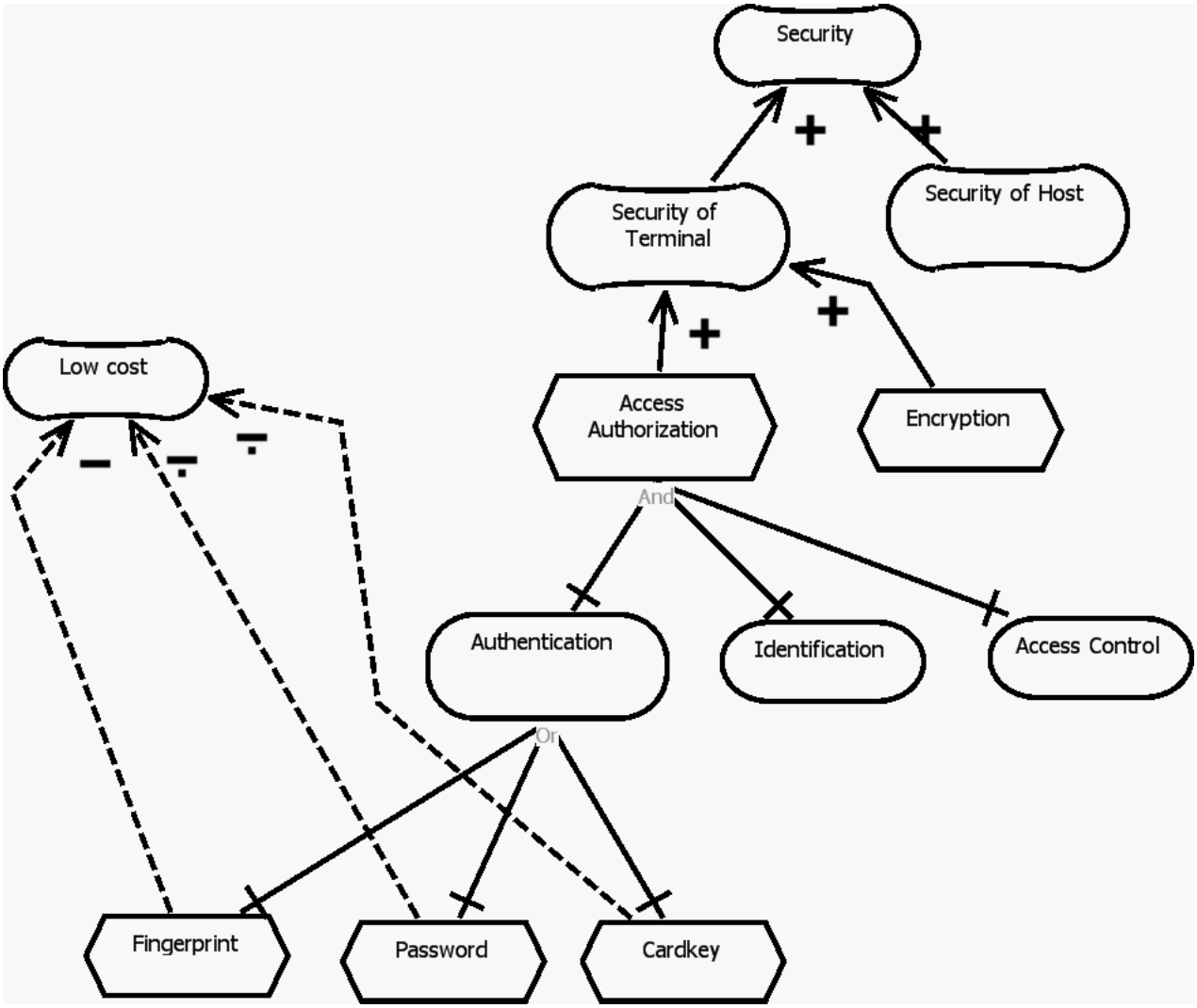

Figure 4 - Security - General

Availability - AoGRL

