Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Modelling Public Security Operations

Analysis of the Effect of Key Social, Cognitive, and Informational Factors with Security System Relationship Configurations for Goal Achievement

Alexis Morris

William Ross

Mihaela Ulieru

Adaptive Risk Management Lab
Faculty of Computer Science
University of New Brunswick

Scientific Authority:
Paul Chouinard
DRDC Centre for Security Science

Defence R&D Canada – Centre for Security Science
Contractor Report
DRDC CSS CR 2012-028

Canada

Scientific Authority

Paul Chouinard

DRDC Centre for Security Science

Operational Research

Approved by

Dr. Denis Bergeron

DRDC Centre for Security Science

Section Head, Operational Research

Approved for release by

Dr. Mark Williamson

DRDC Centre for Security Science

Document Review Panel Chairman

Abstract

More so than engineered systems, human factors, and specifically having humans-in-the-loop, can lead to unforeseen behaviours resulting in unexpected organizational failures. In the world of emergency response, these failures may be related not only to response activities, but also to information processing and sharing that consequently undermine the organizational ecosystems' situational awareness of unfolding events. The TIF project, Modelling Public Security Operations, has the goal of accounting for the human factor by more fully exploring its inherent complexity through experiments and simulations. This report presents the design, implementation and results of a Holistic Security Ecosystem (HSE) simulator for representing organizations and decision making processes and the impact of key social, cognitive and informational factors. Earlier research investigated key factors, processes, and simulation methodologies.

Résumé

Plus que les systèmes sophistiqués, les facteurs humains, et plus particulièrement lorsque des humains interviennent, peuvent mener à des comportements imprévus entraînant des échecs organisationnels imprévus. Dans le monde des interventions d'urgence, ces échecs peuvent être reliés non seulement aux activités d'intervention, mais aussi au traitement et à l'échange de l'information qui minent la capacité de l'organisation à jauger la situation à mesure qu'elle évolue. Le projet FIT, la modélisation des opérations de sécurité publique, vise à tenir compte du facteur humain en examinant plus amplement sa complexité inhérente au moyen d'expériences et de simulations. Le présent rapport porte sur la conception, l'instauration et les résultats de la simulation d'EHS pour représenter les organisations et le processus de prise de décisions, et pour simuler l'incidence des principaux facteurs sociaux, cognitifs et informationnels. Les principaux facteurs, processus et méthodes de simulation ont été examinés dans le cadre de précédents travaux de recherche.

Executive summary

Modelling Public Security Operations: Analysis of the Effect of Key Social, Cognitive, and Informational Factors with Security System Relationship Configurations for Goal Achievement

Alexis Morris; William Ross; Mihaela Ulieru; DRDC CSS CR 2012-028; Defence R&D Canada Centre for Security Science

Introduction or background: This report summarizes and evaluates research performed by the University of New Brunswick (UNB) in the context of the DRDC project, "*Modelling Public Security Operations*," which aims to investigate decision-making in complex meta-organizations. The UNB component of this initiative has involved the design and implementation of a simulation approach, the Holistic Security Ecosystem (HSE) simulation, for representing organizations and the decision-making process and for simulating the impact of key social, cognitive, and informational factors on the joint effectiveness of a security ecosystem. This report presents the design, implementation and results of a Holistic Security Ecosystem (HSE) simulator for representing organizations and decision making processes and the impact of key social, cognitive and informational factors. Earlier research investigated key factors, processes, and simulation methodologies.

Results: This work has presented the latest extension to the HSE simulation with the development of an improved simulator based on a comprehensive architectural design. This design has been implemented and tested on a validated scenario that builds on models proposed in previous project deliverables. The simulator incorporates key human-factor and business-process models based on a multi-dimensional approach that includes the structural, functional, normative, cognitive, social, information, and physical dimensions. The main objective of the research documented in this report —namely, to present the analysis of the effect of key social, cognitive, and information factors, as well as configuration relationships, on goal achievement—has been shown for the domain of information sharing and the goal of joint-consensus achievement. The experimental results indicate that the tested parameters within the cognitive factor set outweigh the parameters in both the social and the information factor sets.

Significance: This work has laid the foundation for future multi-agent systems analysis of the impact of human factors on organizational outcomes by addressing the following key concerns: (i) the selection of a method to capture and discuss fuzzy human factors, (ii) a design approach for including human factors within agents, (iii) a methodology for conducting simulated human-factor analysis, and (iv) the development of a proof-of-concept simulator for testing multiple human-factor configurations. Although there remains much to be added, the current HSE simulation tool provides a usable and extensible tool for investigating human factors.

Future plans: Future work will involve the documentation of "lessons learned" throughout the course of this research.

Sommaire

Modélisation des opérations de sécurité publique : Analyse de l'incidence des principaux facteurs sociaux, cognitifs et informatifs avec la configuration de la relation du système de sécurité sur l'atteinte des objectifs

Alexis Morris; William Ross; Mihaela Ulieru; RDDC CSS CR 2012-028; Centre des sciences pour la sécurité de R & D pour la défense Canada

Introduction ou contexte : Ce rapport résume et évalue les recherches effectuées par l'Université du Nouveau-Brunswick (UNB) dans le contexte du projet de modélisation des opérations de sécurité publique de RDDC, qui vise à étudier la prise de décisions dans des métaorganisations complexes. Dans cette étude, les travaux de l'UNB comportaient la conception et l'instauration de l'approche de la simulation d'écosystèmes holistiques de sécurité (EHS) pour représenter les organisations et le processus de prise de décisions, et pour simuler l'incidence des principaux facteurs sociaux, cognitifs et informationnels sur l'efficacité globale d'un écosystème de sécurité. Le présent rapport porte sur la conception, l'instauration et les résultats de la simulation d'EHS pour représenter les organisations et le processus de prise de décisions, et pour simuler l'incidence des principaux facteurs sociaux, cognitifs et informationnels. Les principaux facteurs, processus et méthodes de simulation ont été examinés dans le cadre de précédents travaux de recherche.

Résultats : Les présents travaux portent sur le dernier ajout à la simulation d'EHS, avec l'élaboration d'une modélisation basée sur une conception architecturale complète. Ce concept a été mis en place et mis à l'essai à l'aide d'un scénario validé inspiré de modèles proposés avec les produits livrables de projets précédents. La simulation comprend des modèles de facteurs humains et de processus opérationnels importants créés en fonction d'une approche incluant les dimensions structurelles, fonctionnelles, normatives, cognitives, sociales, informationnelles et physiques. L'objectif principal de la recherche présentée dans ce rapport – à savoir, l'analyse de l'incidence des principaux facteurs sociaux, cognitifs et informationnels, de même que la configuration des relations sur l'atteinte des objectifs – a été établi pour le domaine d'échange d'information et l'atteinte d'un consensus. Les résultats expérimentaux démontrent que les paramètres analysés des facteurs cognitifs surpassent ceux des facteurs sociaux et informationnels.

Importance : Ces travaux ont ouvert la voie à la future analyse de systèmes multi agents concernant l'incidence des facteurs humains sur les résultats organisationnels, en abordant les principales préoccupations suivantes : (i) la sélection d'une méthode pour saisir des facteurs humains flous et en discuter; (ii) une approche de la conception permettant d'inclure les facteurs humains dans les agents; (iii) une méthodologie pour effectuer des analyses simulées des facteurs humains; (iv) l'élaboration d'une simulation basée sur la validation des faits pour mettre à l'essai les multiples configurations de facteurs humains. Même si d'autres améliorations sont nécessaires, la simulation d'EHS actuelle constitue un outil utile et ajustable pour analyser les facteurs humains.

Perspectives : Les travaux futurs incluront la documentation des leçons retenues tout au long de cette recherche.

Table of contents

List of figures

List of tables

1 Overview

The DRDC TIF initiative entitled "*Modelling Public Security Operations,"* [1], aims at exploring decision-making in complex meta-organizations through the study of human factors and their impact on the operational capacities of organizations. As one of the key partners in this initiative, the University of New Brunswick has been charged with the design and development of simulation studies related to this topic (specifically investigating simulation methods and tools for representing organizations and human factors). Over the course of this study, three earlier deliverables, [2, 3, 4] have presented relevant key factors, processes, and simulation methodologies: the first, [2], presented a proof-of-concept simulator for emergency response—known as the Holistic Security Ecosystem (HSE) simulator—that explored the response to a harbour fire; the second, [3], presented social, cognitive, and informational models that could be used to extend the initial simulator design and which shifted the focus of the study from emergency response to consensus building; and the third, [4], presented the findings from a verification and validation workshop in which the new problem domain scenario and initial human factor models were examined by a team of experts.

This deliverable presents the design, implementation, and results of the new HSE simulator, which transitions the problem domain from one of joint-response to one of joint-threat-detection. This is highly relevant as it focuses human-factor elements toward a very common and critical practice: information sharing.

1.1 Project Objective & Milestones

Below are the primary outcomes for the TIF research on the development and analysis of tools, techniques, and best practices for modelling public security operations. The current deliverable is highlighted, and its objectives are discussed in the following section.

1. Design of the HSE simulation (Oct 2009)
2. Implementation of the HSE simulation (Jan 2010)
3. Extension of the HSE simulation to include social, cognitive, and informational conceptual models (Sept 2010)
4. Verification of the extended HSE simulation (Dec 2010)
5. Analysis of the effect of key social, cognitive, and informational factors (Aug 2011)
6. Analysis of the effect of security system relationship configurations on goal achievement (Aug 2011)
7. Evaluation of the HSE “proof of concept” (Feb 2012)

1.2 Deliverable Objectives

The current document serves as a combined deliverable of project milestones 5 and 6, which represent the analysis of the effect of key social, cognitive, and informational factors, as well as configuration relationships, on the achievement of joint-consensus. It presents an improved HSE

simulator and the design of experiments showing the effect of these key factors on goal achievement. While the simulation results are of importance, the primary focus of this deliverable is on the applicability of the improved simulator as a general tool for analysis.

2 Background

The early approach to the HSE Simulation problem provided a proof-of-concept simulation of a meta-organization of joint-responders, as well as an early process: from modelling to execution to results (see Figure 1). It proposed the use of core components involving the OperA multi-agent modelling methodology, [10], and a corresponding implementation in the Brahms Agent Environment, [9]. Furthermore, the simulation results underscored the usefulness of the approach for developing agents according to standard policies.

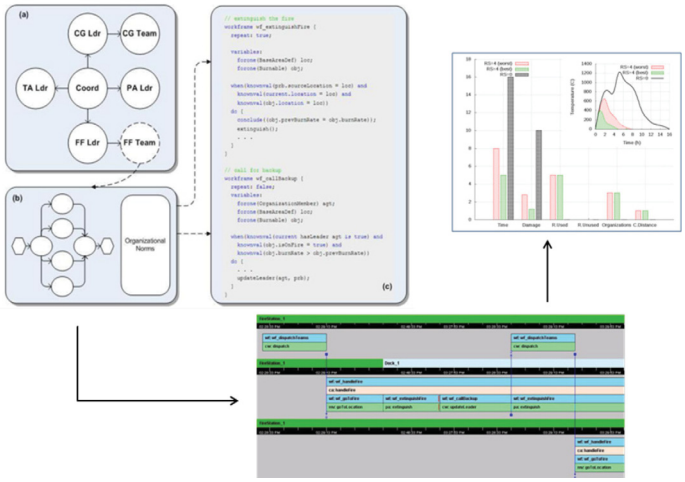


Figure 1: The early HSE simulation process showing modelling, execution, and results.

The development of the earlier HSE highlighted the five-dimensional approach for modelling agents according to their structural, functional, human, normative, and physical characteristics. These were extended to a more developed methodology involving seven key dimensions, which expanded human into cognitive and social components and which also included an information dimension (see Figure 2).

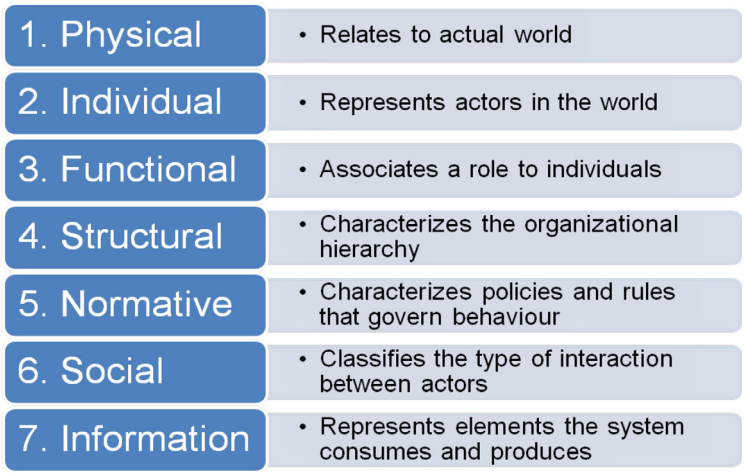


Figure 2: The seven dimensional modelling perspective.

2.1 Early HSE Human Factor Models

The previous deliverable presented the key human factors in the HSE simulation, which were validated by expert stakeholders in the field as being those of interest for experimentation. All of the human factors have been partitioned according to four dimensions: human, functional, normative, and structural. These factors are shown in Figure 3, and include culture and stress, which models appear in academic literature and rely on the multi-dimensional modelling approach [6, 7, 8, 11].

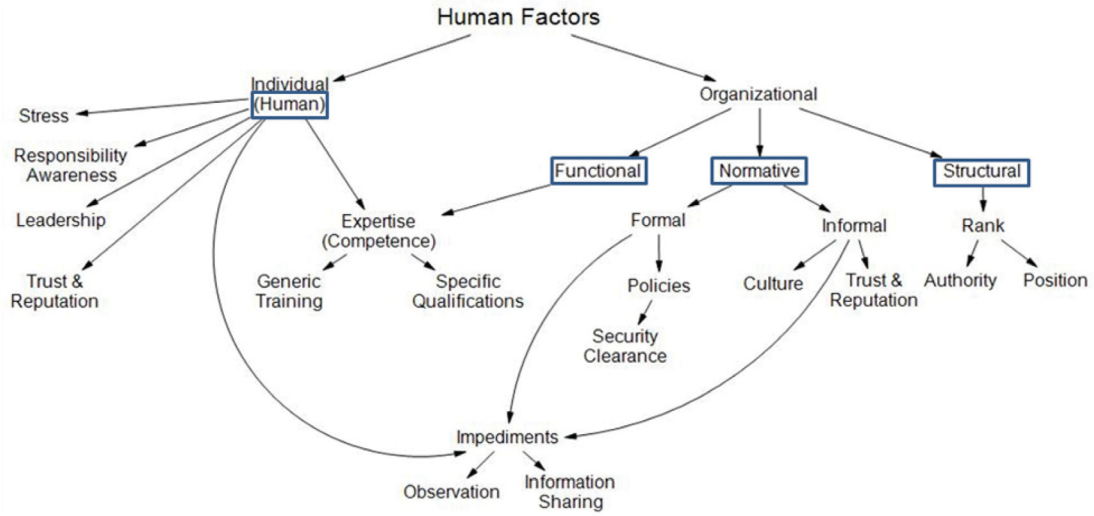


Figure 3: Human factors identified and included in the simulation design.

Figure 4 and 5 expand upon the two impediments listed in Figure 3: respectively, impediments to information sharing and impediments to observation. These have been highlighted in the previous deliverable and incorporated into the improved HSE simulator.

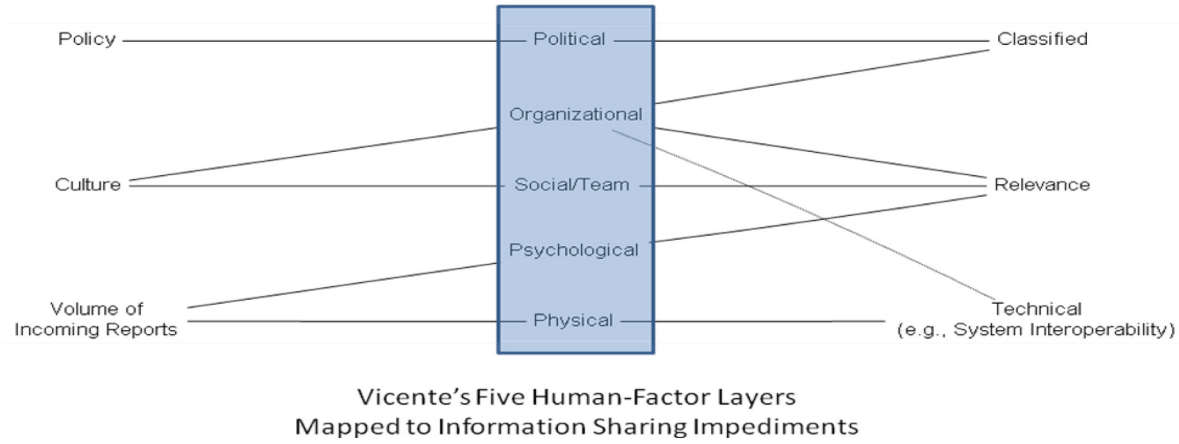


Figure 4: Impediments to information sharing, according to Vicente's human-factor layers.

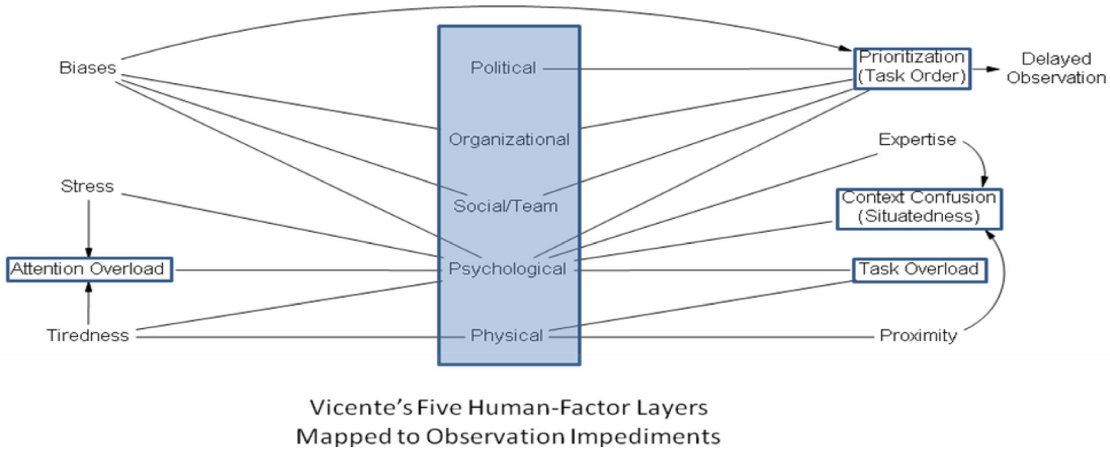


Figure 5: Observation impediments used in the simulation, according to Vicente's Human Factor layers.

3 Scenario: Modelling and Simulating Consensus with HSE

This section outlines the consensus problem and presents the key agents, as described in the previous deliverable. It also presents the scenarios, from the previous deliverable, which detail the time to a critical event within a generic port loosely based on the Halifax harbour.

Consensus is here considered as the agreement among a group of agents, based on their unique perspectives of global events, about whether or not an incident is an imminent threat. In terms of event horizon, where an incident occurs at time 0, the consensus problem occupies the range between -2 and 0 (see Figure 6).

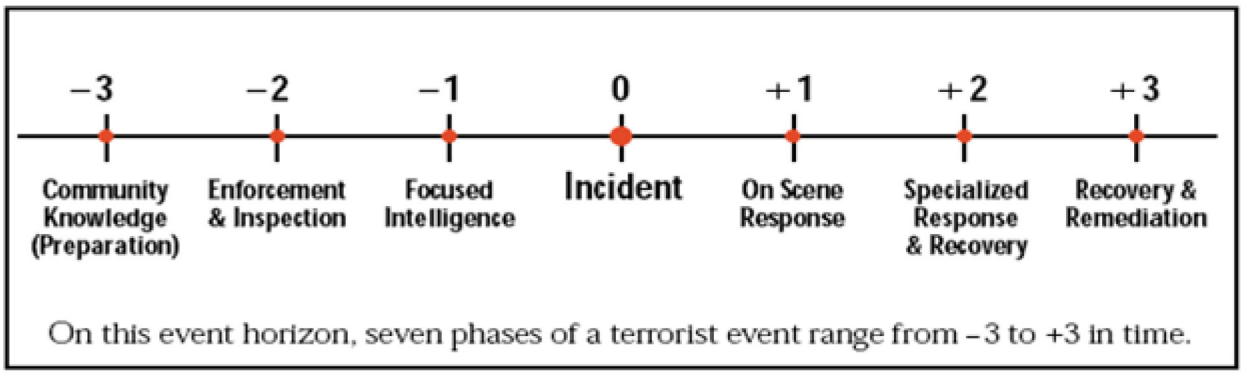


Figure 6: The event horizon leading to an incident and response. Focus of the deliverable is -3 to 0.

3.1 Scenario Background

- The Canadian government has decided to allow offshore drilling close to an environmentally sensitive area. A port near to the proposed site is busy constructing a new dock to support the drilling operation.
- A fictional protest group, calling themselves *Freedom of the Sea*, has voiced its opposition to the decision and has published a manifesto calling on all Canadians and others to aid them in their fight against the "destructors of the environment." This group has already staged several well-attended protests and has received international attention and support.
- The group decides to send a strong message, and in this study, two scenarios are considered: a domestic attack and an offshore attack.
- Level-0 Organizations and Roles are seen in Figure 7 below, which has been cross-validated from the previous deliverable and used as the simulation base.

