Managing ISR sharing policies at the network edge using Controlled English

Christos Parizas[a], Diego Pizzocaro[a], Alun Preece[a]
Petros Zerfos[b]

[a]School of Computer Science and Informatics, Cardiff University, UK

[b]IBM T.J. Watson research Center Hawthorne, NY, USA

ABSTRACT

In domains such as emergency response and military operations the sharing of Intelligence, Surveillance and Reconnaissance (ISR) assets among different coalition partners is regulated through policies. Traditionally, policies are created at the center of a coalitions network by high-level decision makers and expressed in low-level policy languages (e.g. Common Information Model SPL) by technical personnel, which makes them difficult to be understood by non-technical users at the edge of the network. Moreover, policies must often be modified by negotiation among coalition partners, typically in rapid response to the changing operational situation. Commonly, the users who must cope first with situational changes are those on the edge, so it would be very effective if they were able to create and negotiate policies themselves. We investigate the use of Controlled English (CE) as a means to define a policy representation that is both human-friendly and machine processable. We show how a CE model can capture a variety of policy types, including those based on a traditional asset ownership model, and those defining team-based asset sharing across a coalition. The use of CE is intended to benefit coalition networks by bridging the gap between technical and non-technical users in terms of policy creation and negotiation, while at the same time being directly processable by a policy-checking system without transformation to any other technical representation.

Keywords: Controlled English, High-level Policy languages, ISR system configure & control, Sensor networks, Distributed decision-making

1. INTRODUCTION

From conventional military to disaster relief operations accurate, reliable and actionable intelligence is needed in order for the operations to be effective. The proportion of this intelligence is increasingly produced by Intelligence, Surveillance and Reconnaissance (ISR) systems, which provide key capabilities to the command authorities for intelligence collection, exploitation and battle management. An ISR system can be for example used for boarder reconnaissance and surveillance or object detection and localisation. In aforementioned environments ad-hoc Communities of Interest (CoIs) act together to achieve a set of common objectives forming coalitions. Recent history shows that coalition operations are going to be the norm and not the exception.[1] A coalition is a set of organisations that work together usually in peer-to-peer environments where, through collective collaboration, they are able to jointly perform tasks that they would not be able to perform or perform poorly otherwise.[2] Coalition partners own different sets of resources, which they are willing to share with different subsets of collaborative responders in accordance with policies and procedures. Several issues emerge due to the multi-partner dimension of coalitions. Especially in military operations, ISR resources are nationally-owned and operated systems and so their sharing is often limited by security constraints,[1] which is a defining factor in the collaboration between coalition partners. These constraints are usually expressed through policies. A policy is a condition-action pair, where the specified action is executed if the condition evaluates to true.

An additional characteristic of the aforementioned environments is that they are highly dynamic. The decision makers operating in such an endeavour are usually required to deal with military, social, political and economic effects taking place simultaneously at the area of operation (AO).[3] These effects are interrelated and make the environment that the decision makers want to influence more complex and dynamic and at the same time less understood and predictable. The need for agile tasking of ISR systems is pointed in several studies such as,[4] where a plan for management of coalition sensor networks was proposed. Together with issues related to ISR asset deployment in highly dynamic environments, the different constraints imposed by security, privacy and sharing issues of such resources in a coalition context are usually regulated through policies. Thus we need to consider a policy development and enforcement model which is able to quickly, easy and distributedly form, reform and negotiate access to resources according to operational changes.

A key step towards the development of such a model is to push policy development (thus, the decision making center) close to the source of situational changes in order to reduce the reaction time. The users who must first cope with unexpected operational changes are those at or near the edge of the network, so we believe it would be very beneficial if they were able to form, reform and negotiate policies themselves without waiting for a central authority to approve each ISR access request. The Network Edge approach to designing command and control (C2) concepts, organizations and systems to meet requirements of complex endeavors has become popular in recent years as it involves the empowerment of individuals at the edge of the organization.[5] An emerging issue related to pushing decision making through policy formation at or near the edge, is the technical gap between existing low-level policy languages and non-technical users that operate in these areas. The vast majority of personnel at the network and organizational edges are not IT experts and so lack technical skills, e.g. in terms of formal policy languages. Well-known policy enforcement models such as the Watson Policy Management Library[*] (WPML) currently support low-level policy languages such as the Common Information Model Simple Policy Language[†] (CIM-SPL), which are difficult to understand and use for policy development by non-technical users at the edge.