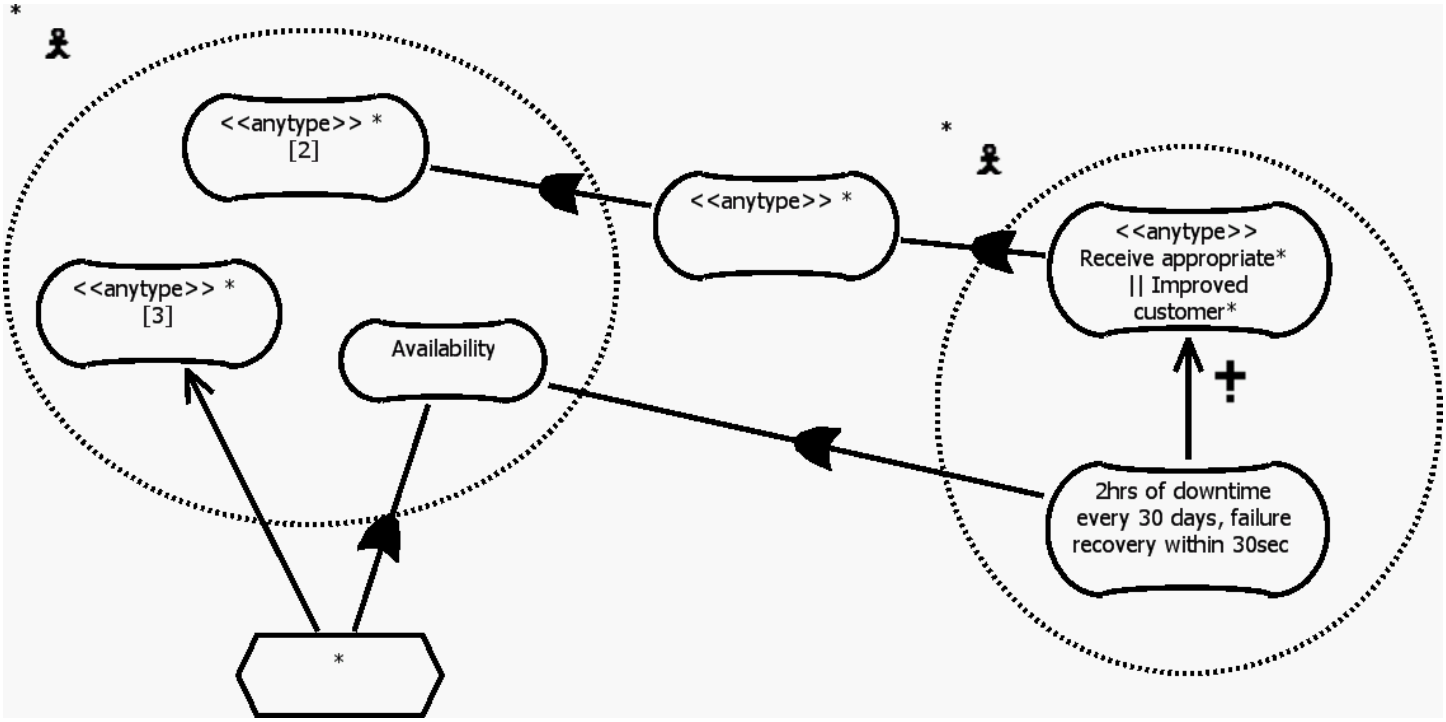

Figure 5 - Availability - AoGRL

Cost