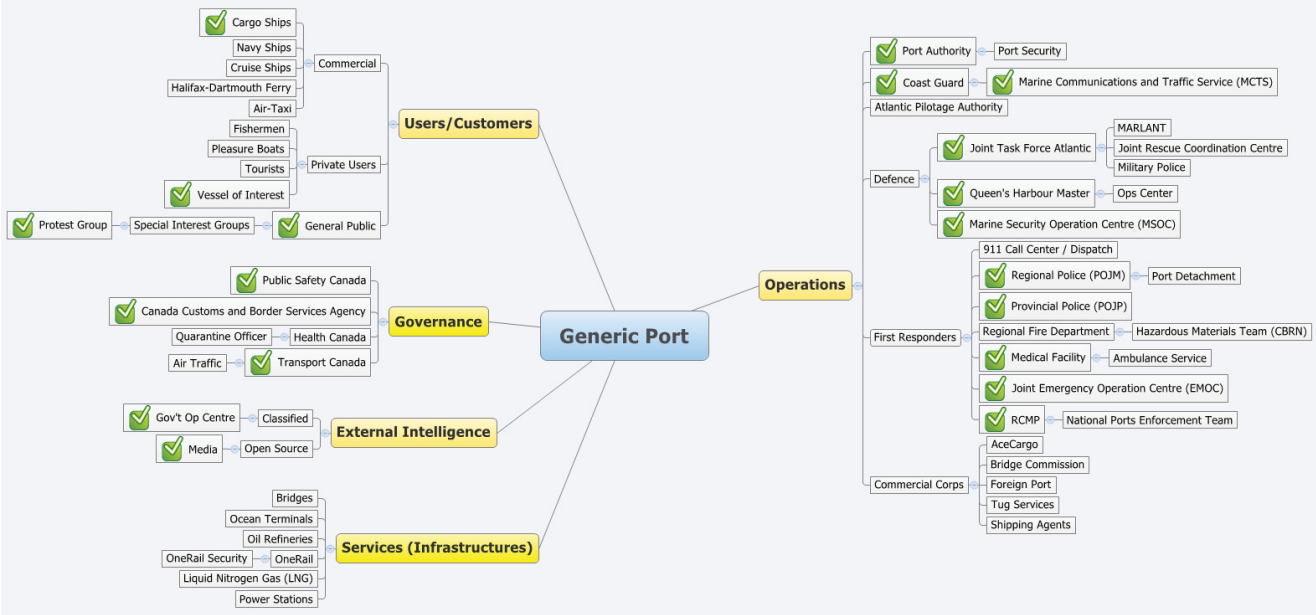


Figure 7: The HSE generic port overview diagram showing key organizations and units. The check marks indicate agents in the final simulation.

3.2 Indicators

Routine and non-routine events developed for simulation are shown below. Routine events (see Figure 8) are those daily activities considered by the organization to be normal. Although they are non-threatening, agents are unaware if they are a part of a larger scheme. Additionally, these events result in additional "noise" in the system that affects the reception level a person has for observing other events.

Non-routine events (see Figure 9) are those activities considered by the organization to be out-of-the-ordinary, potentially involving procedures that are rarely used or requiring action that falls outside of the procedures document. These are weighed internally by an organization to determine if they are part of a serious larger-scale threat.

Simulated Routine Events	
Number	**Indicator**
1	Vessel or agent submits pre-arrival information report 96hrs before arrival (PAIR)
2	Vessel submits pre-arrival check in 24hrs before arrival
3	Vessel or agent submits pre-arrival information report 96hrs before arrival (PAIR)
4	Vessel submits pre-arrival check in 24hrs before arrival
5	Pilot embarks
6	Vessel is cleared for entry
7	Pilot of large vessel requests tug boat support
8	Vessel submits pre-departure clearance forms
9	Vessel is cleared for departure
10	Pilot of large vessel requests tug boat support
11	Tug boats arrive to vessel
12	Non-conventional large vessel applies for movement clearance for entry/departures
13	Water-born commercial activity (tugs, ferries, fueling barge, tour-boats, diver operations, fisherman)
14	Cruise ship activities
15	Air-Taxi activities
16	Cargo ship activities
17	Naval vessel movement in harbour
18	Tides and current changes
19	Weather conditions (e.g., fog)

Figure 8: Routine events.

Simulated Non-Routine Events	
Number	**Indicator**
1	Warnings and alerts
2	Large quantities of explosives reported missing in port of origin
3	Police infiltration intelligence
4	Heightened alert
5	Purchasing and fitting out a ship
6	Purchases of large quantities of fertilizer
7	Embarkation of a large number of barrels of petroleum, oils, lubricants (POL)
8	Reports of explosions, particularly in rural or wooded areas.
9	Inquiring about operations, equipment, assets, or security measures about which they should have no job-related issues; Or employees using video camera/observation equipment that is not job related.
10	Victim with chemical burns, missing fingers / hands, and potentially not forthcoming about how incident occurred.
11	Press releases of possible attacks
12	Declaration of MARSEC 2
13	Causing a fire or explosion, conducting blasting or setting off fireworks, including setting a flare or other signalling device without port approval
14	Casting adrift a ship
15	A telephone call, postal mail, or email making threat.
16	Conducting a demonstration or protest in the port.
17	Police infiltration intelligence about infiltrated ships en route to halifax crew reports
18	Transporting/loading Ammonium nitrate (fertilizer product) on board a ship (without port approval)
19	Declaration of MARSEC 3
20	Dead ship moves without port approval
21	Distress call over radio to CCT-MCTS, or other vessel
22	Reports of a struggle/ takeover/ weapons seen onboard vessel of interest (VOI)
23	Missed pilot/vessel communication checkpoint or loss of communication
24	Vessel diverts from planned track (radar detection)
25	Taking off or landing a sea-plane without port approval
26	Inability to establish communications with aircraft
27	COLLISION/Grounding
28	Man overboard

Figure 9: Non-routine events.

3.3 Timeline – Problem 1

These events have been included in a potential timeline for an attack on the generic port. The two scenarios and their timelines are reiterated below from the previous deliverable. It should be noted that the event-horizon for each begins at least three months prior to the incident and progresses from long-term to mid-term to near-term. In addition, the "active" problem used in the current simulation is Problem 1: the domestic attack.

Problem 1 (one possible variation)

A local branch of the protest group has purchased a boat and is reinforcing the hull. The group has performed further demonstrations and more are being planned. A large quantity of fertilizer has been purchased from stores within 100 km of the dock, and an anonymous threat arrives that failure to abort the planned offshore drilling will be met with violence. There has also been increased vandalism around the dock. Despite their efforts, the decision still stands, so some members of the group decide to retaliate according to a plan: drive the boat into the harbour, stage a distraction (e.g., man over board), and let the dead boat filled with explosives drift/motor into an important port structure.

Domestic Attack from Local Source: Collision with Port Structure			Problem 1 Timeline												
Event Type	**Timeline Ordering**	**Indicator**	**Over 3 Months**	**Week 12**	**Week 11**	**Week 10**	**Week 9**	**Week 8**	**Week 7**	**Week 6**	**Week 5**	**Week 4**	**Week 3**	**Week 2**	**Week 1**	**D-Day**
Non Routine	**Long-term**	Warnings and alerts	X													
Non Routine	**Mid-term**	Purchasing and fitting out a ship		X												
Non Routine	**Mid-term**	Heightened alert						X								
Non Routine	**Mid-term**	Press releases of possible attacks						X	X							
Non Routine	**Mid-term**	Inquiring about operations, equipment, assets, or security measures about which they should have no job-related issues; Or employees using video camera/observation equipment that is not job related.						X	X	X						
Non Routine	**Mid-term**	Conducting a demonstration or protest in the port.						X	X	X						
Non Routine	**Near-term**	Causing a fire or explosion, conducting blasting or setting off fireworks, including setting a flare or other signalling device without port approval						X	X	X	X	X	X	X		
Non Routine	**Mid-term**	***Declaration of MARSEC 2***								X						
Non Routine	**Near-term**	Purchases of large quantities of fertilizer										X				
Non Routine	**Mid-term**	Victim with chemical burns, missing fingers / hands, and potentially not forthcoming about how incident occurred.										X				
Non Routine	**Mid-term**	Reports of explosions, particularly in rural or wooded areas.										X	X			
Non Routine	**Near-term**	Casting Adrift a Ship												X		
Non Routine	**Near-term**	Dead ship moves without port approval												X		
Non Routine	**Near-term**	***Declaration of MARSEC 3***												X		
Non Routine	**Near-term**	Embarkation of a large number of barrels of petroleum, oils, lubricants (POL)													X	
Non Routine	**Near-term**	Transporting/loading ammonium nitrate (fertilizer product) on board a ship (without port approval)													X	
Non Routine	**Near-term**	A telephone call, postal mail, or email making threat.													X	X
Non Routine	**Near-term**	Distress call over radio to CCT-MCTS, or other vessel														X
Non Routine	**Near-term**	Taking off or landing a sea-plane without port approval														X
Non Routine	**Near-term**	Inability to establish communications with aircraft														X
Non Routine	**Near-term**	COLLISION/Grounding														X

Figure 10: Problem 1 timeline showing events leading up to an incident.

3.4 Timeline – Problem 2

Problem 2 (one possible variation)

Radical members from the protest group, with previous sailing experience, decide to infiltrate a foreign ship coming to the port of interest. Meanwhile, additional protests are taking place on Canadian soil. Intelligence sources warn of a possible attack at Canadian ports by ships en route from Amsterdam. A ship coming from Amsterdam into Canada has a known member of the protest group on board. The ship submits all of its pre-arrival reports on time and is allowed into the port. As the pilot begins navigating the ship into the harbour, the members of the protest group and their sympathizers on board take control of the ship. They then navigate the ship into an important port structure.

Domestic Attack from Offshore Source: Collision with Port Structure			Problem 2 Timeline												
Event Type	**Timeline Ordering**	**Indicator**	**Over 3 Months**	**Week 12**	**Week 11**	**Week 10**	**Week 9**	**Week 8**	**Week 7**	**Week 6**	**Week 5**	**Week 4**	**Week 3**	**Week 2**	**Week 1**	**D-Day**
Non Routine	**Long-term**	Warnings and alerts	X													
Non Routine	**Near-term**	Police infiltration intelligence				X										
Non Routine	**Mid-term**	Press releases of possible attacks						X	X							
Non Routine	**Mid-term**	Inquiring about operations, equipment, assets, or security measures about which they should have no job-related issues; Or employees using video camera/observation equipment that is not job related.						X	X	X						
Non Routine	**Mid-term**	Conducting a demonstration or protest in the port.						X	X	X						
Non Routine	**Near-term**	Causing a fire or explosion, conducting blasting or setting off fireworks, including setting a flare or other signalling device without port approval						X	X	X	X	X	X	X		
Non Routine	**Mid-term**	***Declaration of MARSEC 2***								X						
Non Routine	**Mid-term**	Large quantities of explosives reported missing in port of origin										X	X			
Non Routine	**Mid-term**	Police infiltration intelligence about infiltrated ships en route to halifax Crew Reports												X		
Non Routine	**Near-term**	Dead ship moves without port approval												X		
Non Routine	**Near-term**	***Declaration of MARSEC 3***													X	
Routine	**Near-term**	Vessel or agent submits pre-arrival information report 96hrs before arrival (PAIR)													X	
Routine	**Near-term**	Vessel submits pre-arrival check in 24hrs before arrival													X	
Non Routine	**Near-term**	A telephone call, postal mail, or email making threat.													X	X
Non Routine	**Near-term**	Distress call over radio to CCT-MCTS, or other vessel														X
Non Routine	**Near-term**	Reports of a struggle/ takeover/ weapons seen onboard vessel of interest (VOI)														X
Non Routine	**Near-term**	Missed pilot/vessel communication checkpoint or loss of communication														X
Non Routine	**Near-term**	Vessel diverts from planned track (radar detection)														X
Non Routine	**Near-term**	Taking off or landing a sea-plane without port approval														X
Non Routine	**Near-term**	Inability to establish communications with aircraft														X
Non Routine	**Near-term**	COLLISION/Grounding														X

Figure 11: Problem 2 timeline showing events leading up to an incident.

3.5 Simulation Process Model

The objective of the simulator is to test the various factors that impact information sharing to determine under what conditions the organizations involved can agree that an incident is imminent (and, conversely, under what conditions they are unable to reach consensus). The business process model for information sharing used by all agents in the simulation is captured in Figure 12.

When an event (marked by an indicator) takes place, the agent has the potential to *observe* it, provided the agent is not being impeded by any observation impediments. The agent will then *document* the indicator and perform a *risk check* to determine if it is associated with an incident (or problem). If it is, the agent has the option to *publish* the indicator to other agents in the system (i.e., share information); however, the agent may be impeded by various publishing impediments.

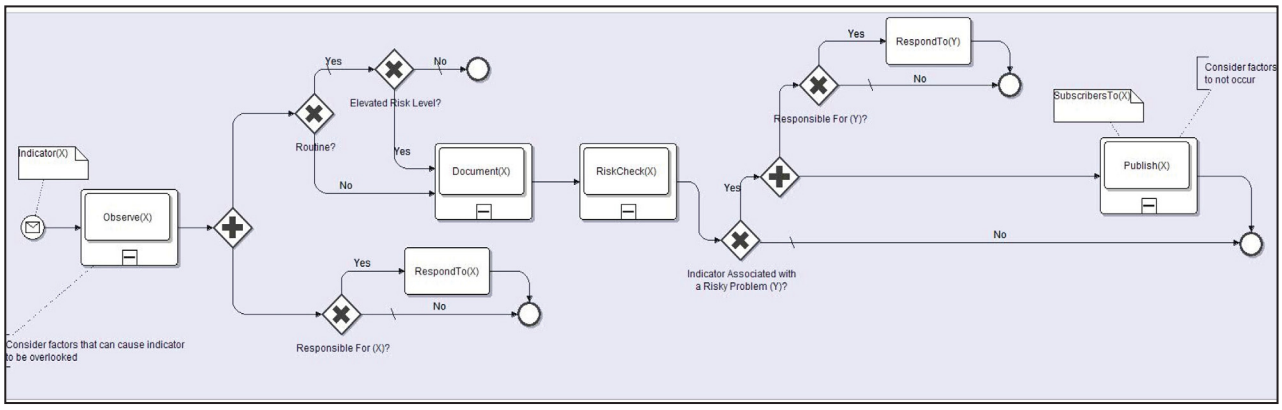


Figure 12: The information sharing model as a business process.

In the current study, the success of the safety-and-security community will depend on whether its members reach consensus regarding the domestic attack. The exact definition of consensus is left

to the analyst. However, the process model is shown in Figure 13, in which consensus is defined as some percentage of the community that agrees an incident is imminent.

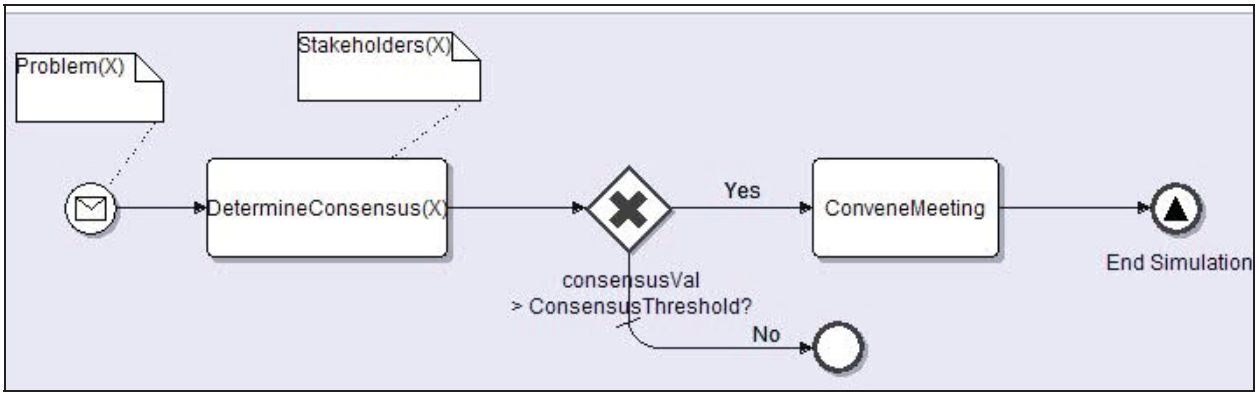


Figure 13: Determining a consensus.

3.6 System Dynamics View of Simulation Process Model

These business processes have been incorporated into a causal loop model (see Figure 14), along with the various human factors and impediments, showing the overall relationships of the components that have been included in the simulation.

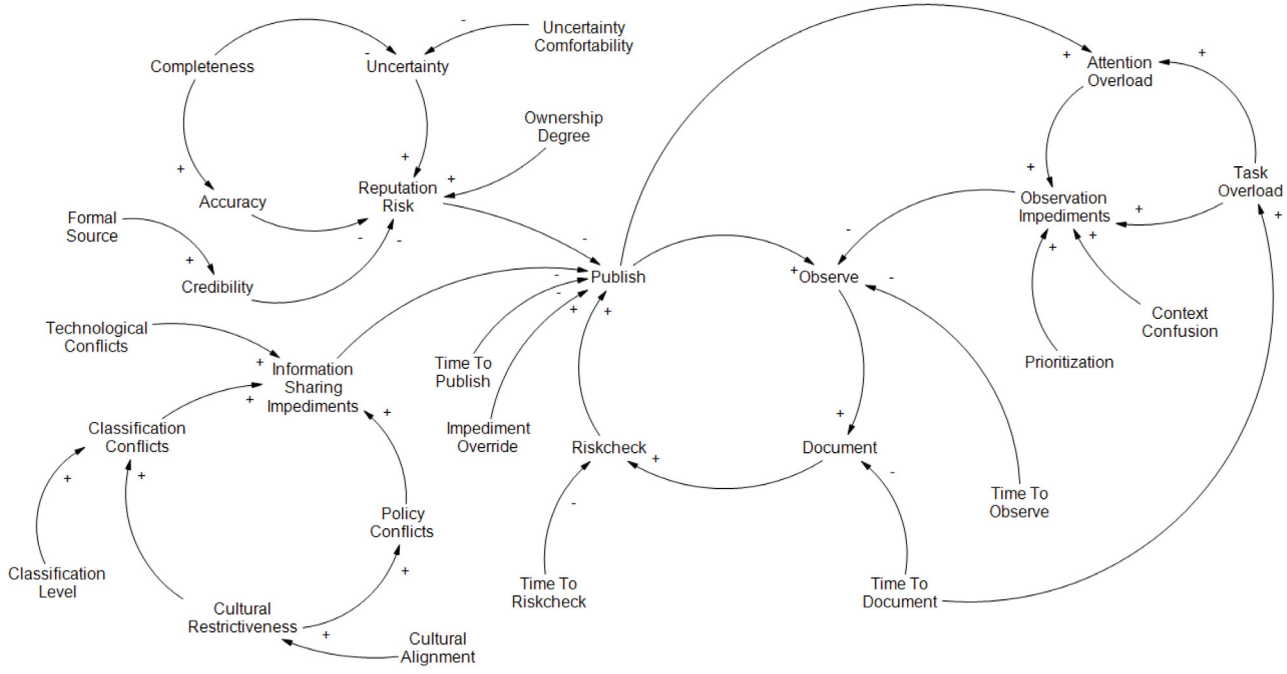


Figure 14: System dynamics incorporated into the simulation.

4 HSE Architecture Development

The HSE approach presents models from the previously presented Extensible Resource Library (ERL) framework (see [3, 4]) as simulation parameters that can be adjusted by the user through a spreadsheet interface (see Figure 15). These parameters, which reflect structural, functional, normative, human (cognitive and social), physical, and information dimensions, are automatically incorporated into the configuration of a multi-agent simulation environment (Brahms), where they instantiate and influence the behaviours of agent organizations. These organizations interact over time, according to defined business processes and events that take place within the system based on scenario timelines.