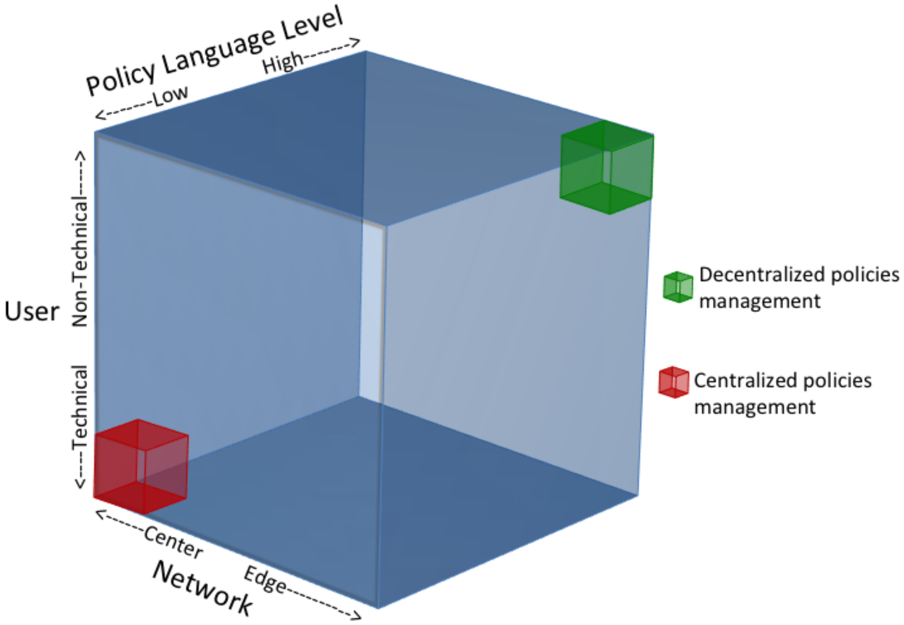

Figure 1. Pushing the policies formation at the edge.

In Figure 1 we portray the aforementioned hypothesis and present the centralized and decentralized policy management approaches in the operation/organisation network. The three axes in the blue cube represent the three main features related to ISR policy enforcing in a coalition environment. The user types that operate in such environments in terms of their IT expertise, which varies from Technical to Non-Technical, the place in the organization network where users operate which varies from Center (e.g. a military base) to Edge (e.g. warfare

[*] `https://www.ibm.com/developerworks/community/groups/service/html/communityview?communityUuid=ed556565-1d91-4289-94ae-213df1340350`

[†] `http://www.dmtf.org/sites/default/files/standards/documents/DSP0231_1.0.0.pdf`

theater) and the level of the applied policy language which might be either Low (e.g. a technical language understood only by IT experts) or High (e.g. a language close to natural language easy to be understood by non-experts). The red cube represents the current state of policy development and enforcement models, which can be developed by technical users operating near or at the center of the organisation, using low-level policy representation languages and are cumbersome compared to the highly dynamic military environment. The green cube represents the problem space in which our contribution is situated. A policy model, which is able to cope with highly dynamic environments by enabling the policies development by non-technical users, who operate near or at the edge using high-level interface policy languages. In other words, the red cube represents a centralised directive management system based on the Industrial Age model, while the green represent a decentralised, emergent management system based on the Information Age model.[6] It is worth noting that the user and network variables in Figure 1 are not binary ones. This means that the users can span from IT experts to users who lack any technical skills including those with different technical knowledge levels. We claim that a high-level interface policy model can empower non-technical users (e.g. military planners and intelligence analysts) while at the same time cause no loss of technical users' expressiveness power (e.g. power provided via usage of low-level policy languages). As far as the organisation network is concerned we focus on users that operate at any place in between the military headquarters and the head of a battlefield operation.