Figure 6 - Cost

Overview

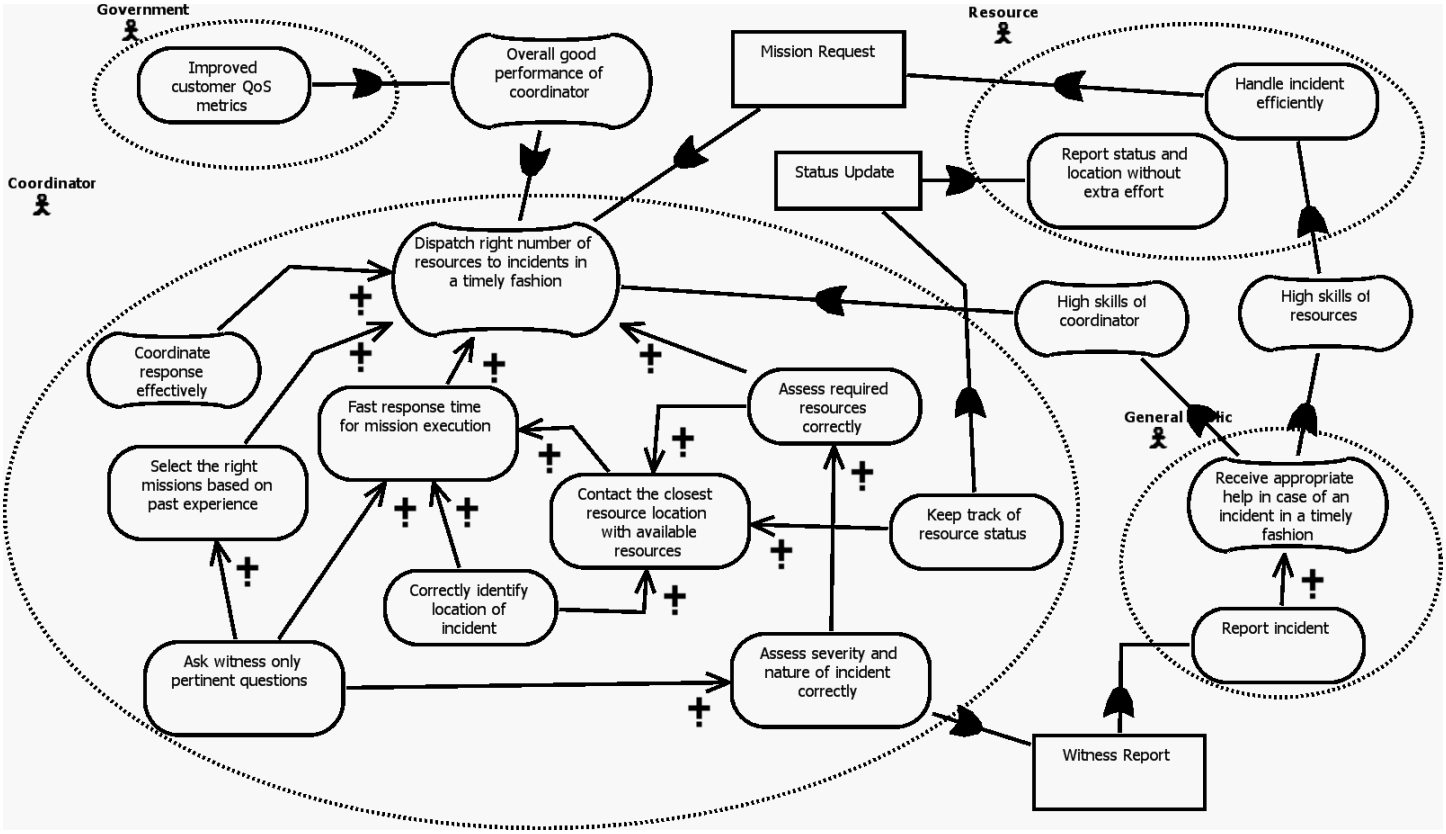

Figure 7 - Overview