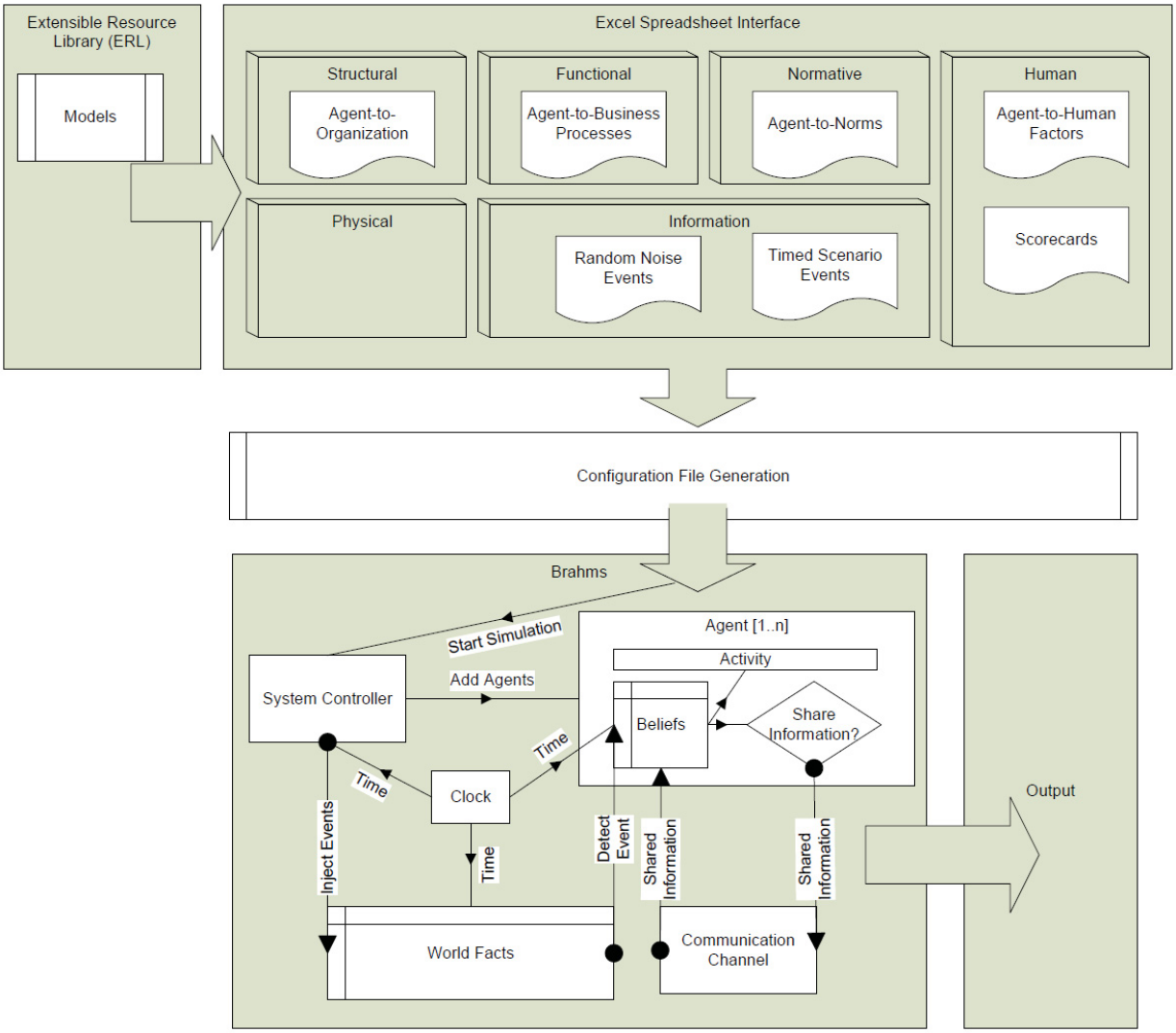


Figure 15: The HSE architecture showing ERL models, spreadsheet interface, configuration file generation, Brahms agent execution, and output.

4.1 The HSE Spreadsheet Interface

The ERL models have been described previously as part of the scenario, and have been incorporated into the design of a spreadsheet interface, which has several key roles in the overall system. The spreadsheet interface is designed to facilitate the entry of agent parameters in a user-friendly format that allows for swift customization of the scenario without the need for code manipulation. It acts as an interface between the actual Brahms multi-agent simulation environment and the system analyst. As such, the spreadsheet allows for setting the scenario, generating Brahms configuration files, executing the simulation, and displaying outputs of execution runs.

In order to define the scenario, a wide range of initialization parameters are required. Figure 16 shows the primary interface for these scenario settings.

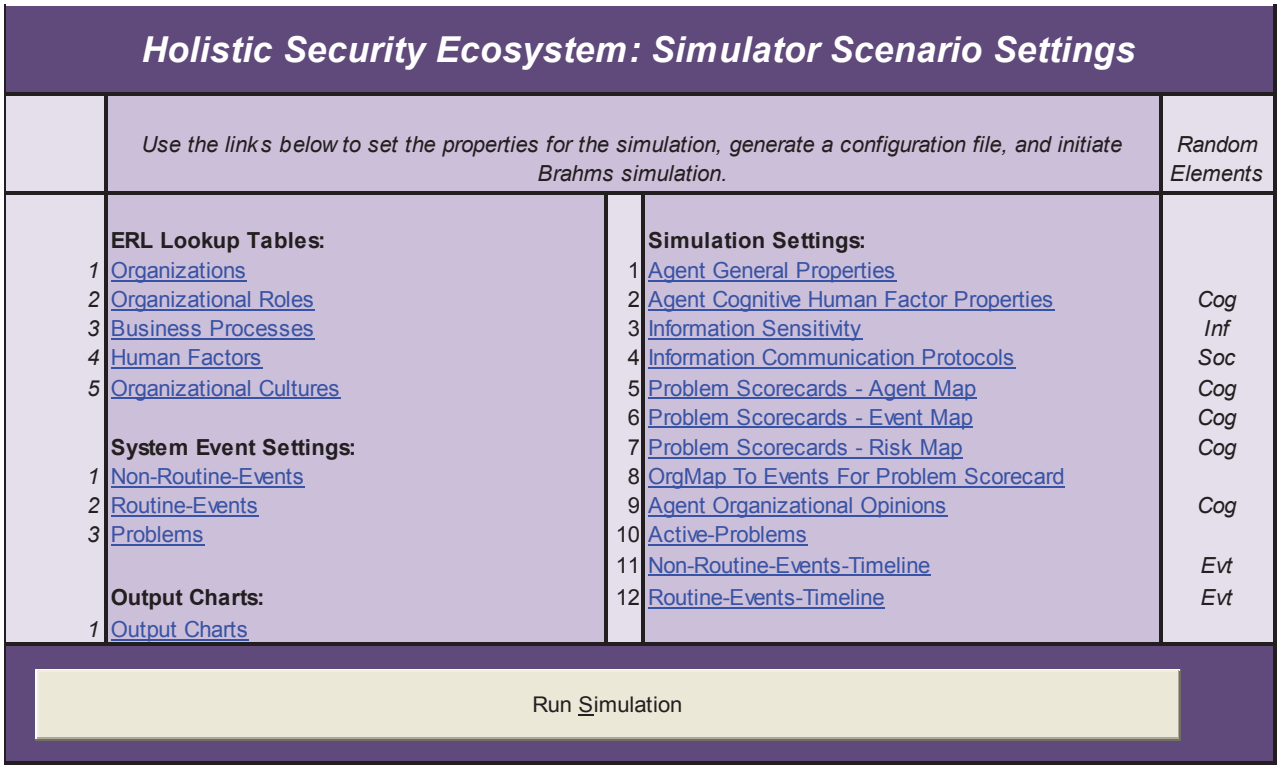
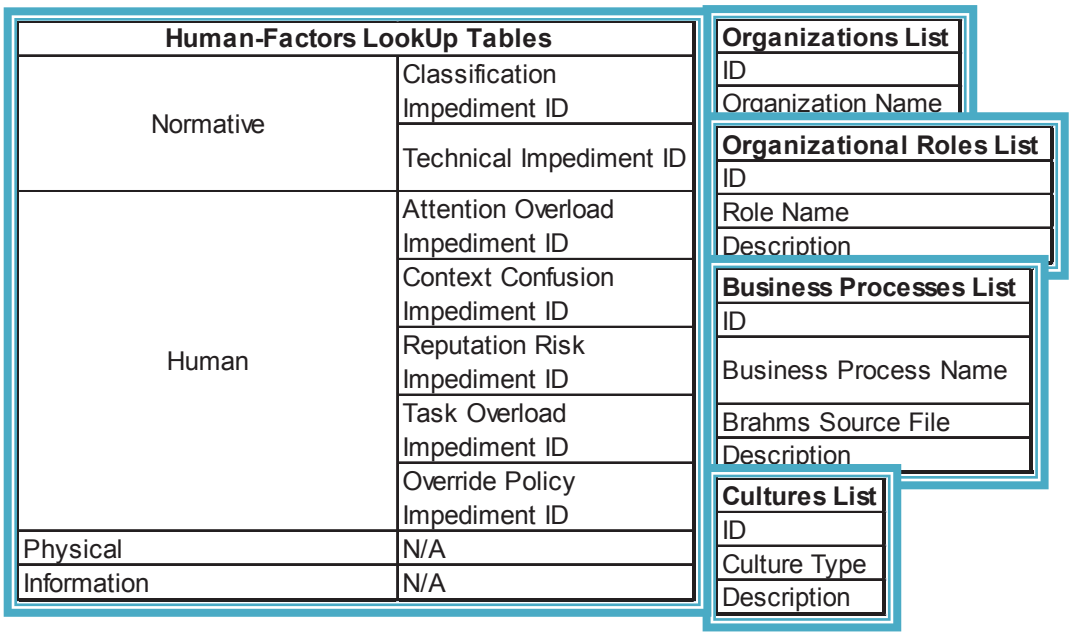


Figure 16: The HSE simulator scenario settings main panel showing lookup tables, event settings, charts, and simulation settings options. Settings with random elements are labelled as Cognitive (Cog), Information (Inf), Social (Soc), or Events (Evt).

The main simulator scenario settings panel allows for the editing of general organizational lookup tables, system event settings, and simulation-specific settings. This panel also allows for the execution of the simulation, and links to the simulation output stored in the spreadsheet.

4.1.1 ERL Lookup Tables

There are a number of key lookup values that are used as agent parameters. These are shown below in **Error! Reference source not found.** indicating settings for organizations, roles, business processes, cultures, and human factors. They refer to the parameters developed in the previous deliverables.



Human-Factors LookUp Tables	
Normative	Classification Impediment ID
	Technical Impediment ID
Human	Attention Overload Impediment ID
	Context Confusion Impediment ID
	Reputation Risk Impediment ID
	Task Overload Impediment ID
	Override Policy Impediment ID
Physical	N/A
Information	N/A

Organizations List
ID
Organization Name

Organizational Roles List
ID
Role Name
Description

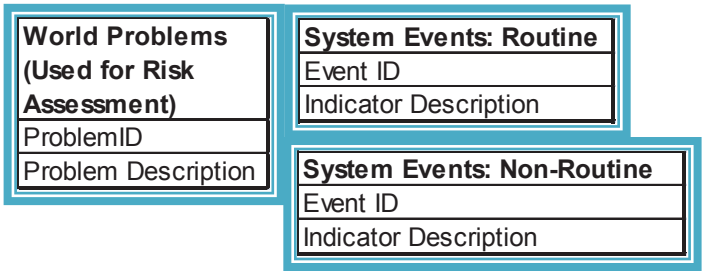
Business Processes List
ID
Business Process Name
Brahms Source File
Description

Cultures List
ID
Culture Type
Description

Figure 17: Headings in the spreadsheet used for lookups and parameters.

4.1.2 System Event Settings

Additionally, parameters are included for world problems and system events (both routine and non-routine) as shown in **Error! Reference source not found.**.



World Problems (Used for Risk Assessment)
ProblemID
Problem Description

System Events: Routine
Event ID
Indicator Description

System Events: Non-Routine
Event ID
Indicator Description

Figure 18: Headings in the spreadsheet for system event settings

4.1.3 Simulation Settings

The simulation consists of a host of parameters related to agent general settings, cognitive human factor settings, cognitive agent opinions about organizations, and agent information sensitivity. These are seen below in **Error! Reference source not found.**.

Agent General Settings	
	Agent Num
	Agent ID
Structural	Organization ID
	Role ID
Functional	Business Process ID
Normative	Classification Impediment ID
	Technical Impediment ID
Human	Attention Overload Impediment ID
	Context Confusion Impediment ID
	Reputation Risk Impediment ID
	Task Overload Impediment ID
	Override Policy Impediment ID
Physical	N/A
Information	N/A

Cognitive Human Factors for Agents	
	Agent ID
Human Factors	Reputation Risk Threshold (%)
	Organizational Alignment (True/False)
	Uncertainty Comfort (%)
	Risk Level Threshold (1-5)
	Attention Overload Frequency (0-20%)
	Context Confusion Frequency (0-20%)
	Task Overload Frequency (0-20%)
Processing Times	Observation Time (Mins)
	Documenting Time (Mins)
	Risk Checking Time (Mins)
	Publishing Time (Mins)

Agent-Information Matrix
Agent ID
Routine Event ID
NonRoutine Event ID
Classification Level (1-5)
Ownership Degree (%)
Uncertainty (%)
Accuracy (%)
Completeness (%)
Credibility (%)
Technical Impediment Level (1-5) [Threshold]

Cognitive Agent Opinions About Organizations
Agent ID
Organization ID
Cultural Restrictiveness (1-5)
Classification Clearance (1-5)
Technical Clearance (1-5)

Figure 19: Headings in the spreadsheet for agent general settings

Furthermore, there are parameters for setting scorecards for each agent, including event and risk maps, as listed in **Error! Reference source not found.**.

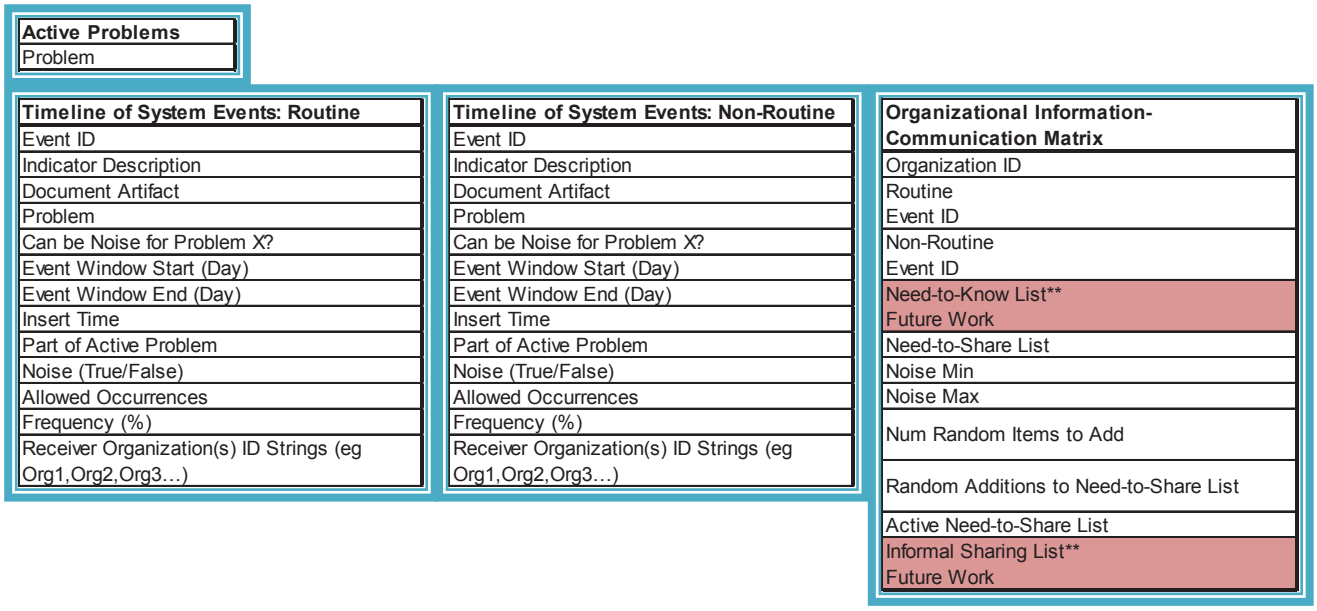
Scorecard Thresholds per Agent
Agent ID
Reputation Risk Threshold (%)
reputationRiskThreshold
SC_ID Min
SC_ID Max
Scorecard Type ID
Scorecard Type

Problem Scorecards - Risk Map
Agent ID
Scorecard ID
Total Possible Score
Score
% Selected
LikelihoodThreshold
Min%
Max%
Internal Threat Level

Problem Scorecards - Event Map
Agent ID
Scorecard Num
Problem ID
Goldilocks Randomness
Goldilocks Override
Communication Requirement
Is Used in Simulation Timeline
Part of Scorecard?
Routine Event ID
NonRoutine Event ID
Observed (Y/N)
Active Event Score

Figure 20: Headings in the spreadsheet for problem scorecard settings

Finally, there are settings for parameters involving the scenario: namely, setting the active problem, the timeline for system events (routine and non-routine), and the communication network (see **Error! Reference source not found.**).



Active Problems
Problem

Timeline of System Events: Routine
Event ID
Indicator Description
Document Artifact
Problem
Can be Noise for Problem X?
Event Window Start (Day)
Event Window End (Day)
Insert Time
Part of Active Problem
Noise (True/False)
Allowed Occurrences
Frequency (%)
Receiver Organization(s) ID Strings (eg Org1,Org2,Org3…)

Timeline of System Events: Non-Routine
Event ID
Indicator Description
Document Artifact
Problem
Can be Noise for Problem X?
Event Window Start (Day)
Event Window End (Day)
Insert Time
Part of Active Problem
Noise (True/False)
Allowed Occurrences
Frequency (%)
Receiver Organization(s) ID Strings (eg Org1,Org2,Org3…)

Organizational Information-Communication Matrix
Organization ID
Routine Event ID
Non-Routine Event ID
Need-to-Know List** Future Work
Need-to-Share List
Noise Min
Noise Max
Num Random Items to Add
Random Additions to Need-to-Share List
Active Need-to-Share List
Informal Sharing List** Future Work

Figure 21: Headings in the spreadsheet for setting the active simulation problem, timelines, and communication network.

4.2 Simulator Execution Settings

The spreadsheet contains various parameters for setting the simulation configuration, including Brahms settings, number of iterations, and randomness settings. Figure 22 shows these simulation settings.

Simulation Execution Settings		
Brahms Source Folder	C:\Brahms Code\InfoShareModel3\source	
Brahms Build Folder	C:\Brahms Code\InfoShareModel3\build	
Main Project File Name:	InfoShareModel3	
Num Iterations	30	Execution 1
Random Cognitive Settings (True,False)	FALSE	
Random Social Settings (True, False)	TRUE	
Random Information Settings (True, False)	FALSE	
Random Event Settings (True, False)	TRUE	
Randomness Configurations	**Colors used to mark random variables**	**Must Change in Code**
Cog		*rand()*
Cog		*randbetween(1,5)*
Cog		*randbetween(true,false)*
Cog		*randbetween(30,120)*
Cog - ScorecardEventScore		*randbetween(1,10)*
Cog - Score in Risk Map		*randbetween(min,max)*
Soc		*rand()*
Soc		*randbetween(1,5)*
Soc		*randbetween(min,max)*
Inf		*rand()*
Inf		*randbetween(1,5)*
Event		*rand()*
Event - Frequency		*randbetween(min,max)*
Reset Random Values	Reset Random Parameters	

Figure 22: Simulation execution settings used by the spreadsheet interface to run the Brahms agent environment multiple times with various randomness settings.

4.2.1 Simulation Execution Process

The process of executing the simulation involves four stages: the setting (and resetting) of base parameters, the randomization of certain parameters according to simulation execution settings, the automatic configuration and generation of Brahms agent code, the compilation and execution of the agent environment, and the gathering and display of data outputs.

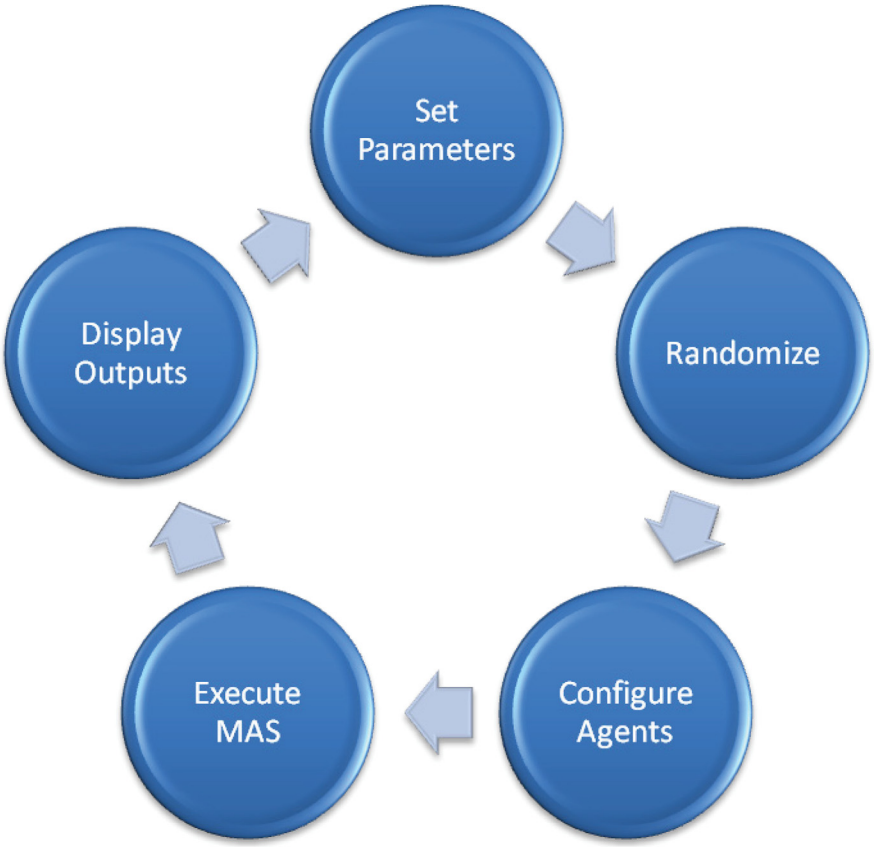


Figure 23: The HSE architecture execution procedure.

4.2.1.1 Set Parameters

Parameters are set according to the scenario selected in Deliverable 4 of this work, the validation and verification of simulation designs. These parameters are shown in the previous sections describing the spreadsheet. In addition, various default values have been set for key parameters. These key parameters are as follows: agent cognitive human-factor properties, information sensitivity, information communication protocols, problem scorecards, agent organizational opinions, routine events timeline, and non-routine events timeline.

4.2.1.2 Randomize

The key parameters within the system are randomized according to four categories as shown in Figure 24—random information settings, random cognitive settings, random social settings, and random timeline settings—and each can be turned on or off for experiments. Each random value is set according to a specific parameter type shown in Figure 22 (e.g., *rand* and *randbetween*).