In this paper we use a Controlled Natural Language (CNL) named Controlled English[7] (CE) as a means to define a policy representation that is both human-friendly and unambiguous for computers. CE is a human understandable version of Common Logic that is used here to represent and execute a set of high-level [‡] formal rules. The main goals of this paper are:

- to propose a CE-based ontology, which captures the main entities, their properties and the relationships between them of ISR resource sharing in a coalition operation; and
- to investigate whether CE is expressive enough to capture a variety of high-level, attribute-based authorisation policies related to a coalition operation scenario.

We show that a CE-based policy language model benefits a coalition network by: (1) bridging the gap between technical and non-technical users, (2) lowering the technical barrier between non-technical users and the policy language representation and (3) being directly processable by a policy-checking system (no need for any transformation to other technical representations is needed).

The remainder of this paper is organised as follows: In Section 2 we discuss the strengths of *edge* C2 approach, we compare a CE-based policy language, in terms of user friendliness, with a well-known predecessor and we highlight the benefits of *edge* C2 using CE as policy representation. In Section 3 we define and develop in CE an ontology to capture the multi-partner sharing aspects of a coalition operation. In Section 4 we demonstrates the expressiveness of CE as a policy language by developing and executing on the ontology a variety of attribute-based authorisation rules. Finally, in Section 5 we summarise our contributions and discuss future work.

2. ACHIEVING EDGE C2 USING CE

In this section we present an overview of *edge* C2[5] approach, we discuss its strengths and characteristics and we also investigate in which military operations it better fits based on literature. Moreover, we discuss the benefits of *edge* C2 using CE as policy representation language by highlighting the advantages of CE in terms of user friendliness and understandability, which greatly benefit non-technical users.

As previously noted[6] the complexity, uncertainty and dynamics of military operations as far as the collection of entities involved in such endeavours has highly increased in recent years. Therefore the demand for more agile corresponding forces (e.g. human decision-makers, ISR systems and system management methods) increases as well. Over the years the nature of C2 has significantly changed and the currently applied approaches, which are described and further analysed in[3] are presented below.

[‡] In this paper by using the term high-level (language or rule) we refer to the level of interface with the user.

- Conflicted
- De-Conflicted
- Coordinated
- Collaborative
- Edge

Each of these differs from the others along one or more of the following dimensions: (1) Allocation of decision rights, (2) Patterns of interaction and (3) Distribution of information. Moving from the *conflicted* to the *edge* approach the allocation of decision rights goes from no rights to the collective to dynamic and tailored self-allocation to individuals. The patterns of interaction that take place between and among entities goes from no interaction to unlimited and unbounded horizontal interaction, while the information distribution goes from crucial organic information to real time sharing of all available and relevant information (in accordance with policies).

As mentioned previously, the *edge* model empowers the users who operate at the edge of the network while in addition allowing for intra-edge communication without requiring permission from a central authority. Crucial preconditions for a successful application of *edge* model apart from the need for enhanced peer-to-peer horizontal interaction among the users on the field, is the moving of senior personnel into roles operating at the edge.[5] As a result, the need for intermediaries is reduced and an unbundled C2 is achieved. Thus, commanders operating at the edge become more responsible and take further substantial initiatives such as, sharing and allocation of resources and engagement rules establishment in a highly dynamic manner as a response to operational changes. Establishing a broader and deeper degree of shared awareness and understanding as well as a higher adaptability of the collective C2 process, the *edge* seems to be a promising and more effective approach than others.[3] However, it is worth noting that what drives the decision of choosing the appropriate C2 approach for a specific operation lies on the operational effectiveness, which is affected by factors such as nature and capabilities of partners and the dynamics of the situation. Given the aforementioned characteristics of *edge* C2 approach and its inherent agility, it seems to be an ideal approach for contemporary multi-partner, complex and dynamic coalition operations.