Availability

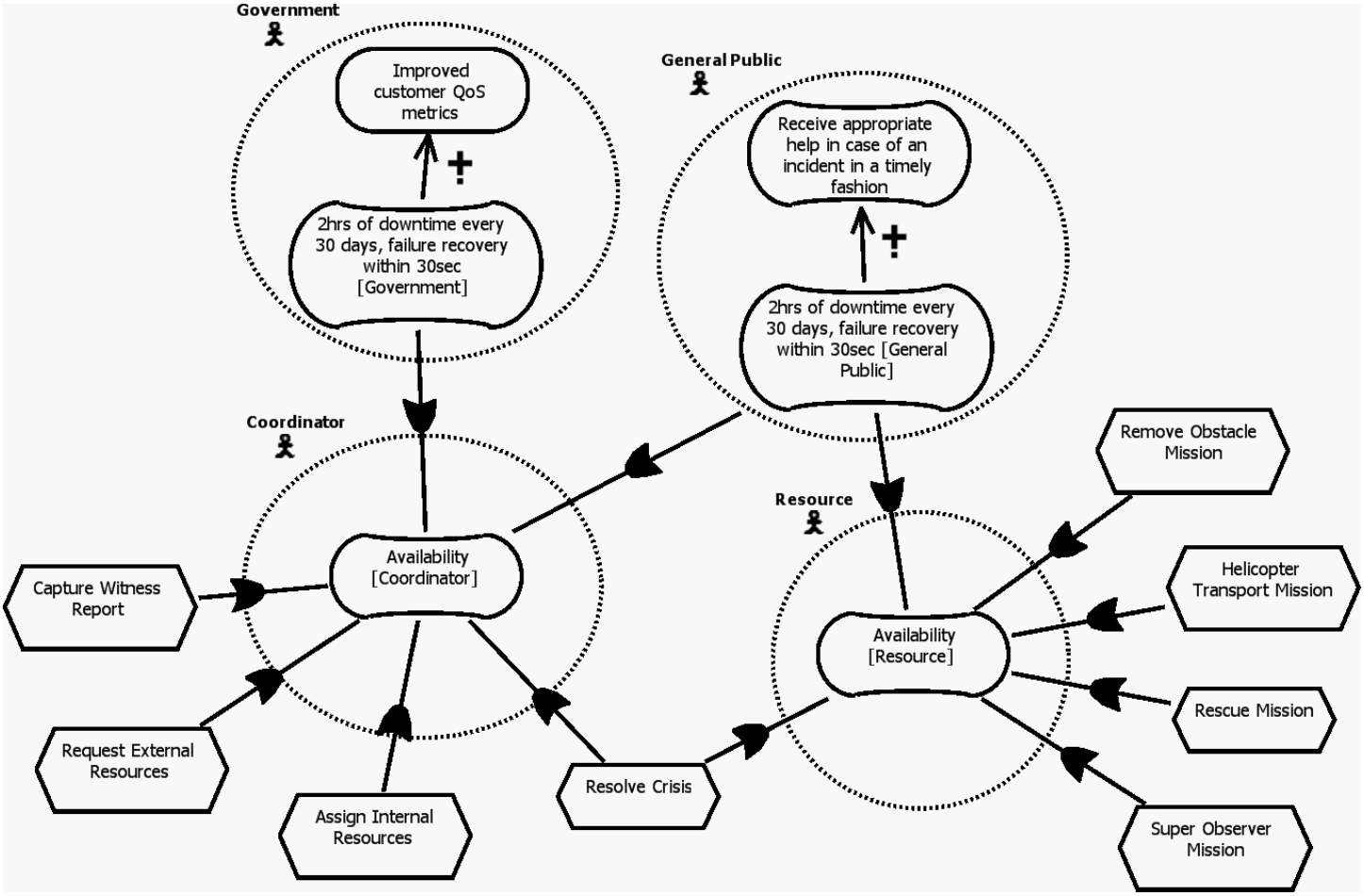

Figure 8 - Availability