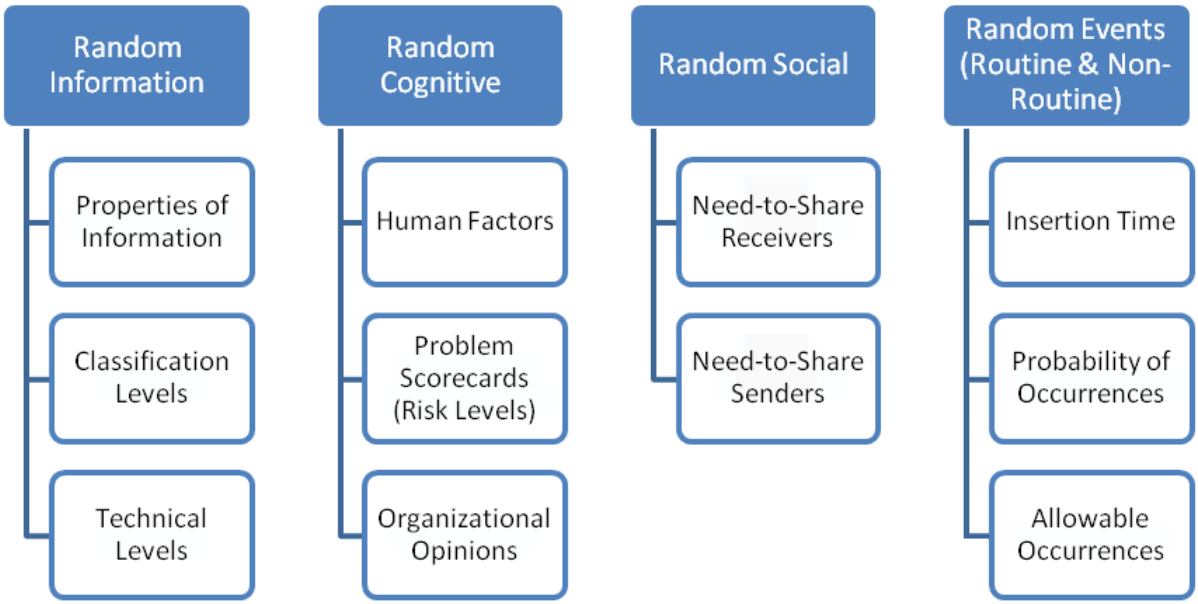


Figure 24: Random Information, Cognitive, Social, and Event parameters within the simulation.

Random Information Settings

The information settings refer to the perceived characteristics of a particular piece of information that is communicated to an agent. These include the *classification level, ownership degree, uncertainty level, accuracy, completeness*, and *credibility* of the information. Information randomness in the system affects the agent's degree of sensitivity to information it encounters. This sensitivity impacts the amount of information sharing publishing impediments within the system.

Random Cognitive Settings

Randomized cognitive settings involve: (i) human factors, (ii) scorecards and associated risk levels, and (iii) the agent's organizational opinions. First, the human factors represent the agent's threshold about *reputation risk*, its *alignment with the organization*, its *degree of comfort with uncertainty*, its *security risk level thresholds*, and the *time* it takes the agent to observe, document, risk-check, and publish events/indicators. Next, the *scorecard* type used by the agent can be randomized according to a "Goldilocks" factor, which relates to adding or removing indicators from the scorecard. This in essence provides three different scorecards: one with too many indicators in relation to the scenario (i.e., imperfect-over-communication or "too hard"), one with

too few indicators (i.e., imperfect-under-communication or "too soft"), and one with the exact number of indicators (i.e., perfect-communication or "just right"). In addition, the *indicator score* for each item in the scorecard can also be randomized, as well as the *risk thresholds* defining the different risk levels (e.g., green, blue, yellow, orange, and red). The final aspect of cognitive randomness involves the agent's opinion about its own organization's *cultural restrictiveness* and the *classification clearance* and *technical clearance* of the other organizations in the system.

Random Social Settings

Randomness in terms of the social configuration is reflected in the amount of communication that takes place during the simulation. The number of *need-to-share receivers* and *senders* is varied here according to random parameters. The base communication network defined by the scenario is modified through the random addition of extra communication receivers and senders, thus, corresponding to increases in the communication network.

Random Events (Routine & Non-routine)

System events take place "normally" according to a pre-set timeline. However, the exact day on which an event will occur (i.e., its *insertion time*) is selected randomly between a specified start and end interval. Additionally, to simulate noise in the system, events can take place more than once up to a maximum of an *allowed number of occurrences* variable. This variable is chosen at random between a minimum and a maximum number. The *probability of an event occurring* on any given day is also specified by a random variable.

4.2.1.3 Configure Agents

The spreadsheet creates files that can be read by the selected agent framework (Brahms) for all of the key components in the system. These files contain the parameters (*beliefs* and *facts* in Brahms), as well as the actions (*workframes* in Brahms), for the agents, problem scorecard objects, event controller object, event indicator objects, organization objects, and role objects. Figure 25 lists these configuration files, showing which ones contain parameters and actions.

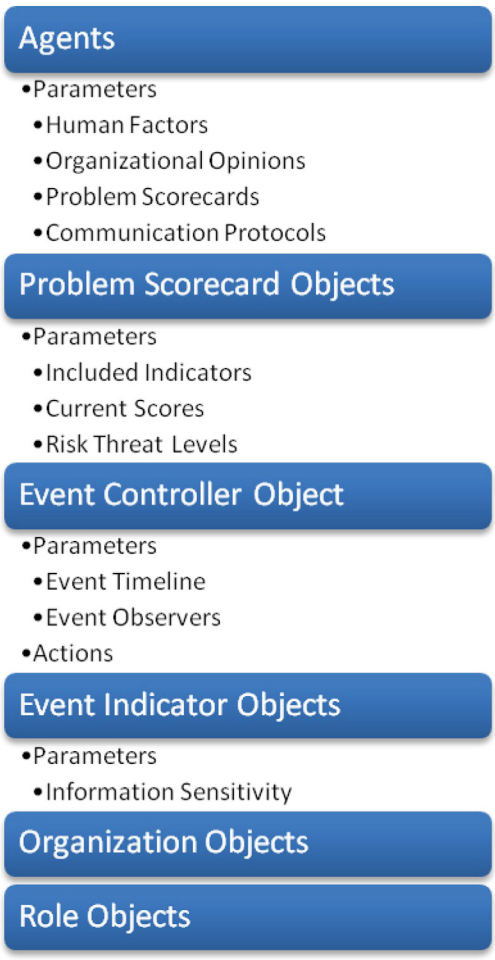


Figure 25: Simulation configuration files: agents, problem scorecards, event controller, event indicators, organizations, and roles.

Agents in the simulation have parameters related to human factors, organizational opinions, problem scorecards, and communication protocols output to their configuration file. Scorecard objects used by these agents to compute the risk level of a particular incident need to be outputted as configuration files, as well. These files include information such as which indicators are contained in the scorecard and the score associated with these indicators. The event controller is an object that injects both routine and non-routine events into the system, according to the parameters set in the spreadsheet, such as insertion time. It must also be outputted in a

configuration file. The event indicator objects represent the information within the system. They must be outputted in order to enable the spreadsheet interface user to decide which information will appear in the simulation and what properties this information will have. Finally, two kinds of placeholder objects are generated: one for the organizations within the simulation and the other for the roles within the simulation. Both of these are used for system configuration, effectively associating agents to organizations and roles.

4.2.1.4 Execute MAS

The multi-agent simulation (MAS) execution takes place in three phases: (i) the initialization phase, wherein the number of iterations and experiment factors are set, and the associated randomized columns are updated in the spreadsheet; (ii) the configuration file generation and storage phase, in which these parameters are outputted to files consumable by the MAS; and (iii) the compilation and execution phase, in which these files, along with the model files, are fed into the MAS execution engine. The HSE spreadsheet acts as the control layer in the overall process, and collects and processes the simulation results afterwards.

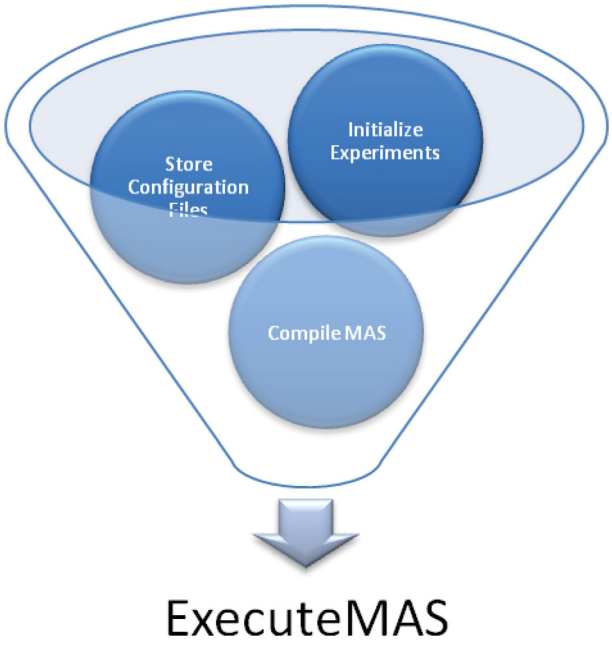


Figure 26: MAS initialization and execution.

4.2.1.5 Display Outputs

During the execution of the simulation, agents interact and output various status messages that can be harvested by the HSE spreadsheet interface. This data is time stamped with the simulation time (i.e., the simulated day). The four types of data outputted by a Brahms agent are as follows:

- Scorecard risk levels
- Need-to-share and publishing impediment override sharing events
- Observation impediments (i.e., attention overload, context confusion, and task overload)
- Publishing impediments (i.e., classification level, technical level, and reputation risk)

Once finished harvesting the data, the HSE spreadsheet interface then generates a visualization "dashboard," using a pivot-table and a series of pivot-charts. Figure 27 presents this process graphically.

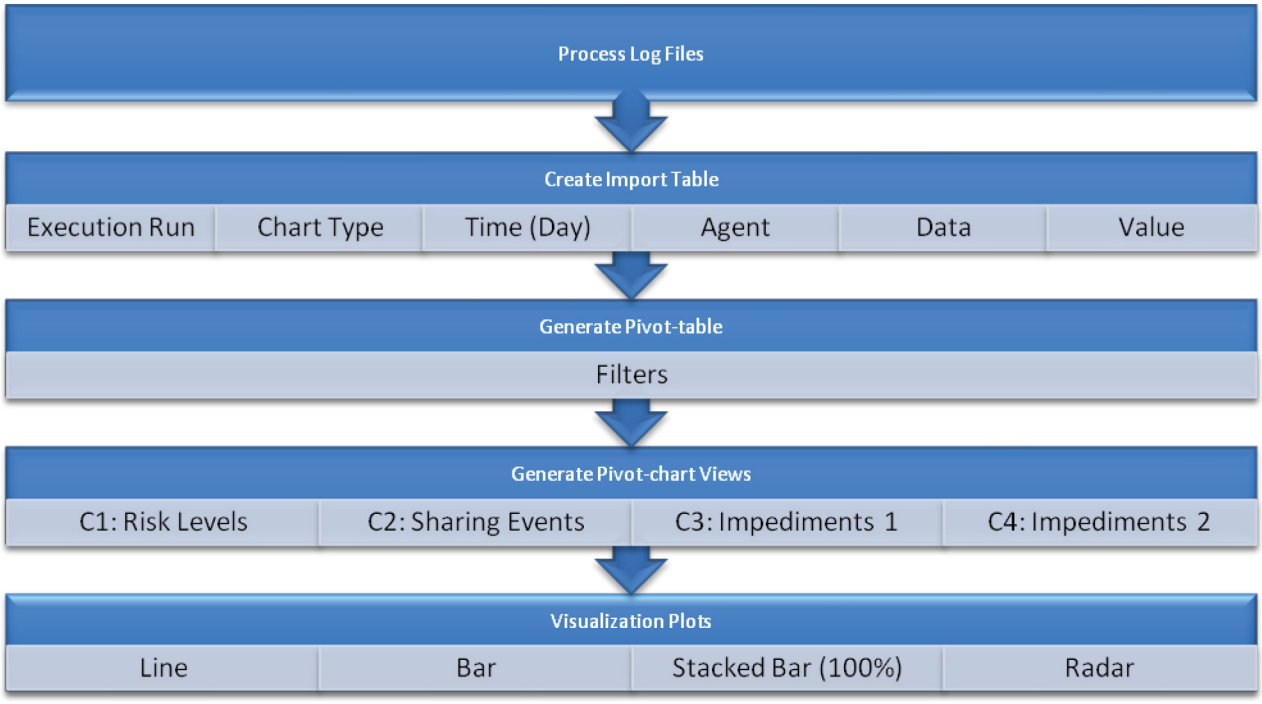


Figure 27: The process of gathering data and generating display output.

4.2.1.6 Import Table:

Data gathered from the MAS execution are imported into a table showing key outputs (see Figure 28) that include the execution identification number, the chart type associated with the data entry, the simulation day the entry was made by the agent, the agent who outputted the data, the data identifier, and the value. This information is taken directly from the MAS log files.

ExecID	Chart	timeDay	agent	data	value
Exec1	C3	Day001	Agent11_RCMP		ObservationImpediment
Exec1	C3	Day001	Agent11_RCMP		ObservationImpediment
Exec1	C3	Day001	Agent01_Govt_Op_Centre		ObservationImpediment
Exec1	C3	Day001	Agent20_Harbour_Master		ObservationImpediment
Exec1	C3	Day001	Agent19_MCTS		ObservationImpediment
Exec1	C3	Day001	Agent01_Govt_Op_Centre		ObservationImpediment
Exec1	C3	Day001	Agent20_Harbour_Master		ObservationImpediment
Exec1	C3	Day001	Agent19_MCTS		ObservationImpediment
Exec1	C1	Day001	Agent01_Govt_Op_Centre	riskLevel	green
Exec1	C1	Day001	Agent02_JTFA	riskLevel	green
Exec1	C1	Day001	Agent03_POJP	riskLevel	green
Exec1	C1	Day001	Agent04_POJM	riskLevel	green
Exec1	C1	Day001	Agent05_Transport_Canada	riskLevel	green
Exec1	C1	Day001	Agent06_Public_Safety_Canada	riskLevel	green

Figure 28: Sample table output harvested from MAS execution log files.

4.2.1.7 Pivot-table and Chart Views:

Pivot tables and four types of charts are generated from the output data as the standard view. The use of the pivot table allows for flexible analysis of the data, which can be filtered according to execution run, chart type, and/or agent. This is particularly useful when discussing the experiment results, as it is possible to see the data associated with a single agent or a group of agents, such as the set of important agents representing the consensus group. Figure 29 shows a sample of this pivot data and chart view. The line, bar, and radar plot charts show essentially the same information (for different viewing), while the stacked bar chart (lower left) shows the percentage over time of the data for the selected chart type.

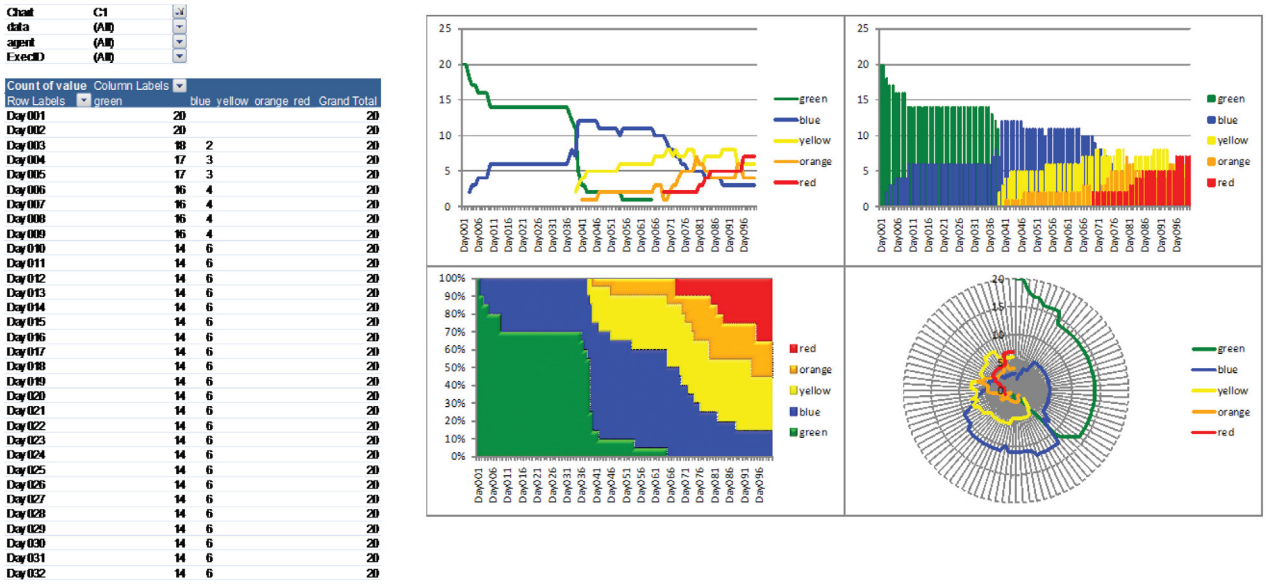


Chart	C1
data	(All)
agent	(All)
ExecID	(All)

Count of value	Column Labels				
Row Labels	green	blue	yellow	orange	red	Grand Total
Day 001		20				20
Day 002		20				20
Day 003		18	2			20
Day 004		17	3			20
Day 005		17	3			20
Day 006		16	4			20
Day 007		16	4			20
Day 008		16	4			20
Day 009		16	4			20
Day 010		14	6			20
Day 011		14	6			20
Day 012		14	6			20
Day 013		14	6			20
Day 014		14	6			20
Day 015		14	6			20
Day 016		14	6			20
Day 017		14	6			20
Day 018		14	6			20
Day 019		14	6			20
Day 020		14	6			20
Day 021		14	6			20
Day 022		14	6			20
Day 023		14	6			20
Day 024		14	6			20
Day 025		14	6			20
Day 026		14	6			20
Day 027		14	6			20
Day 028		14	6			20
Day 029		14	6			20
Day 030		14	6			20
Day 031		14	6			20
Day 032		14	6			20

Figure 29: Visualization dashboard showing pivot-table (filtered for Chart 1) and four plots of sample execution output.

Chart 1: Threat Levels for the Active Problem

The first chart type presents the agents' beliefs about the threat level of the active problem over the course of the simulation. This threat level is set by individual agents and represents their perception about whether or not a dangerous incident is imminent based on increasing threat levels (green, blue, yellow, orange, and red). Four sample output views of this information are shown below in Figure 30.

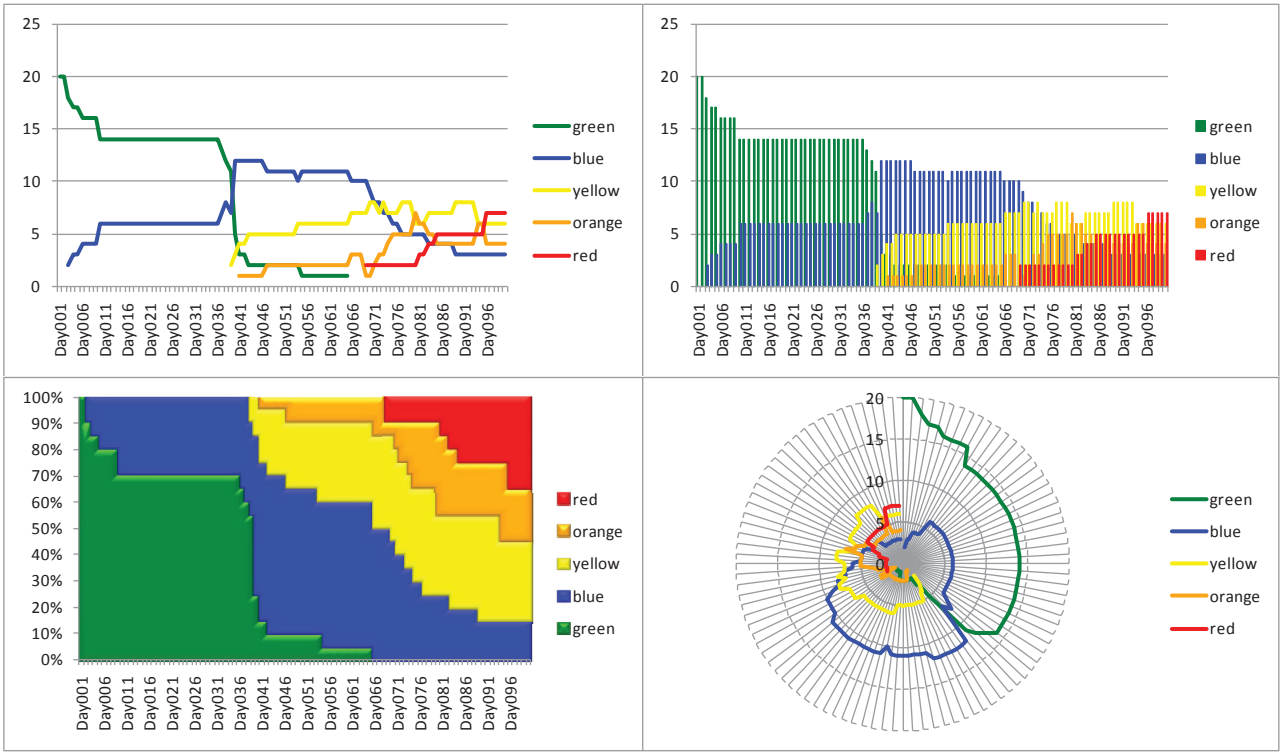


Figure 30: Chart 1 sample showing four views of agent threat levels.

Chart 2: Need-to-Share and Publishing Impediment Override Sharing Events

The second chart type shows the total number of sharing events that take place in the system. These come in two flavours: the standard need-to-share (N2S) events and the sharing events that take place as the result of an agent overriding a publishing impediment. Samples are shown in Figure 31 below.