Controlled Natural Languages (CNL) were first introduced as an alternative means of knowledge formal representation and they were applied in particular to Semantic Web development. CNLs tried to bridge the gap between formal representation languages (e.g. OWL[§])[8] and natural languages (e.g. English) and introduce a user-friendlier knowledge representation form than the common formal languages, which are admittedly hard to be understood by people unfamiliar with formal notations.[9] Moreover, CNLs being a subset of natural languages (NL) are less complex and ambiguous, so they present improved interpretation for machines compared to NLs. In this work we use Controlled English[7] (CE) as a means to define a policy representation. CE is a type of CNL designed to be readable by a native English speaker whilst representing information in a structured and unambiguous way. The structure of CE is simple but fully defined by a syntax, which makes the language parsable by computer systems. CE aspiring to provide a human-friendly representation format that is directly targeted non-technical, domain-specialist users to encourage a richer integration between human and machine reasoning capabilities.[7] Finally, CE is intended to be the "human face" of the logical specification of the ontology and instances of the ontology while in addition it can also encompass the representation of logical inference rules, facts and rationale.[7]

We argue that it is generally difficult to measure how easy or difficult it is for a language to be understood and learned by a human. Since we have not experimentally tested CEs understandability with the understandability of other lower level well-known policy languages such as CIM-SPL we cannot safely claim that CE is a user friendlier representation than its predecessors. However, there are in literature several works[10–12] which conducted experiments to test and compare the friendliness to humans of CNLs versus formal languages such as OWL. The results of the experiments in all cases led to the fact that CNLs like CE can do better in terms

[§] `http://cies.hhu.edu.cn/pweb/~zhuoming/teachings/MOD/N4/Readings/5.3-B1.pdf` of understandability than formal languages; in addition they can achieve better results in situations where users have little or no technical training.

We introduce and further explain the CE structure and syntax in section 3 where we define the coalition assets sharing ontology. Here, we present a simple authorisation policy rule expressed in both: CIM-SPL in Table 1 and CE in Table 2 representations to show the different levels of human-friendliness of the two approaches. Suppose the simple scenario in a coalition operation context where an authorisation policy, which allows a user to access an asset if the user and the asset are both affiliated with the same partner.

Subject: user
Object: asset
Condition: users partner == assets partner
Decision: allow

```
Condition
{
    subject.affiliation() == object.affiliation()
}
Decision
{
    canAccess.allow()
}
```

Table 1. CIM-SPL representation

```
if
    ( the asset A is affiliated to partner P ) and
    ( the user U is affiliated with the partner P )
then
    ( the user U canAccess the asset A )
.
```

Table 2. CE representation

As these examples show, CE is a more user-oriented representation compared to CIM-SPL, while instead CIM-SPL seems a more concise one compared to CE. It is straightforward to non-technical users to read and understand the policy rule implemented in CE even if they have little or no knowledge of the domain model. CE representation is not far away from the policy plain-text explanation above. On the contrary in order for a user to understand the policy rule implemented in CIM-SPL, some technical-programming skills are needed. However, some training is also needed for a user in order to develop policy rules in CE; for example they need to be aware of the underpinning CE model which determines what kind of sentences can be stated in CE. Although, provided that CE is defined by syntax and grammar rules inherently closer to NL, we believe that also via particular user interfaces (such as Conversational UIs[¶]): the training time for a user to learn composing policies is significantly shorter than the time needed for a user to learn how to develop policy rules in representations such as CIM-SPL. Due to the high level of user-friendliness, the use of CE in operations where *edge* C2 is applied seems to have a wide range of applicability for non-technical users operating at the edge.

Furthermore, the use of high-level languages like CE, which is understood by a larger number of operators, for expressing, extending and modifying domain models (i.e. ontologies) and rules strengthens the connection between loosely-coupled partners in the coalition by helping them understand their current approaches, determine their needs, measure their progress and develop common strategic vision.[3] A side effect of CE's usage is that out of the responders a large part of the society in the AO might be able to potentially participate and contribute to operations[13] due to its readability skills, which make it understood by a native English speaker. Thus, in case it is needed CE can facilitate the establishment of crowd sourcing systems.

3. CONCEPTUALISATION OF THE ONTOLOGY IN CE

In previous work[14] we used CE to express the elements of an OWL-based knowledge base, developed in order to allow automatic matching of sensing tasks and ISR asset types based on the capabilities required and provided by each sensing platform.[15] The motivation for using CE was to increase the transparency of the system in order to support a more interactive Human-in-the-Loop approach. Thus, human users were able to work in a more

[¶] As recently observed in Wired by Dr. Ron Kaplan from Nuance Communications' NLU R&D Lab – `http://www.wired.com/opinion/2013/03/conversational-user-interface/` – checked 27th March 2013.

cooperative manner with the system by exploring the various means of achieving a task and easier consider the option of joining-sharing existing ones. In this paper we focus on the development of a CE-based policy model, extending the previous ontology, in order to deal with the multi-partner sharing aspect of coalition operations. In such case, assets are owned by different parties and can be reserved for the exclusive usage of the owning partner or shared with different subsets of users affiliated to other partners through attribute-based policies.