Impact of Use Cases

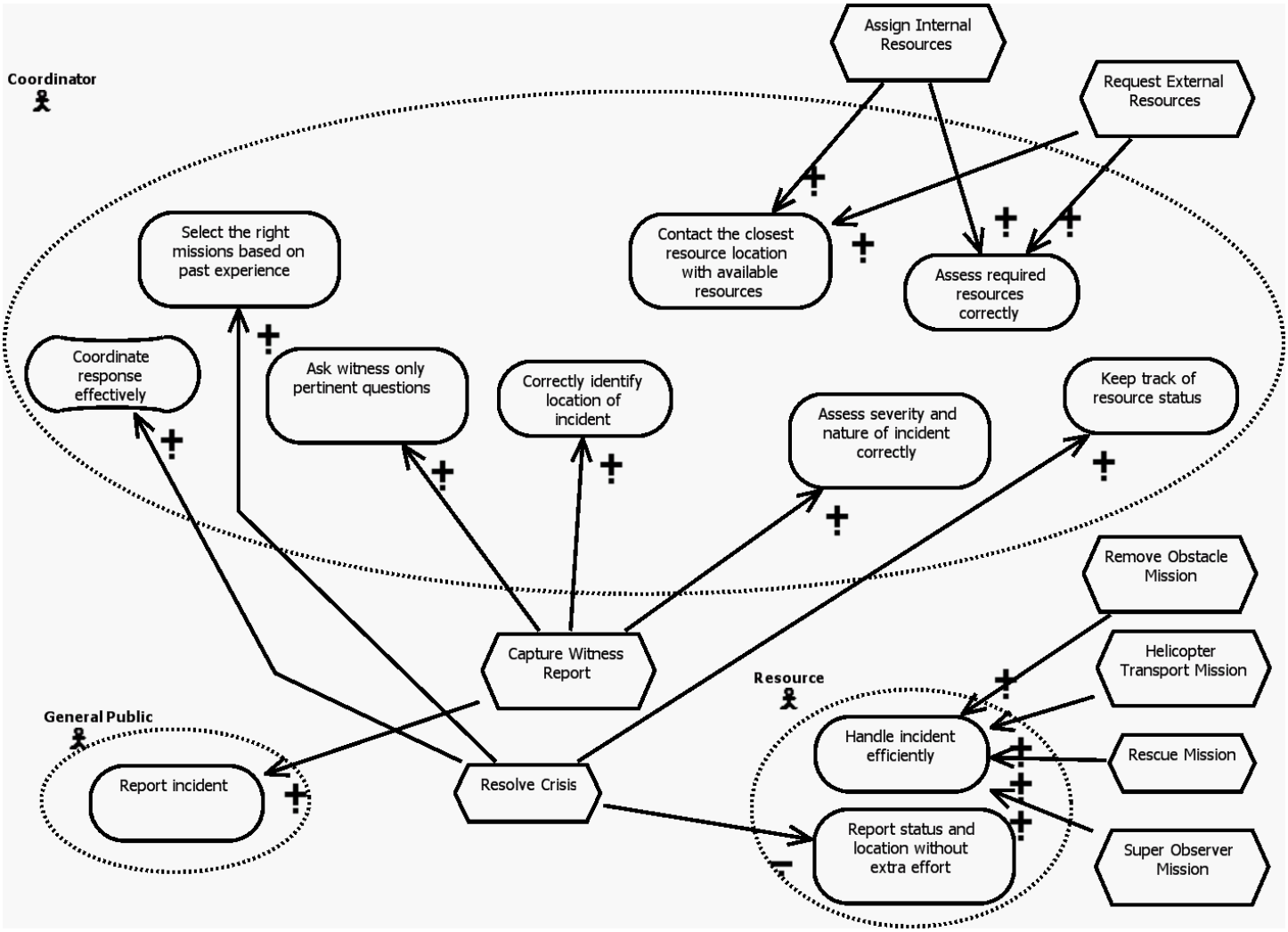

Figure 9 - Impact of Use Cases