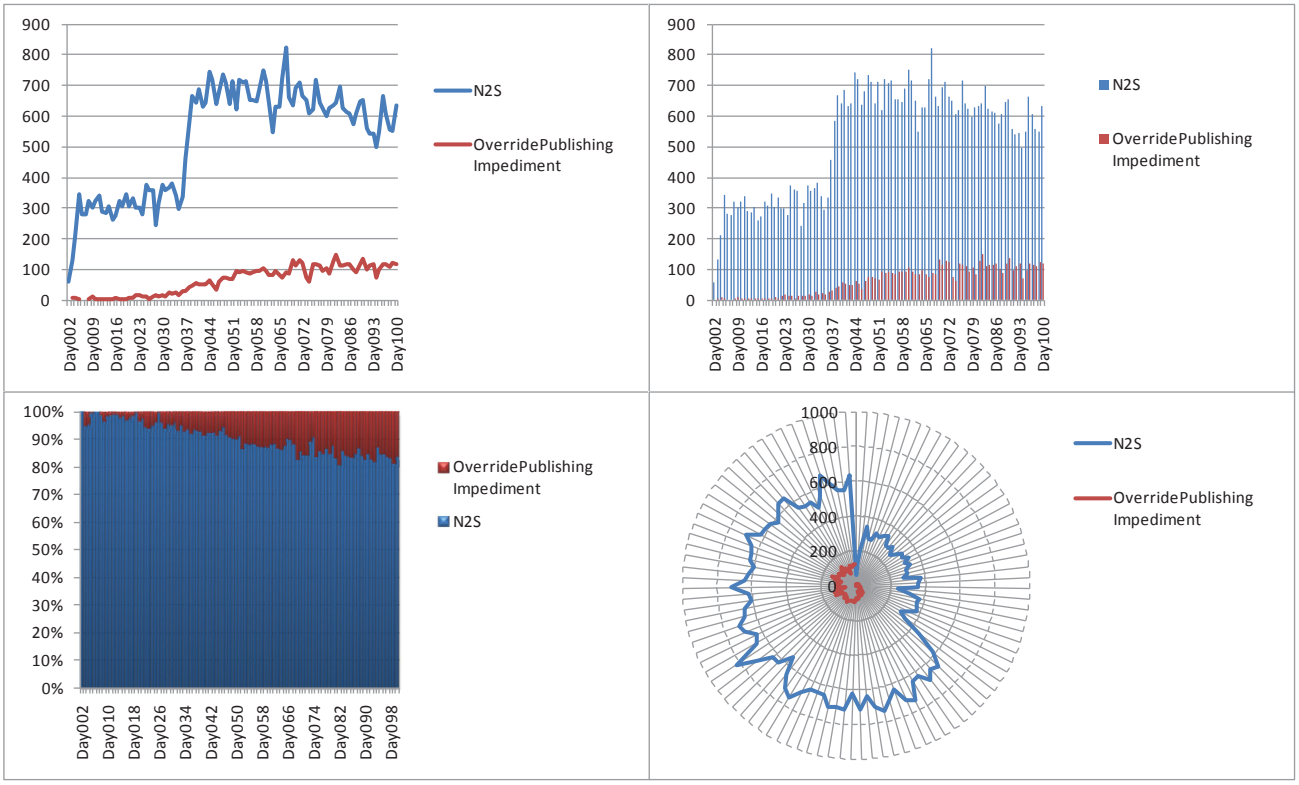


Figure 31: Chart 2 sample showing need-to-share and publishing impediment override sharing events over time.

Chart 3: Observation Impediments

The third chart type shows system impediments to observation over time (due to attention overload, context confusion, and task overload). Samples are shown in Figure 32 below.

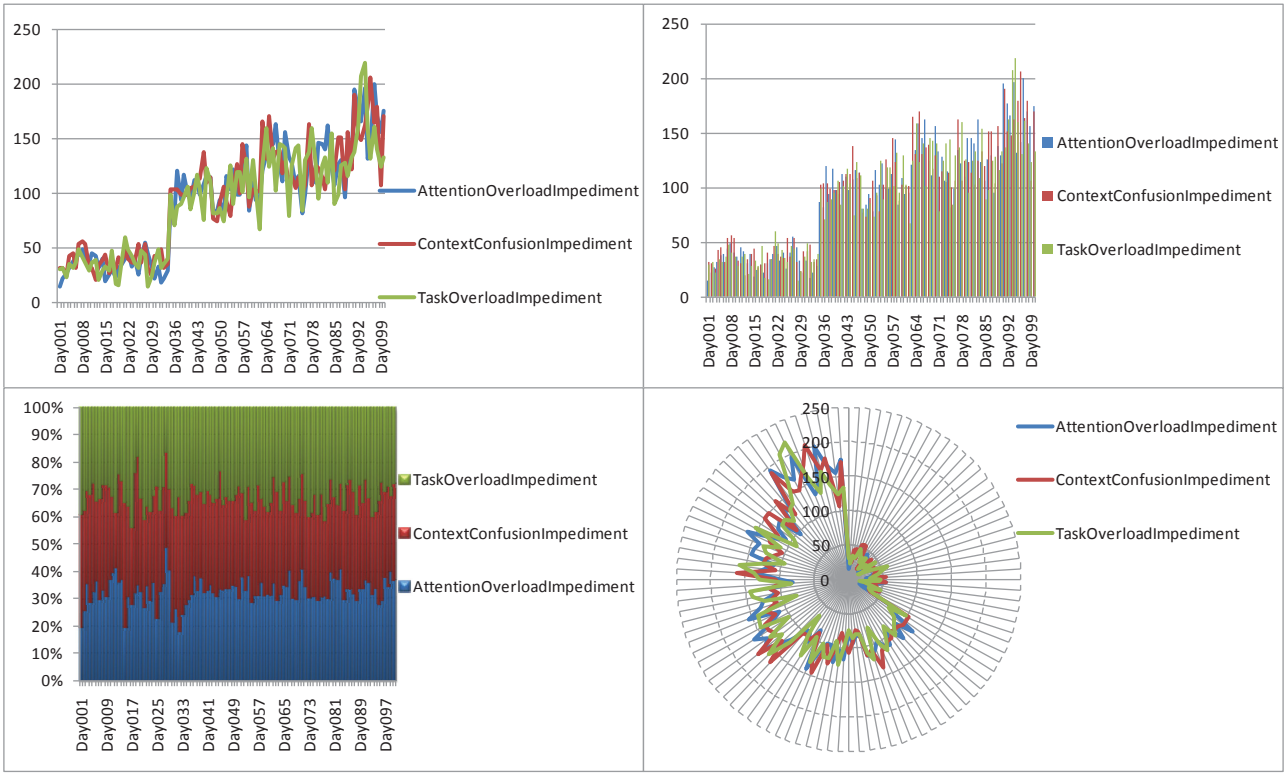


Figure 32: Chart 3 sample showing impediments to observation.

Chart 4: Publishing Impediments

The fourth chart type shows system impediments to publishing over time (due to classification level, technical level, and reputation risk level). Samples are shown in Figure 33 below.

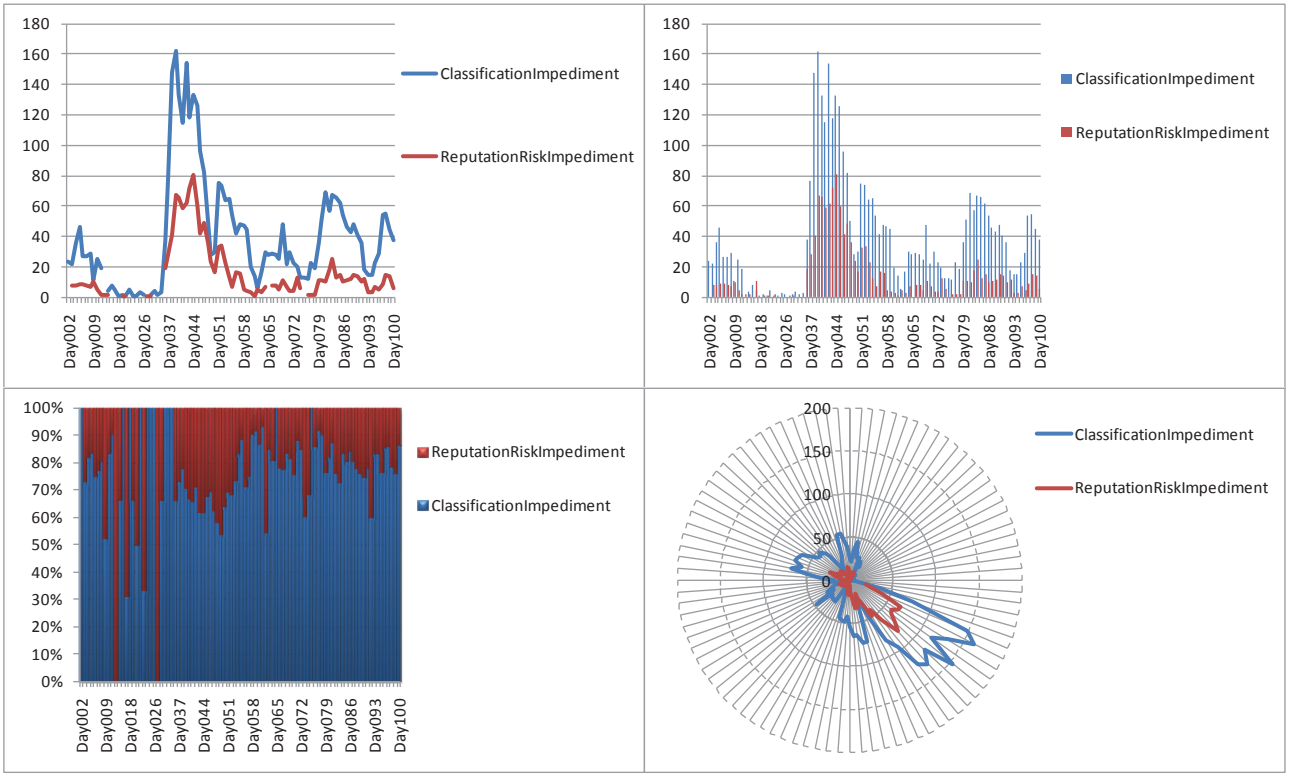


Figure 33: Chart 4 sample showing publishing impediments.

5 HSE Brahms Implementation

According to Figure 15, the main components in the HSE Brahms implementation architecture are the agents themselves, the system controller, and the clock. During each simulation run, these components perform the key tasks as outlined in Figure 34.

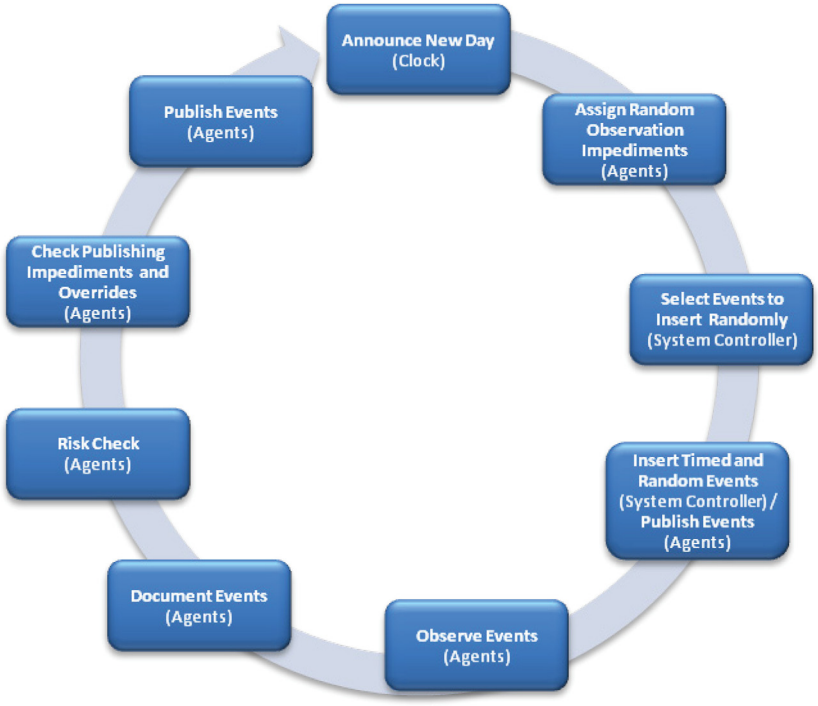


Figure 34: Brahms execution process.

The simulation proceeds according to the timeline defined in the spreadsheet on the scale of a single day. At the beginning of each day, the clock notifies all the agents in the system, as well as the system controller, that a new day has begun. The agents then get assigned randomly whether or not they will be impeded by an observation impediment on that day and the system controller selects at random which events will be inserted into the system besides those that are scheduled to appear on that day. The simulation then continues with the system controller injecting these events into the system and there being observed by the unimpeded agents. It should be noted that besides the system controller, communication from other agents can also be observed by the agents in the system. This communication is defined in the spreadsheet interface. Once the observation takes place (which could be delayed due to impediments), the agents undergo a process of documenting the event and performing a risk check to determine if the event might possibly belong to a particular problem (or incident) their organization can handle. Finally, the agents check their publishing impediments and overrides to determine whether to publish the event to other agents in the system.

The first four steps of the Brahms execution process happen each day of simulation. However, the observe → document → risk-check → publish agent process may extend several days, depending on impediments and the processing times of the agents.

Within the Brahms portion of the architecture, the classes can be divided according to two broad categories: the base framework classes and those classes related to the 7D methodology. The base framework consists of two main classes, as shown in Figure 35: a *system controller*, which is used to inject events into the world randomly and according to a set timeline; and a *clock*, which is used to notify the agents and the system controller when a new day takes place, as well as when the simulation ends.

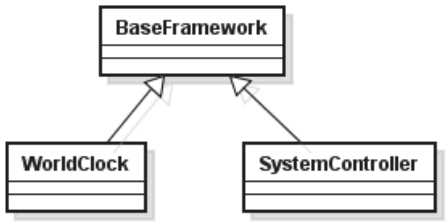


Figure 35: Base framework classes.

The remaining classes are partitioned into three tiers—information, organization, and physical—as shown in Figure 36. The most important tier is the organization one. It holds the central class, *unit*, which represents the individual members (or agents) within the simulation. These agents inherit from five key classes: *structural*, which relates to the agent's position within an organization; *functional*, which defines the actions the agent is able to perform; *normative*, which specifies the conditions under which the agent's actions can be undertaken; *cognitive*, which captures the mental constraints of the agent; and *social*, which contains the relationship constraints of the agent. Example subclasses related to each of these classes will be described below.

The information and physical tiers are less involved and refer, respectively, to the components being transmitted during communication and the physical reality faced by the agents. In the current implementation, physical resource models for such things as communication infrastructure have not been included; however, a simplified geography model has been captured.

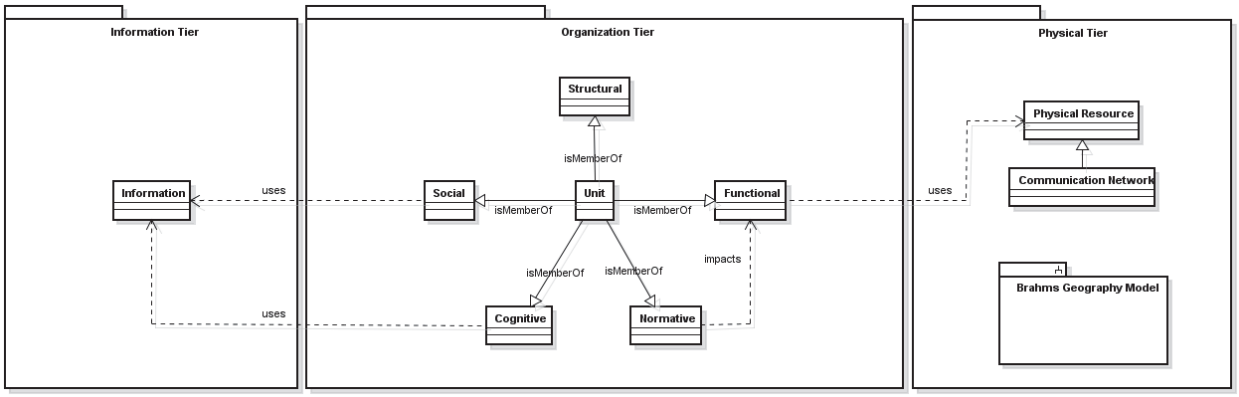


Figure 36: Brahms ERL classes.

The structural class, as shown in Figure 37, has two subclasses: *organization*, which contains associated properties of an organization; and *role*, which is used to define the various roles existent within the system. The current implementation treats an organization as monolithic, i.e., represented by a single agent. However, relations such as *subordinate-to* and *colleague-of* can be used to specify the structure of a multi-agent organization.

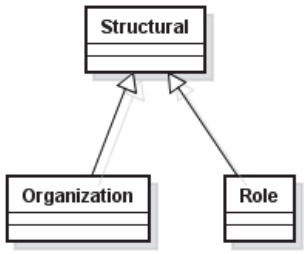


Figure 37: Structural classes.

Figure 38 shows that the *information sharing business process* class inherits from the functional class. This subclass contains the four main actions performed by the agents in the simulation: observe, document, risk check, and publish. These have been described in detail in Deliverable 4, [4], and have also been described above.

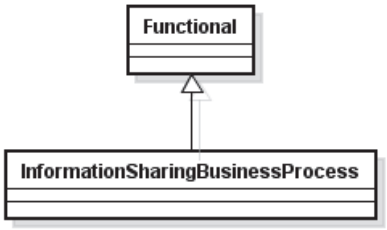


Figure 38: Functional classes.

The normative class currently has one direct descendant, *policy impediment*, which is further sub classed into *classification impediment* and *technical impediment* as shown in Figure 39. These latter impediments are based on the agent's beliefs about information properties, as well as beliefs about the classification and technical levels of the other organizations in the system. These impediments can result in publishing impediments, whereby an agent has a belief that it ought to share information with a specific agent but is unable to do so because of a policy impediment.

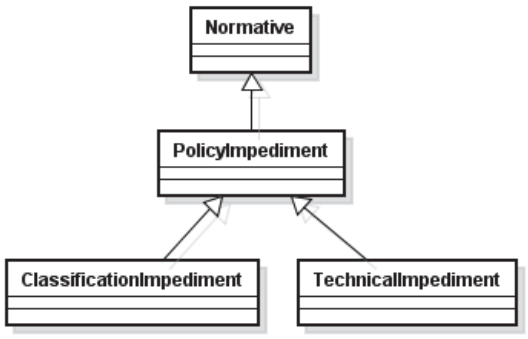


Figure 39: Normative classes.

The cognitive class, shown in Figure 40, is sub classed into two: the *scorecard* class, which contains a mapping of indicators and associated scores, representing the agent's knowledge of how to identify problems and determine threat risk; and the *human factor* class, which is further sub classed into *processing times*, *reputation risk impediment*, *override policy*, and *observation impediment* classes.

The processing times define the length of time (in minutes) it takes an agent to perform each of its four key tasks: observe, document, risk check, and publish. The reputation risk impediment relates to whether or not the agent will refuse to publish for fear of damaging its organization's reputation. It is a function of the properties of the specific indicator (i.e., certainty, ownership degree, credibility, and accuracy), as well as how comfortable the agent is with uncertainty. The override policy determines whether or not the agent will choose to publish the information regardless of a policy or reputation risk impediment. This is based on the cultural restrictiveness of the organization, the agent's alignment to its organization's culture, and the current risk level of the scorecard. Finally, the various observation impediments—*attention overload impediment*, *context confusion impediment*, and *task overload impediment*—determine whether or not the agent will be delayed in observing an indicator. These impediments are governed by a stochastic model and have a percentage chance of occurring on any given day.

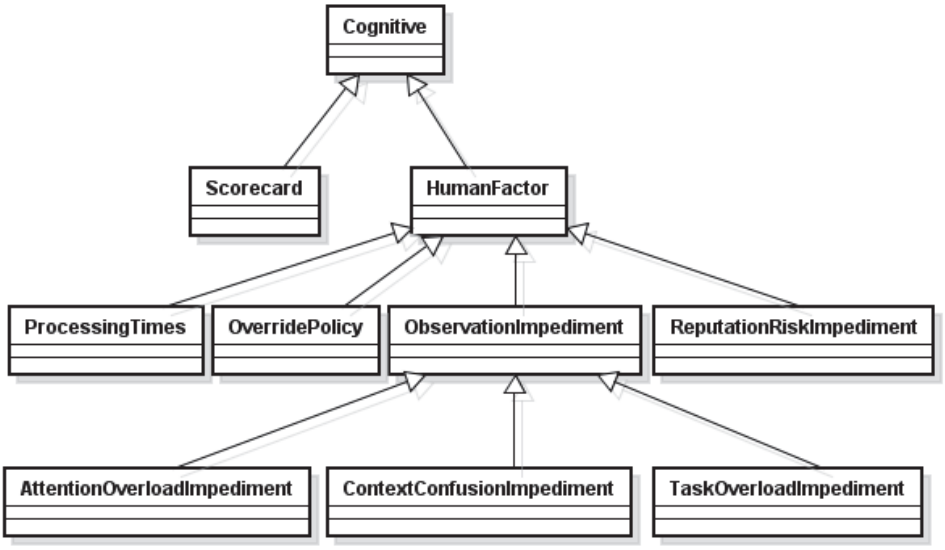


Figure 40: Cognitive classes.

Figure 41 shows the social class along with its two subclasses: *organization culture* and *need to share link*. The organization culture model is simple at the moment, consisting of a range from 1 to 5, where one extreme, 1, indicates a performance-oriented culture and the other extreme, 5, represents a rule-oriented culture. The other class represents the binding between agents and indicators and defines what other agents should receive this information.

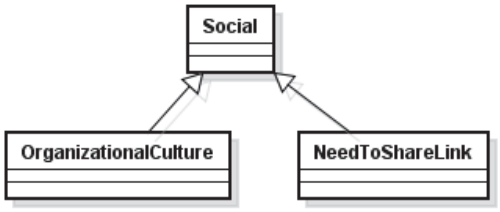


Figure 41: Social classes.

The information class in Figure 42 consists of one subclass: *indicator*. This class contains all of the information properties outlined in the previous section. It is used by the need-to-share-link, social, and information-sharing-business-process classes.

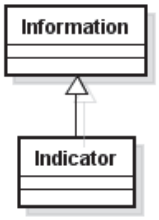


Figure 42: Information classes.

Lastly, the physical class contains one subclass as shown in Figure 43: *port*. This defines the world in which the agents operate. If the geography were more central to the simulation, e.g., if response were being investigated, it could be greatly enhanced to include buildings, streets, river ways, and bridges. However, in this simulation, the port represents more of a conceptual geography than a physical one.

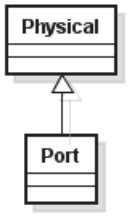


Figure 43: Physical classes.

The overall HSE simulation process from parameter and experiment selection to simulation execution and output is shown in **Error! Reference source not found.**. In this proof-of-concept simulation, the models are basic, but they can be enhanced in the future. For example, the organization culture model in the social dimension can be extended to include the notion of influence as described in previous work, [6, 8]. The extensibility of the ERL framework enables these various model classes to be substituted with other classes at any time. Hence the need for a spreadsheet interface is to make it easy for users to choose their preferred models.

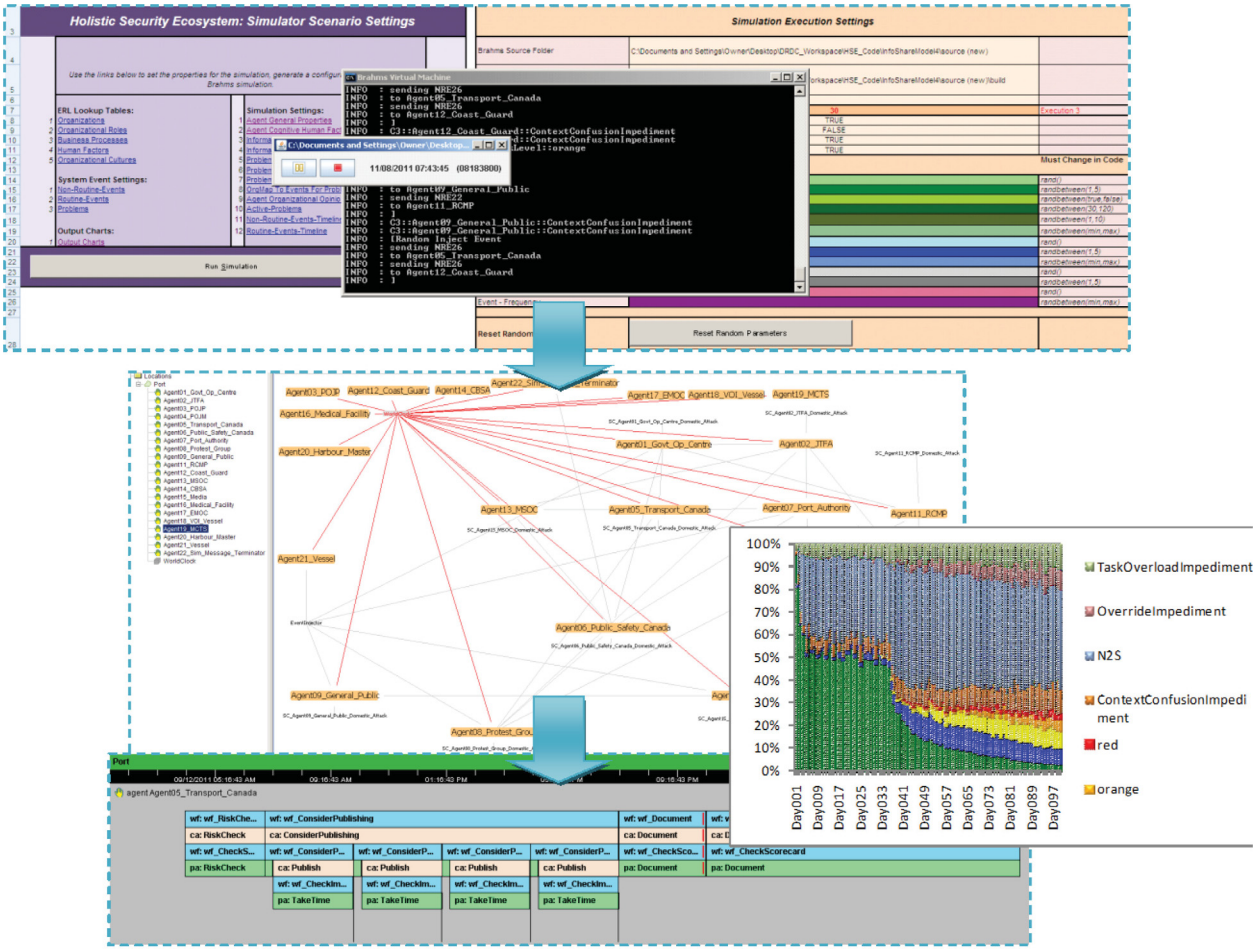


Figure 44: The simulator executing Brahms from the spreadsheet and generating a network, timeline of activities, and outputs

6 HSE Simulation Experiments

In keeping with the objectives of the current deliverable, this section details the experiments which have been developed for the HSE simulator and presents the core analysis. The experiments focus on the interplay between randomizations (and constants) over 30 executions of the simulator for the eight experiments shown in Table 1. These capture all possible combinations of Social, Cognitive, and Information factors. The random event parameters are always set to true, consistent with the premise that when an event takes place and who observes it are not static.

Table 1: The design-set of experiments involving the interplay between Social, Cognitive, and Information factors Events are considered random over all the experiments (by design).

Experiment Number	Randomization of Key Factors				Number Of Executions	Description
	Social	Cognitive	Information	Events		
1	FALSE	FALSE	FALSE	TRUE	30	Baseline experiment with fixed social, cognitive, and information values
2	TRUE	FALSE	FALSE	TRUE	30	Only social values randomized; shows the impact of varying the social network configuration and amount of communication
3	FALSE	TRUE	FALSE	TRUE	30	Only cognitive values randomized; shows the impact of varying cognitive attributes
4	FALSE	FALSE	TRUE	TRUE	30	Only information values randomized; shows the impact of the properties of information
5	TRUE	TRUE	FALSE	TRUE	30	Both social and cognitive factors randomized while holding information properties constant; shows the interplay between social and cognitive factors
6	TRUE	FALSE	TRUE	TRUE	30	Both social and information factors randomized while holding cognitive attributes constant; shows the interplay between social and information factors
7	FALSE	TRUE	TRUE	TRUE	30	Both cognitive and information factors randomized while holding social structure constant; shows the interplay between cognitive and information factors
8	TRUE	TRUE	TRUE	TRUE	30	All factors randomized; shows the interplay between all factors in the system

In addition to the design of the experiments, the following points are highlighted:

- Experiment 1 is used to establish a baseline and is expected to have the earliest time to reach consensus, as there are no publishing impediments in the system. Experiments 5, 6,

7, and 8 show the interplay between at least two factors and offer the more interesting results.

- Default values (i.e., when the factor's randomization is set to false) present a caveat at this point, as they are primarily base parameters that are non-interesting. Setting these with more realistic values presents an opportunity for future studies.

- The current experiments highlight the impact of randomness and noise in the simulation at a high level, i.e., at the level of parameter groups defined according to the key factor sets. A more detailed analysis could investigate specific parameters within each factor set more closely.

6.1 Results and Analysis

The experiments above involve all agents in the system, but the results relate only to a particular subset of agents that are members of the *consensus group*. This group represents the safety-and-security organizations in the system that would be concerned with scenario one: the domestic attack. The selection of this group is presented in Figure 45 and consists of ten agents: Joint Task Force Atlantic (JTFA), Police of Jurisdiction Provincial (POJP), Police of Jurisdiction Municipal (POJM), Transport Canada, Public Safety Canada, Port Authority, RCMP, Coastguard, MSOC, and EMOC.

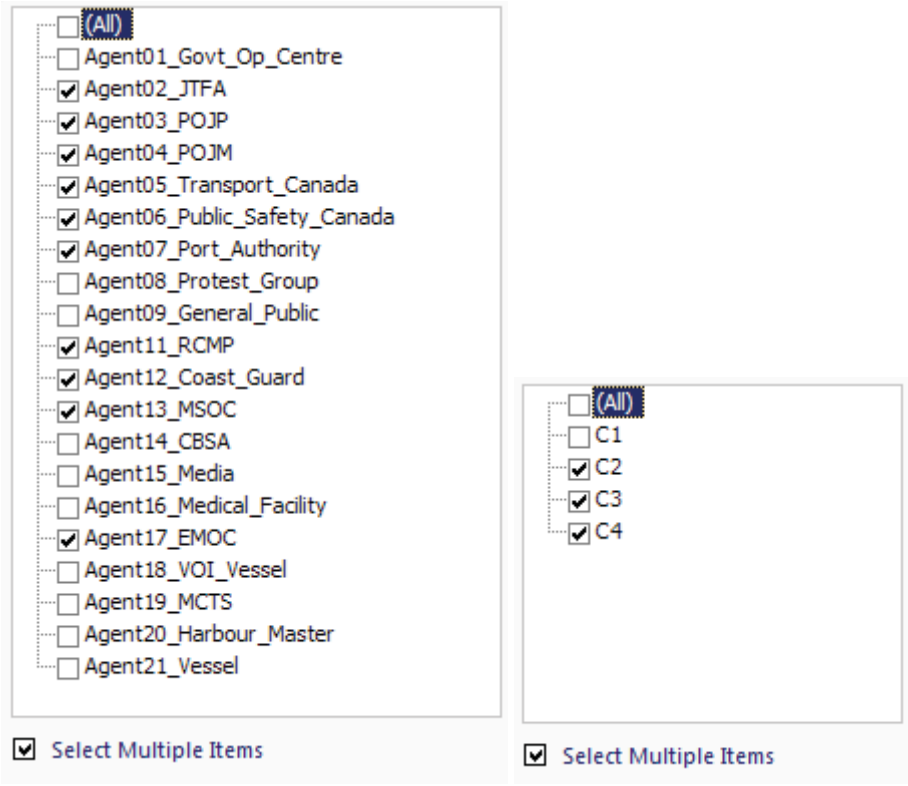


Figure 45: Example of filtering key agents for consensus group. Filtering is also possible for the different charts.

The consensus group provides a filtered viewpoint of the simulation results. Exactly when this group reaches consensus is determined by a particular measurement rule established by an analyst. The threat levels related to the incident have been adopted from the colour-coded standard identified in [12], where green = low risk; blue = guarded risk; yellow = elevated risk; orange = high risk; and red = severe risk. Given the measurement rule that consensus is achieved *"when 50% of the consensus group has a threat level of elevated risk or higher*," the analyst can make use of the figures below to determine the exact day consensus is achieved (if at all).

The choice of consensus being left to the analyst is an example of how this tool is meant to facilitate general analysis, rather than provide the solution directly. In this section, "consensus" will follow the rule above and mean when 50% of the agents believe the problem risk level to be at least elevated (i.e., at least yellow). The results of goal achievement would be very different if consensus were chosen to be 80% instead.

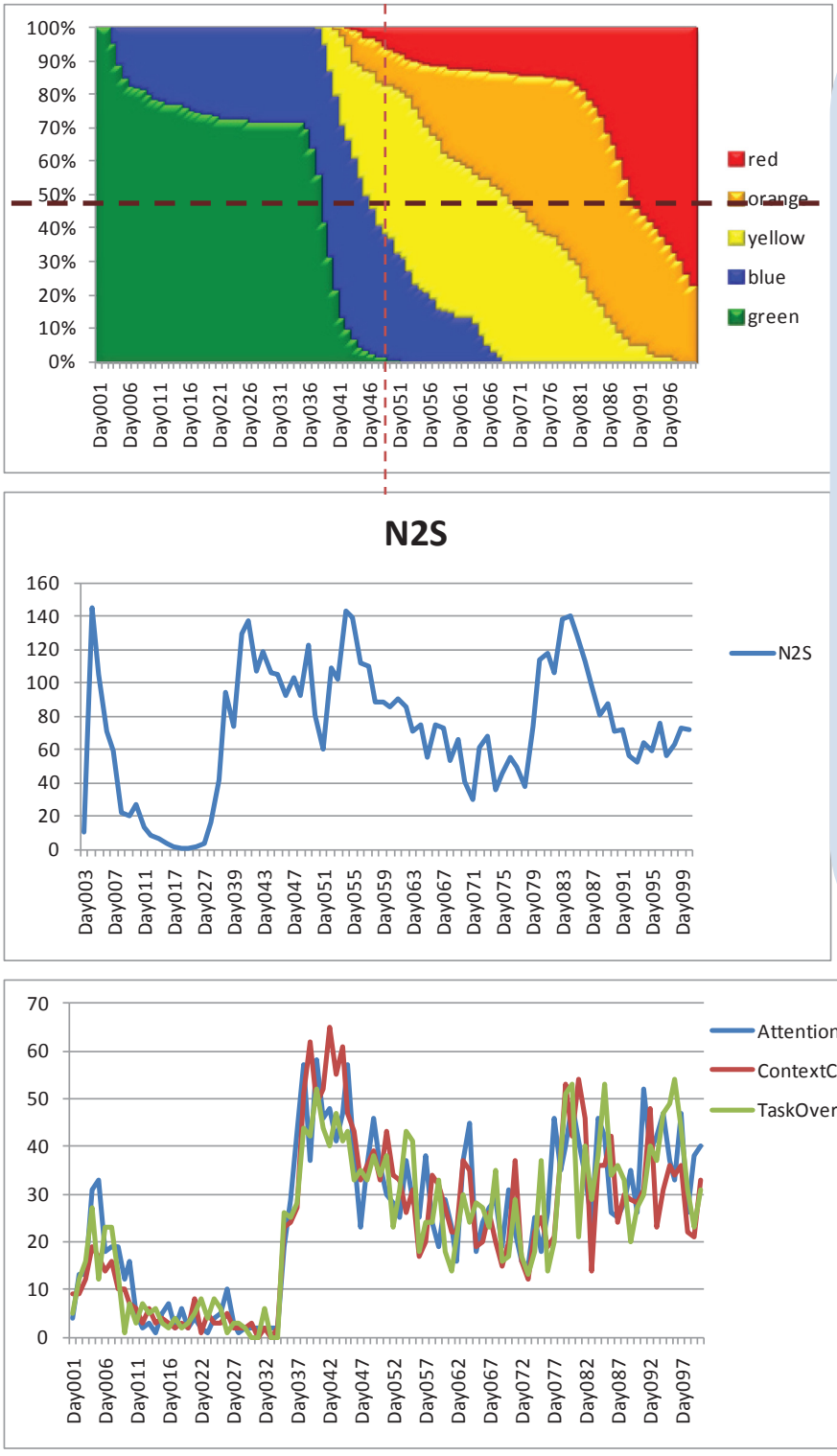
The experiment results below show how key social, cognitive, and information factors impact the achievement of consensus. The C1 charts capture the concensus data and show the percentage of the group (over all 30 execution runs of each experiment) that believe the incident risk level to be at a particular colour. On Day 1 all of the agents believe the risk of a domestic attack to be low (i.e., at level green). Given that the incident timeline leads up to an attack on Day 100, it is expected that a normal execution would show threat levels increasing for the various agents as more events in the timeline are shared.

6.2 Experiment 1: Soc-False Cog-False Inf-False

The parameters that have been randomized in this experiment are shown in Table 2.

Table 2: Tested features in Experiment 1.

Key Component	Parameters	Randomized Features
Social	Need-to-Share Receivers	N/A
	Need-to-Share Senders	N/A
Cognitive	Human Factors	N/A
	Problem Scorecards (Risk Levels)	N/A
	Organizational Opinions	N/A
Information	Information Properties	N/A
	Classification Levels	N/A
	Technical Levels	N/A
Event	Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences
	Non-Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences



Consensus:
In the case of the first experiment, consensus is achieved on Day 46.

Information Sharing:
With no randomization in the system (except events), there are high levels of information sharing (N2S). This correlates with the rate of consensus change (for instance the spike at day 36 resulted in a large shift in opinion from green to blue).

Impediments:
With no core factors randomized, only the observation impediments are activated, which will delay slightly the observing of indicators. It is seen that the three observation impediments are roughly similar due to their default values being equivalent.

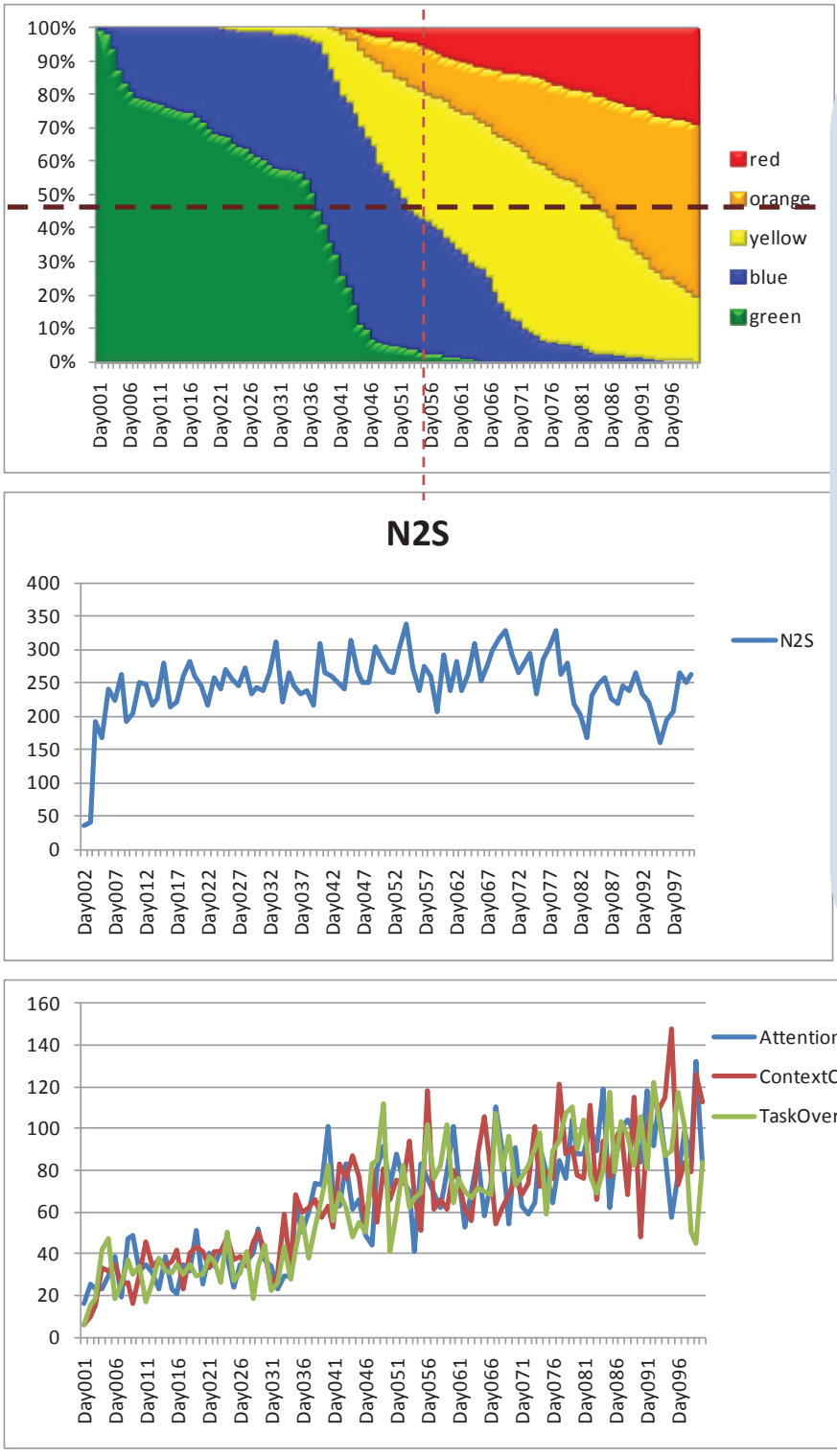
Figure 46: Experiment 1 charts showing consensus outcomes (C1), sharing events (C2), and impediments (C3, C4), with Soc-False Cog-False Inf-False

Experiment 2: Soc-True Cog-False Inf-False

The parameters that have been randomized in this experiment are shown in Table 3.

Table 3: Tested features in Experiment 2.

Key Component	Parameters	Randomized Features
Social	Need-to-Share Receivers	Need-to-Share Receivers
	Need-to-Share Senders	Need-to-Share Senders
Cognitive	Human Factors	N/A
	Problem Scorecards (Risk Levels)	N/A
	Organizational Opinions	N/A
Information	Information Properties	N/A
	Classification Levels	N/A
	Technical Levels	N/A
Event	Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences
	Non-Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences



Consensus:
In the case of the second experiment, consensus is achieved on Day 51, approximately.

Information Sharing:
With social (and event) randomization in the system, there are consistently high levels of information sharing (N2S). In fact, the sharing levels are nearly twice as high as those in Experiment 1. However, because the shared information is not always relevant (i.e., not always part of the scorecard), this combined with observation impediments has the effect of delaying consensus.

Impediments:
With social factors randomized and an increase in the number of sharing events, a corresponding increase in the number of observation impediments occurs because these are governed by a probabilistic model, dependent on the amount of information being sent to the agent

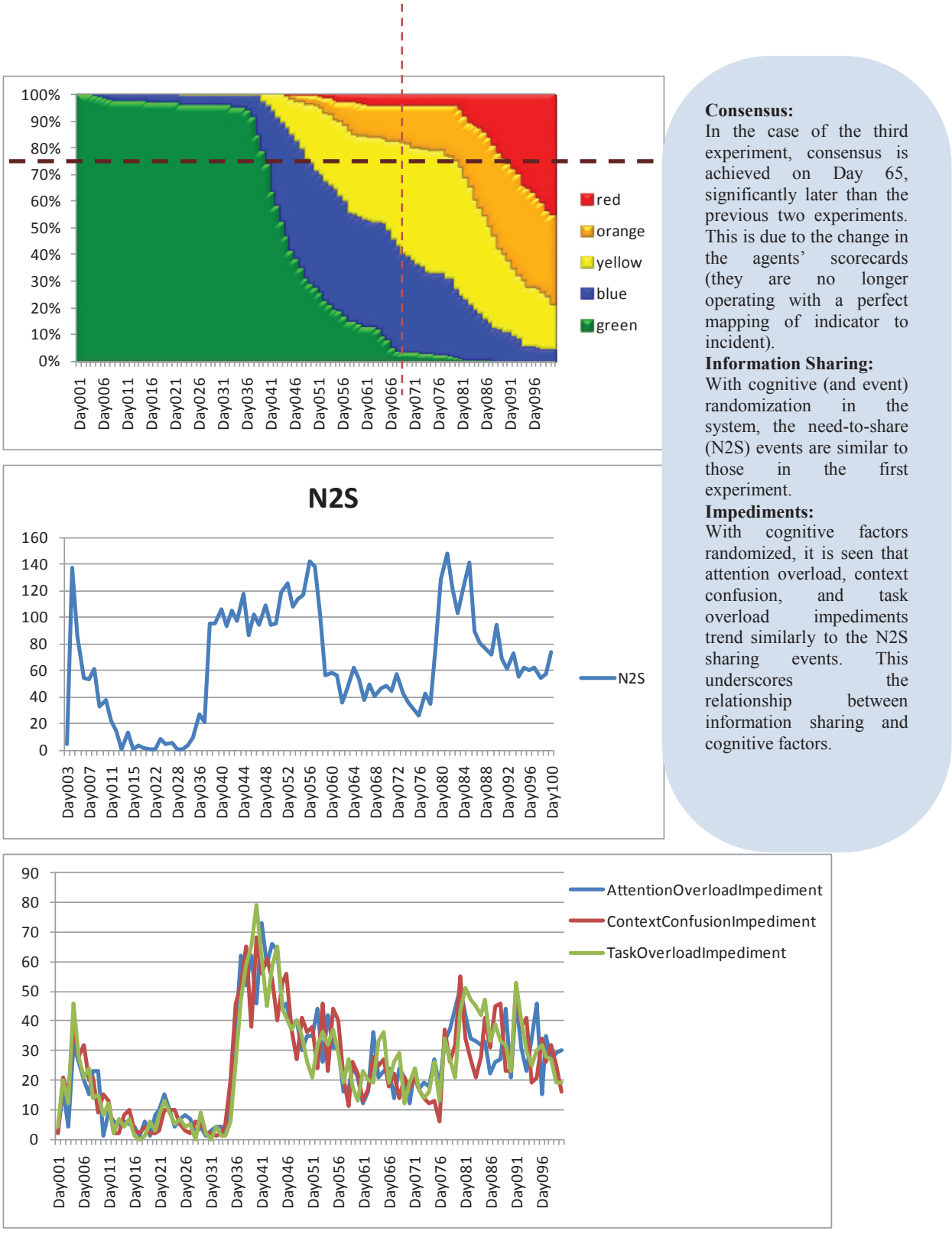
Figure 47: Experiment 2 charts showing consensus outcomes (C1), sharing events (C2), and impediments (C3, C4), with Soc-True Cog-False Inf-False.

6.3 Experiment 3: Soc-False Cog-True Inf-False

The parameters that have been randomized in this experiment are shown in Table 4.

Table 4: Tested features in Experiment 3.

Key Component	Parameters	Randomized Features
Social	Need-to-Share Receivers	N/A
	Need-to-Share Senders	N/A
Cognitive	Human Factors	Reputation Risk Threshold, Organizational Alignment, Uncertainty Comfort, Risk Level Threshold, Attention Overload Frequency, Context Confusion Frequency, Task Overload Frequency, Time (Observation, Documenting, Risk Checking, Publishing)
	Problem Scorecards (Risk Levels)	Scorecard Type, Goldilocks Randomness, Indicator Score, Risk Likelihood Threshold (Green, Blue, Yellow, Orange, Red)
	Organizational Opinions	Cultural Restrictiveness, Classification Clearance, Technical Clearance
Information	Information Properties	N/A
	Classification Levels	N/A
	Technical Levels	N/A
Event	Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences
	Non-Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences



Consensus:
In the case of the third experiment, consensus is achieved on Day 65, significantly later than the previous two experiments. This is due to the change in the agents' scorecards (they are no longer operating with a perfect mapping of indicator to incident).

Information Sharing:
With cognitive (and event) randomization in the system, the need-to-share (N2S) events are similar to those in the first experiment.

Impediments:
With cognitive factors randomized, it is seen that attention overload, context confusion, and task overload impediments trend similarly to the N2S sharing events. This underscores the relationship between information sharing and cognitive factors.

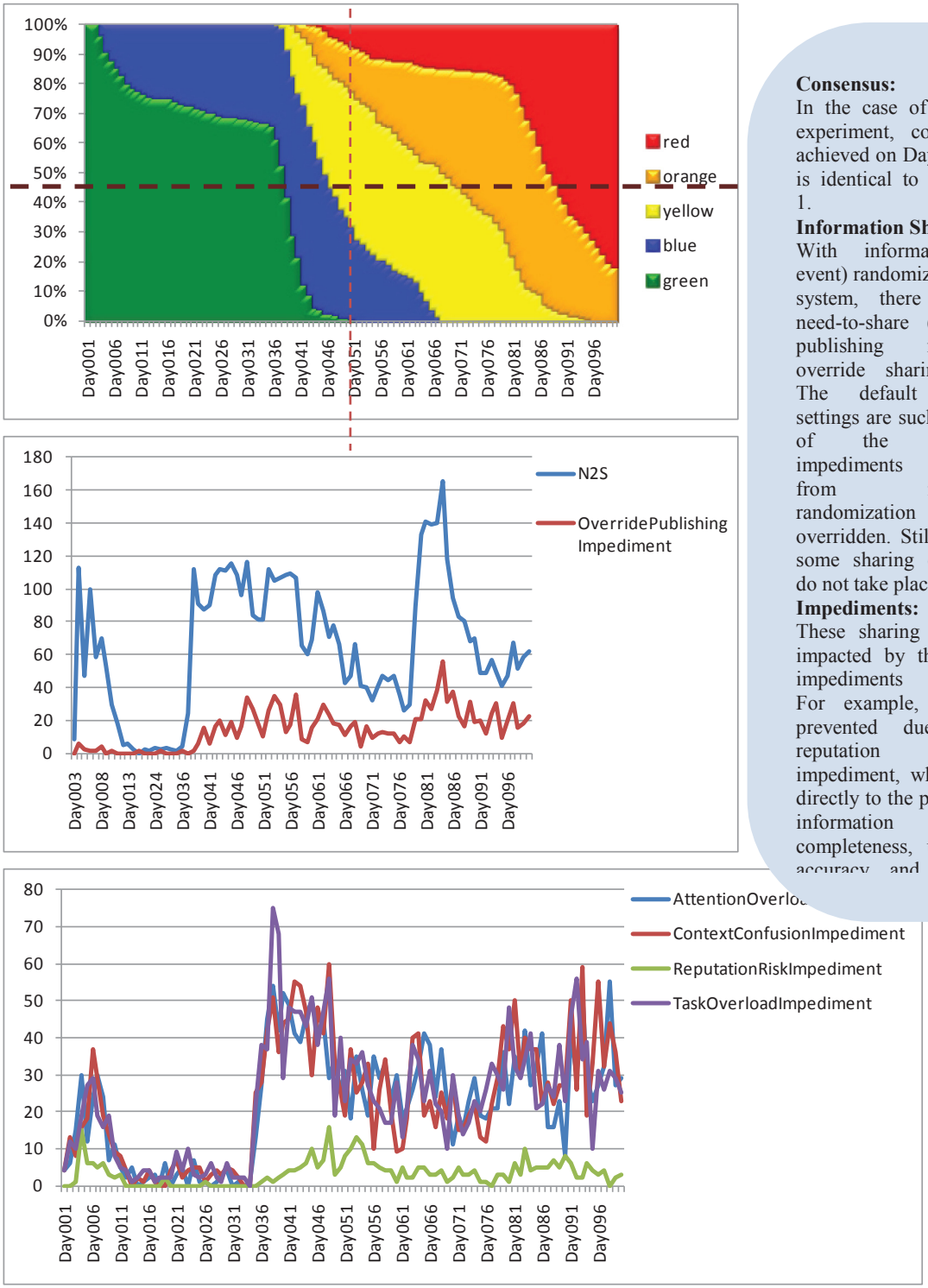
Figure 48: Experiment 3 charts showing consensus outcomes (C1), sharing events (C2), and impediments (C3, C4), with Soc-False Cog-True Inf-False.

6.4 Experiment 4: Soc-False Cog-False Inf-True

The parameters that have been randomized in this experiment are shown in Table 5.

Table 5: Tested features in Experiment 4.

Key Component	Parameters	Randomized Features
Social	Need-to-Share Receivers	N/A
	Need-to-Share Senders	N/A
Cognitive	Human Factors	N/A
	Problem Scorecards (Risk Levels)	N/A
	Organizational Opinions	N/A
Information	Information Properties	Ownership Degree, Uncertainty, Accuracy, Completeness, Credibility
	Classification Levels	Classification Levels
	Technical Levels	N/A
Event	Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences
	Non-Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences



Consensus:
In the case of the fourth experiment, consensus is achieved on Day 46, which is identical to Experiment 1.

Information Sharing:
With information (and event) randomization in the system, there are both need-to-share (N2S) and publishing impediment override sharing events. The default cognitive settings are such that some of the publishing impediments resulting from information randomization can be overridden. Still, there are some sharing events that do not take place.

Impediments:
These sharing events are impacted by the level of impediments occurring. For example, some are prevented due to the reputation risk impediment, which relates directly to the properties of information such as completeness, uncertainty, accuracy and credibility

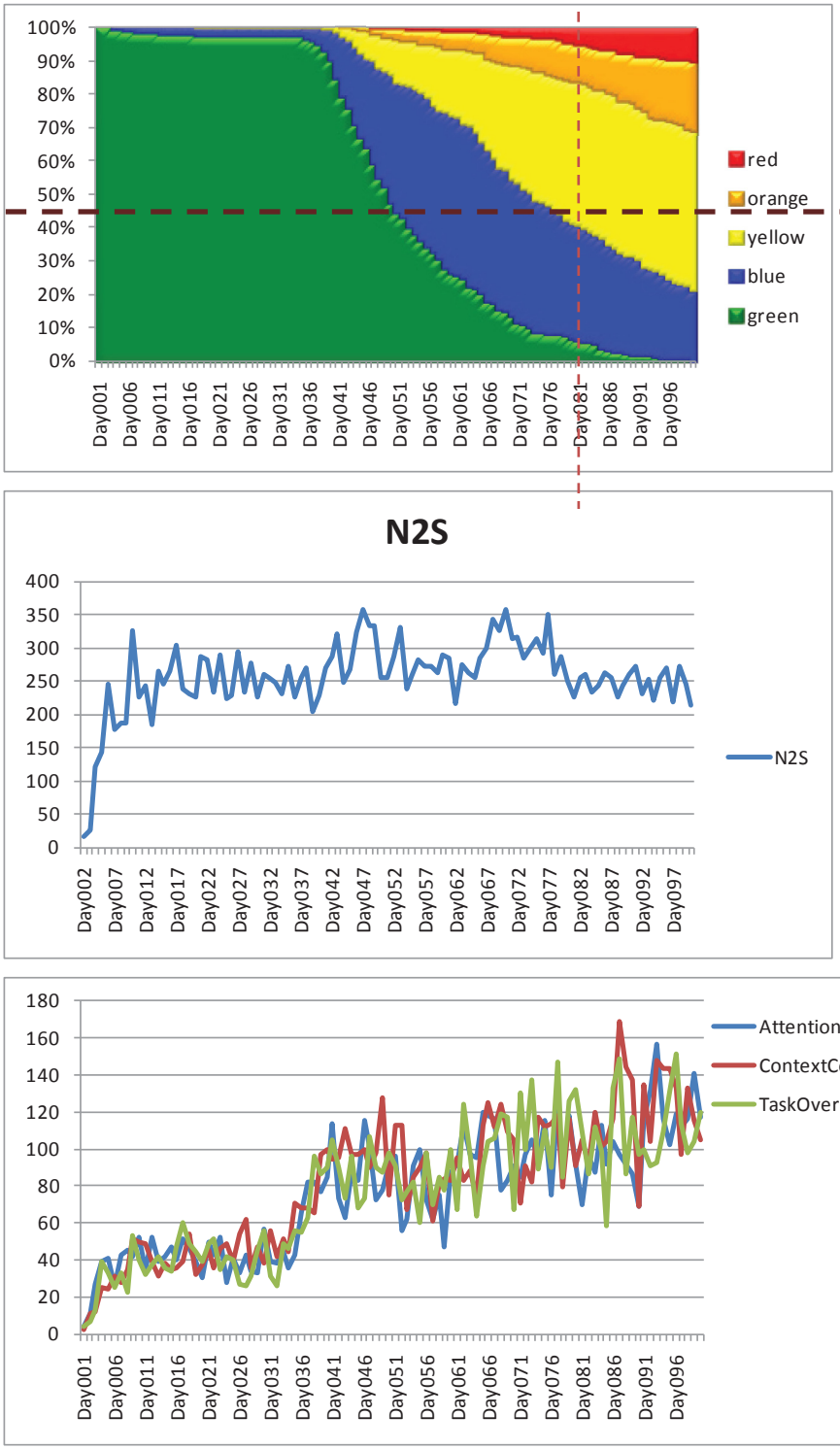
Figure 49: Experiment 4 charts showing consensus outcomes (C1), sharing events (C2), and impediments (C3, C4), with Soc-False Cog-False Inf-True.

6.5 Experiment 5: Soc-True Cog-True Inf-False

The parameters that have been randomized in this experiment are shown in Table 6.

Table 6: Tested features in Experiment 5.

Key Component	Parameters	Randomized Features
Social	Need-to-Share Receivers	Need-to-Share Receivers
	Need-to-Share Senders	Need-to-Share Senders
Cognitive	Human Factors	Reputation Risk Threshold, Organizational Alignment, Uncertainty Comfort, Risk Level Threshold, Attention Overload Frequency, Context Confusion Frequency, Task Overload Frequency, Time (Observation, Documenting, Risk Checking, Publishing)
	Problem Scorecards (Risk Levels)	Scorecard Type, Goldilocks Randomness, Indicator Score, Risk Likelihood Threshold (Green, Blue, Yellow, Orange, Red)
	Organizational Opinions	Cultural Restrictiveness, Classification Clearance, Technical Clearance
Information	Information Properties	N/A
	Classification Levels	N/A
	Technical Levels	N/A
Event	Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences
	Non-Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences



Consensus:
In the case of the fifth experiment, consensus is achieved on Day 72, which is relatively late in the simulation. This is due to the combined effect of delays resulting from more information sharing and imperfect scorecards.

Information Sharing:
With both social and cognitive factors randomized in the system (in addition to event randomization), the number of need-to-share (N2S) events is consistently high. Once again, this is due primarily to the effect of social randomization.

Impediments:
These sharing events are impacted by the level of impediments occurring. As more sharing takes place, more observation impediments occur resulting in delays.

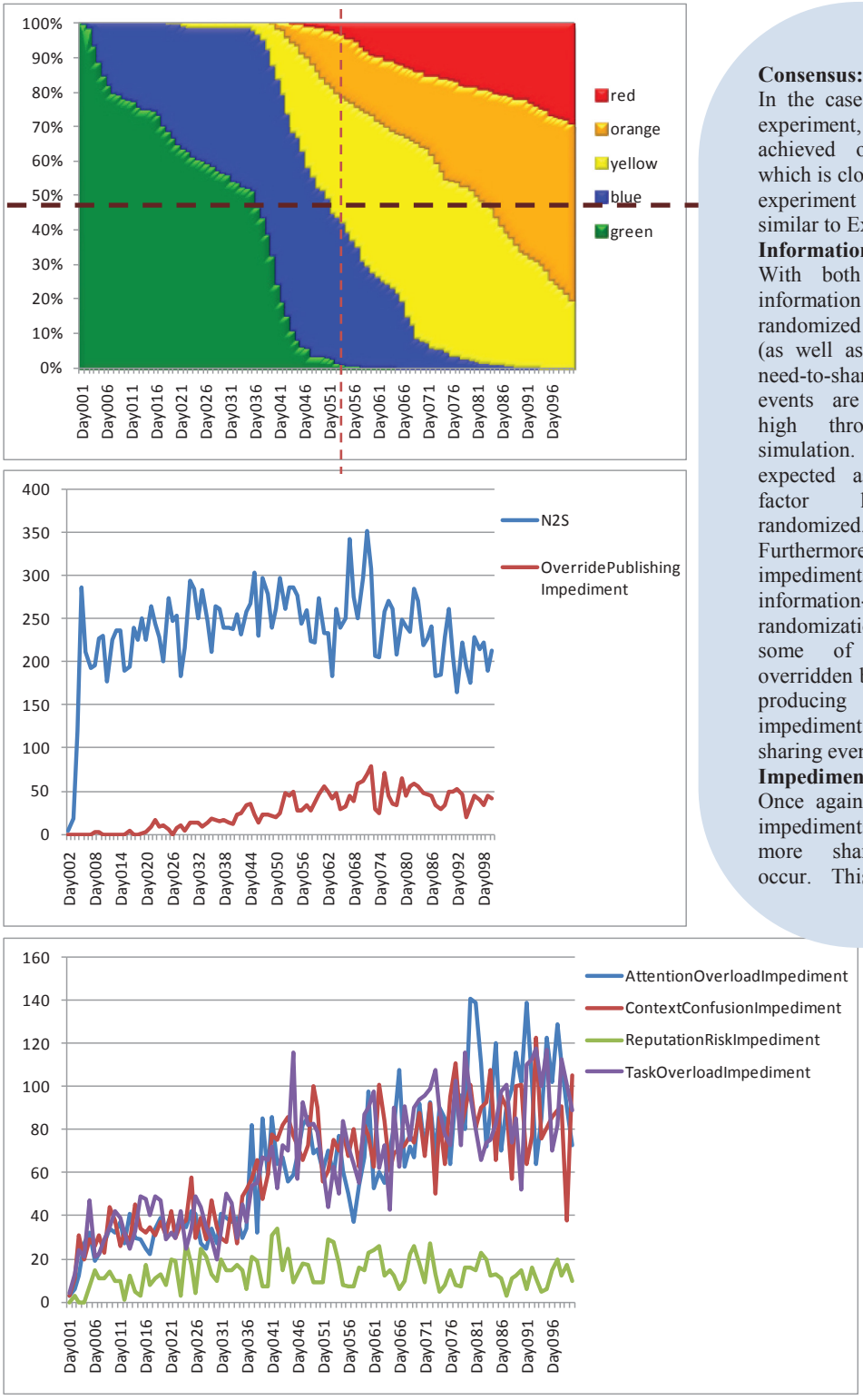
Figure 50: Experiment 5 charts showing consensus outcomes (C1), sharing events (C2), and impediments (C3, C4), with Soc-True Cog-True Inf-False.

6.6 Experiment 6: Soc-True Cog-False Inf-True

The parameters that have been randomized in this experiment are shown in Table 7.

Table 7: Tested features in Experiment 6.

Key Component	Parameters	Randomized Features
Social	Need-to-Share Receivers	Need-to-Share Receivers
	Need-to-Share Senders	Need-to-Share Senders
Cognitive	Human Factors	N/A
	Problem Scorecards (Risk Levels)	N/A
	Organizational Opinions	N/A
Information	Information Properties	Ownership Degree, Uncertainty, Accuracy, Completeness, Credibility
	Classification Levels	Classification Levels
	Technical Levels	N/A
Event	Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences
	Non-Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences



Consensus:
In the case of the sixth experiment, consensus is achieved on Day 50, which is close to the base experiment and very similar to Experiment 2.

Information Sharing:
With both social and information factors randomized in the system (as well as events), the need-to-share (N2S) events are consistently high throughout the simulation. This is expected as the social factor has been randomized.
Furthermore, publishing impediments occur due information-factor randomization; however, some of these are overridden by the agents, producing publishing impediment override sharing events.

Impediments:
Once again, observation impediments increase as more sharing events occur. This results in

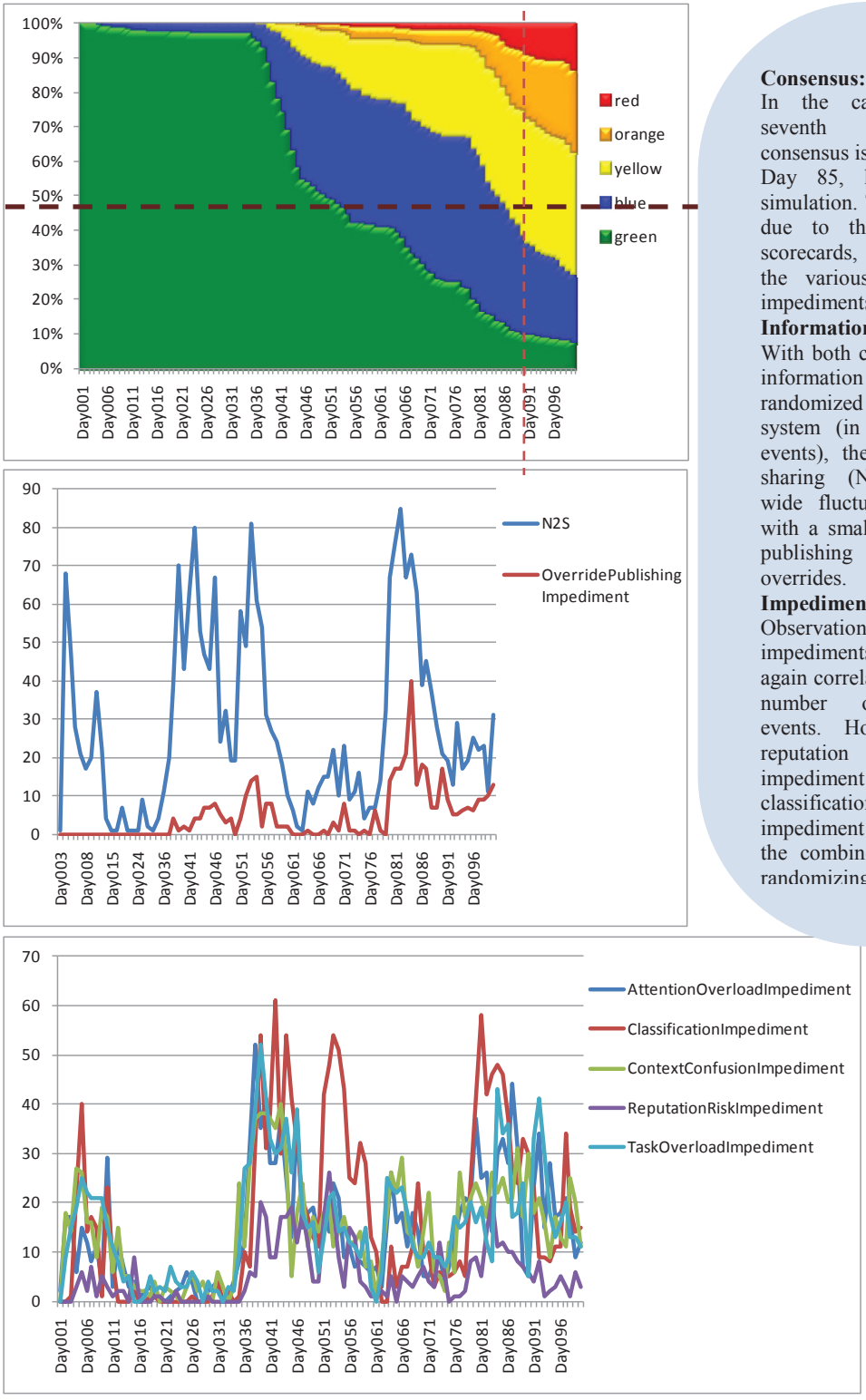
Figure 51: Experiment 6 charts showing consensus outcomes (C1), sharing events (C2), and impediments (C3, C4), with Soc-True Cog-False Inf-True.

6.7 Experiment 7: Soc-False Cog-True Inf-True

The parameters that have been randomized in this experiment are shown in Table 8.

Table 8: Tested features in Experiment 7.

Key Component	Parameters	Randomized Features
Social	Need-to-Share Receivers	N/A
	Need-to-Share Senders	N/A
Cognitive	Human Factors	Reputation Risk Threshold, Organizational Alignment, Uncertainty Comfort, Risk Level Threshold, Attention Overload Frequency, Context Confusion Frequency, Task Overload Frequency, Time (Observation, Documenting, Risk Checking, Publishing)
	Problem Scorecards (Risk Levels)	Scorecard Type, Goldilocks Randomness, Indicator Score, Risk Likelihood Threshold (Green, Blue, Yellow, Orange, Red)
	Organizational Opinions	Cultural Restrictiveness, Classification Clearance, Technical Clearance
Information	Information Properties	Ownership Degree, Uncertainty, Accuracy, Completeness, Credibility
	Classification Levels	Classification Levels
	Technical Levels	N/A
Event	Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences
	Non-Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences



Consensus:
In the case of the seventh experiment, consensus is achieved on Day 85, late in the simulation. This delay is due to the imperfect scorecards, as well as the various publishing impediments.

Information Sharing:
With both cognitive and information factors randomized in the system (in addition to events), the amount of sharing (N2S) shows wide fluctuation levels with a small number of publishing impediment overrides.

Impediments:
Observation impediments are once again correlated with the number of sharing events. However, the reputation risk impediment and classification impediment result from the combined effect of randomizing cognitive

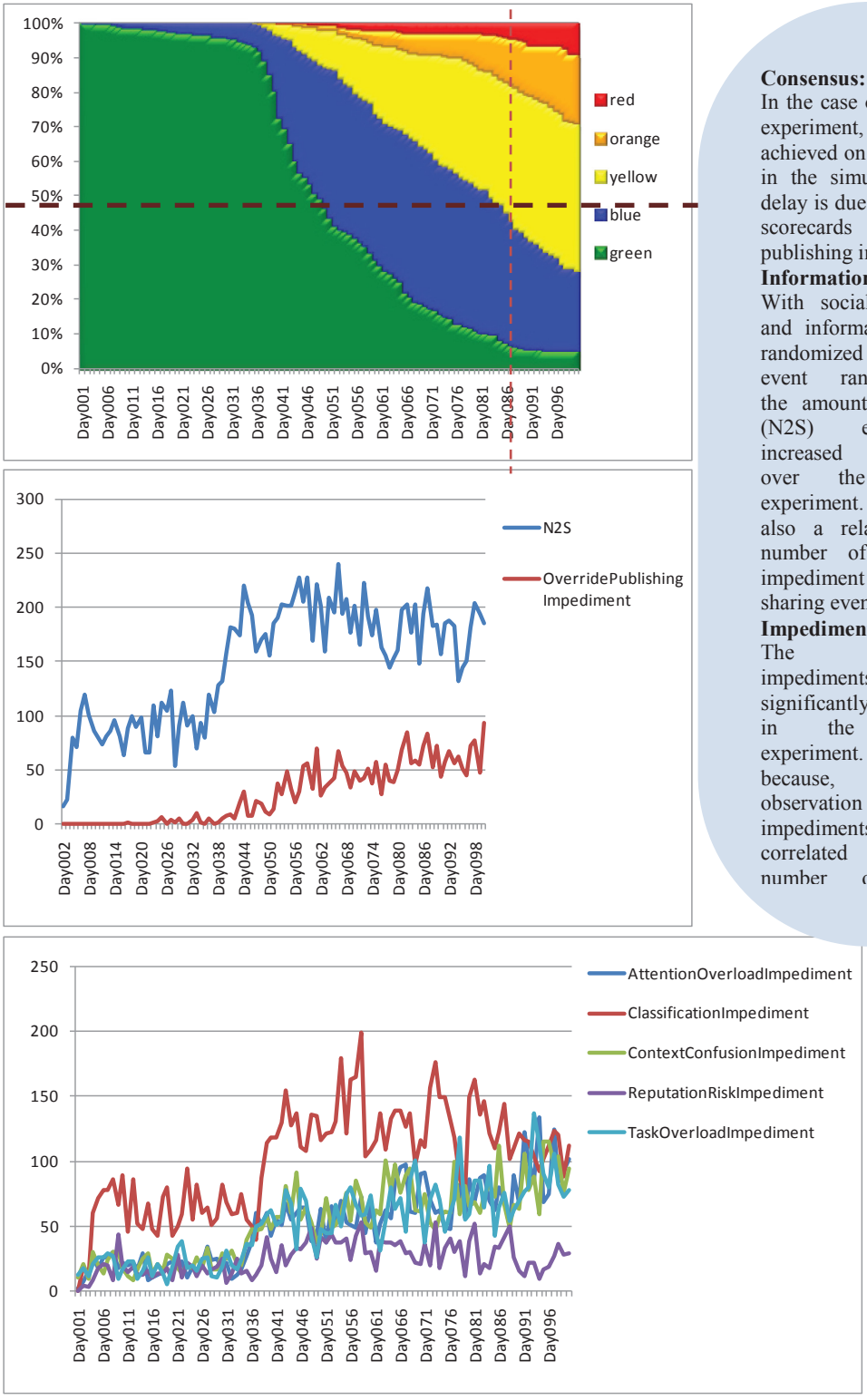
Figure 52: Experiment 7 charts showing consensus outcomes (C1), sharing events (C2), and impediments (C3, C4), with Soc-False Cog-True Inf-True.

6.8 Experiment 8: Soc-True Cog-True Inf-True

The parameters that have been randomized in this experiment are shown in Table 9.

Table 9: Tested features in Experiment 8.

Key Component	Parameters	Randomized Features
Social	Need-to-Share Receivers	Need-to-Share Receivers
	Need-to-Share Senders	Need-to-Share Senders
Cognitive	Human Factors	Reputation Risk Threshold, Organizational Alignment, Uncertainty Comfort, Risk Level Threshold, Attention Overload Frequency, Context Confusion Frequency, Task Overload Frequency, Time (Observation, Documenting, Risk Checking, Publishing)
	Problem Scorecards (Risk Levels)	Scorecard Type, Goldilocks Randomness, Indicator Score, Risk Likelihood Threshold (Green, Blue, Yellow, Orange, Red)
	Organizational Opinions	Cultural Restrictiveness, Classification Clearance, Technical Clearance
Information	Information Properties	Ownership Degree, Uncertainty, Accuracy, Completeness, Credibility
	Classification Levels	Classification Levels
	Technical Levels	N/A
Event	Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences
	Non-Routine-Event Timeline Properties	Insertion Time, Probability of Occurrence, Allowable Occurrences



Consensus:
In the case of the eighth experiment, consensus is achieved on Day 82, late in the simulation. This delay is due to imperfect scorecards and publishing impediments.

Information Sharing:
With social, cognitive, and information factors randomized (as well as event randomization), the amount of sharing (N2S) events is increased significantly over the previous experiment. There is also a relatively high number of publishing impediment override sharing events.

Impediments:
The publishing impediments are significantly higher than in the previous experiment. This is because, like observation impediments, they are correlated with the number of sharing

Figure 53: Experiment 8 charts showing consensus outcomes (C1), sharing events (C2), and impediments (C3, C4), with Soc-True Cog-True Inf-True.

6.9 Summary of Experiments

The experiments have highlighted the relationship between the key factors—social, cognitive, and information—being investigated in this study, and the results are summarized in Table 10. In particular, it is seen that the cognitive factor is the most influential, since randomizing it in isolation results in the largest increase in time-to-consensus when compared with the other factors. Randomizing either the social or the information factor alone results in near baseline-level consensus, a result similar to when these factors are randomized simultaneously. The social factor has some effect on simulation outcome, with a small increase in time-to-consensus, while the information factor results in little-to-no impact. However, when these are combined with the randomized cognitive factor, a surprising increase in the time-to-consensus is seen, pointing to complex relationships across the social-cognitive and information-cognitive boundaries.

Table 10: Summary of the experimental effect of key Social, Cognitive, and Information factors

Experiment Number	Randomization of Key Factors				Observation Impediment Level	Publishing Impediment Level	Publishing Override Level	Time to Consensus
	Social	Cognitive	Information	Events	C3	C4	C2	C1
1	FALSE	FALSE	FALSE	TRUE	High	N/A	N/A	Day 46
2	TRUE	FALSE	FALSE	TRUE	High	N/A	N/A	Day 51
3	FALSE	TRUE	FALSE	TRUE	High	N/A	N/A	Day 65
4	FALSE	FALSE	TRUE	TRUE	High	Low	Low	Day 46
5	TRUE	TRUE	FALSE	TRUE	High	N/A	N/A	Day 72
6	TRUE	FALSE	TRUE	TRUE	High	Low	Low	Day 50
7	FALSE	TRUE	TRUE	TRUE	High	High	Med	Day 85
8	TRUE	TRUE	TRUE	TRUE	High	High	Med	Day 82

7 Discussion

While the current proof-of-concept simulation does include many features, there are many more left to investigate. This section outlines three such examples that were initially planned to be included: need-to-know sharing, technical impediments, and multiple scorecards.

The exploration of need-to-share versus need-to-know (see Figure 54) offers an interesting research landscape. At present, only mandated need-to-share (or push) communication is implemented. Information requests from agents to collect evidence to support or refute that a particular incident is imminent should be added in the future. This would provide further realism to the simulator.

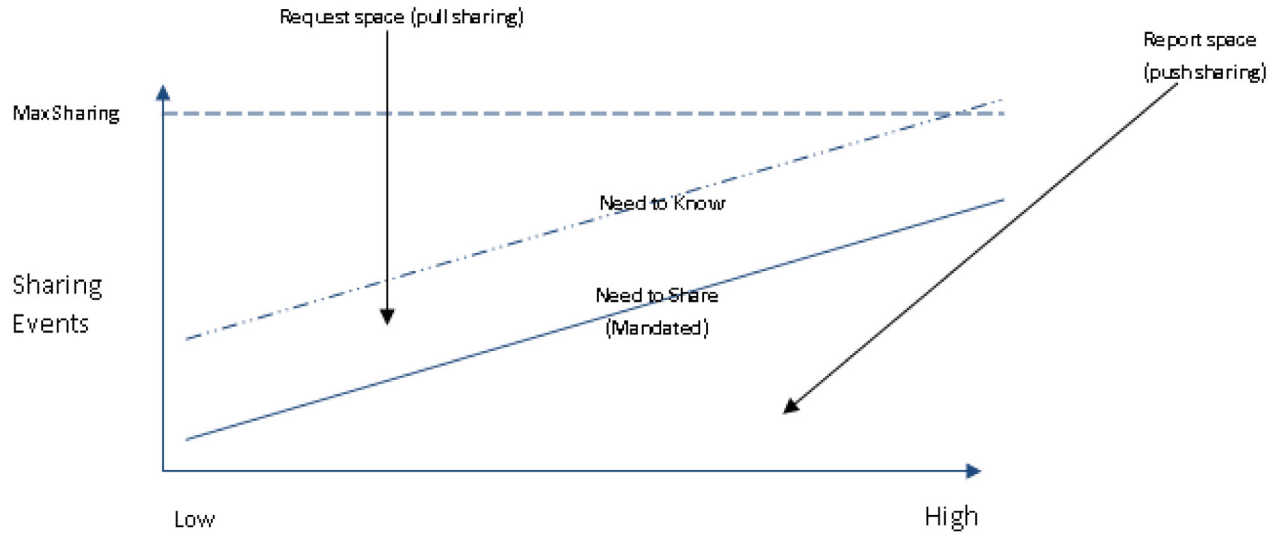


Figure 54: Need-to-Share (Push Sharing) vs. Need-to-Know (Pull Sharing).

While technical impediments have been included in the simulation, this feature was effectively deactivated (i.e., the technical level requirement of all information was set to the lowest level and was not randomized). It is recognized that this is an important feature in real-world analysis of information sharing, as it represents the technical ability of one organization's information system to interoperate with another organization. However, accurately setting this feature would require domain expert knowledge, but should be incorporated in the future.

Finally, all agents in the current simulation rely on a single scorecard to assess whether an incident is imminent based on observed indicators. In actuality, an agent is simultaneously aware of several potential incidents, and various indicators may be shared across these incidents equally. Having multiple scorecards would add further realism to the simulation, but is left for subsequent phases of development.

8 Conclusion and Future Work

This work has presented the latest extension to the HSE simulation with the development of an improved simulator based on a comprehensive architectural design. This design has been implemented and tested on a validated scenario that builds on models proposed in previous project deliverables. The simulator incorporates key human-factor and business-process models based on a multi-dimensional approach that includes the structural, functional, normative, cognitive, social, information, and physical dimensions. The main objective of this deliverable—namely, to present the analysis of the effect of key social, cognitive, and information factors, as well as configuration relationships, on goal achievement—has been shown for the domain of information sharing and the goal of joint-consensus achievement. The experimental results indicate that the tested parameters within the cognitive factor set outweigh the parameters in both the social and the information factor sets.

This work has laid the foundation for future multi-agent systems analysis of the impact of human factors on organizational outcomes by addressing the following key concerns: (i) the selection of a method to capture and discuss fuzzy human factors, (ii) a design approach for including human factors within agents, (iii) a methodology for conducting simulated human-factor analysis, and (iv) the development of a proof-of-concept simulator for testing multiple human-factor configurations. Although there remains much to be added, the current HSE simulation tool provides a usable and extensible tool for investigating human factors. Future work will involve the documentation of "lessons learned" throughout the course of this research.

References

[1] Modelling Meta-Organizational Collaboration and Decision Making. Technology Investment Fund (TIF) Project Proposal. 2007.

[2] Bicocchi, N., Ross, W., Ulieru, M. "Modelling and Simulating Organizations in Emergency-Response Operations." TIF Project Deliverable 1&2. January 2010.

[3] Morris, A., Ross, W., Ulieru, M. "Extending Modelling and Simulation Capabilities for a Generic Harbour Domain." TIF Project Deliverable 3. August 2010.

[4] Modelling Public Security Operations: Verification & Validation of the Extended HSE Simulation. TIF Project Deliverable 4. November 6, 2010.

[5] Vicente, K. The Human Factor: Revolutionizing the way People Live with Technology. Routledge, 2004.

[6] Morris, A., Ross, W., and Ulieru M. Modelling Culture in Multi-agent Organizations, Proceedings of AAMAS 2011, The 10th International Conference on Autonomous Agents and Multi-Agent Systems, Taipei, Taiwan, May 2-6, 2011.

[7] Morris, A., Ross, W., and Ulieru M., and Whitacre, J., The Evolution of Cultural Resilience and Complexity, 8th International Conference on Complex Systems, ICCS 2011, Boston, June 2011.

[8] Ross, W., Morris, A., and Ulieru M. Exploring the Impact of Network Structure on Organizational Culture Using Multi-Agent Systems, 8th International Conference on Complex Systems, ICCS 2011, Boston, MA, USA, June 29-July 2, 2011.

[9] Clancey, W., Sachs, P., Sierhuis, M., Van Hoof, R.: Brahms: Simulating practice for work systems design. International Journal of Human Computer Studies 49(6), 831-866 (1998).

[10] Dignum, V., "A model for organizational interaction: based on agents, founded in logic." Accessed from: http://igitur-archive.library.uu.nl/dissertations/2003-1218-115420/inhoud.htm. 2004.

[11] Morris, A., Ross, W., and Ulieru, M. A system dynamics view of stress: Towards human-factor modeling with computer agents. IEEE International Conference on Systems Man and Cybernetics (SMC), 2010 pp. 4369-4374.

[12] Department of Homeland Security, "Citizen Guidance on the Homeland Security Advisory System." Accessed from: http://www.dhs.gov/xlibrary/assets/CitizenGuidanceHSAS2.pdf

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Adaptive Risk Management Lab
Faculty of Computer Science
University of New Brunswick;

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED
(NON-CONTROLLED GOODS)
DMC A
Review GCEC JUNE 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Modelling Public Security Operations: Analysis of the Effect of Key Social, Cognitive, and Informational Factors with Security System Relationship Configurations for Goal Achievement

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Morris, A.; Ross, W.; Ulieru, M.

5. DATE OF PUBLICATION (Month and year of publication of document.)

December 2012

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

72

6b. NO. OF REFS (Total cited in document.)

12

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contractor Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

TIF Project: Meta-Organizational Collaboration and Decision Making – Project 10af
DRDC Centre for Security Science
222 Nepean St.
Ottawa, ON

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC CSS CR 2012-028

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unclassified

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited Distribution

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

More so than engineered systems, human factors, and specifically having humans-in-the-loop, can lead to unforeseen behaviours resulting in unexpected organizational failures. In the world of emergency response, these failures may be related not only to response activities, but also to information processing and sharing that consequently undermine the organizational ecosystems' situational awareness of unfolding events. The TIF project, Modelling Public Security Operations, has the goal of accounting for the human factor by more fully exploring its inherent complexity through experiments and simulations. This report presents the design, implementation and results of a Holistic Security Ecosystem (HSE) simulator for representing organizations and decision making processes and the impact of key social, cognitive and informational factors. Earlier research investigated key factors, processes, and simulation methodologies**.**

Plus que les systèmes sophistiqués, les facteurs humains, et plus particulièrement lorsque des humains interviennent, peuvent mener à des comportements imprévus entraînant des échecs organisationnels imprévus. Dans le monde des interventions d'urgence, ces échecs peuvent être reliés non seulement aux activités d'intervention, mais aussi au traitement et à l'échange de l'information qui minent la capacité de l'organisation à jauger la situation à mesure qu'elle évolue. Le projet FIT, la modélisation des opérations de sécurité publique, vise à tenir compte du facteur humain en examinant plus amplement sa complexité inhérente au moyen d'expériences et de simulations. Le présent rapport porte sur la conception, l'instauration et les résultats de la simulation d'EHS pour représenter les organisations et le processus de prise de décisions, et pour simuler l'incidence des principaux facteurs sociaux, cognitifs et informationnels. Les principaux facteurs, processus et méthodes de simulation ont été examinés dans le cadre de précédents travaux de recherche.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Organizations, organizational design, whole of government, comprehensive approach, modelling and simulation, agent-based simulation, groups, group dynamics, decision making, group behaviour, enterprise architecture, business process modelling, human factors