Being a type of CNL, CE can be used to define domain models, which take the form of concepts definitions. Obeying to first-order logic these concepts comprise objects, their properties and the relationships between them. CE language supports multiple inheritance and can build hierarchies of concepts; using the "is a" syntax in the conceptualise sentences CE can define concepts, which are specialisation and inherit properties of other concepts. Once the CE model is built, it then can be instantiated accordingly, via defining facts, based on the concepts and relationships defined in the model. CE allows any instance to be asserted as any number of concurrent concepts[16] (e.g. "the user U1 is a private and is an intelligence analysts and is a/an..."). CE can also be used for developing rules, which follow the "if - condition – action" form, which can be executed on the model. Both the rules and the results of the rules execution are expressed in CE sentences; no other formal notations are needed. Together with the decision of a rule's execution a rationale is automatically created by the system and is pushed to the user. Rationale is a set of reasoning steps, each one of which is defined as a "because" relation between multiple conditions in different rules and each single decision conclusion. The reasoning steps follow a backward-chaining interpreter in order to calculate and develop the rationale. In section 4 we exploit the rules creation ability of CE in order to define a variety of high-level, attribute-based authorization polices. It should be noted that CE is not based on the idea of verbalising rules, which are already implemented in a formal language, but the prototyped CE rules can be translated to a formal language representation. The IBM Controlled Natural Language Processing Environment[‖] or briefly CE Store is a web application which provides an information-processing environment within which human and machine agents (i.e. Java coded entities) can develop and interact with existing CE-based conceptual models. Within CE Store different types of agents, amongst other can develop logical inference rules (i.e. policy rules) and execute them on a pre-developed conceptual model.

In order to develop authorisation rules we first need to define the ontology, which captures the major objects, their properties and the relationships between them of an ISR system deployed in a coalition operation environment. To do so, we extend and enrich the ontology defined in,[14] with additional objects that are involved in coalition ISR asset-sharing. The core concepts in our ontology are the Users who are the subjects and the Assets which are the objects of the sharing policy rules. Users, given a set of sharing constraints i.e. conditions either can or cannot access each of the Assets. They create sensing tasks (which feed them with sensing information), can be members of special purpose cross-partner CoIs called Teams[**] and are affiliated with a coalition Partner, while Assets can be accessed by Users, can be either a sensor (e.g. camera, microphone) or a service (e.g. acoustic event detector service, camera sensor recognition service) and are owned by a coalition Partner. The full Assets sharing ontology is presented in Figure 2.

Briefly, the asset-task allocation is a two steps process, which consists of the sharing policies evaluation and an asset-task allocation protocol proposed in our previous work.[17] First the user creates a task and an object, which is related to this task named *AssetList* is created in respect to current sharing policies set by coalition partners. These policies consider different sets of user's and available assets properties/attributes as we explain in section 4. Thus, the *AssetList* entity contains all the candidate assets (i.e. sensors and services) that can be accessed by the task's creator after the sharing policies evaluation. Next, the allocation protocol assigns assets to the tasks they best serve following quantitative (in respect to the matching intelligence providing by the CE-based knowledge base) and qualitative (assets assigned to the tasks which perform higher utility) criteria.

For simplicity we hide all the complex knowledge base and matching process into the blue relationship bubble of Figure 2. With the defined model we can capture sharing policies based on a traditional ownership model as well as sharing policies based on an *edge* team-based model. The traditional sharing approach considers a sharing model making resources either available for other partners to use or alternatively reserving them for the

[‖] `https://www.ibm.com/developerworks/mydeveloperworks/groups/service/html/communityview?communityUuid=558d55b6-78b6-43e6-9c14-0792481e4532`

[**] In a typical *edge* coalition operation within a CoI usually there are a number of smaller, more focused CoIs which are dynamically created in response to an on the field event and execute concurrent missions for only a short time.

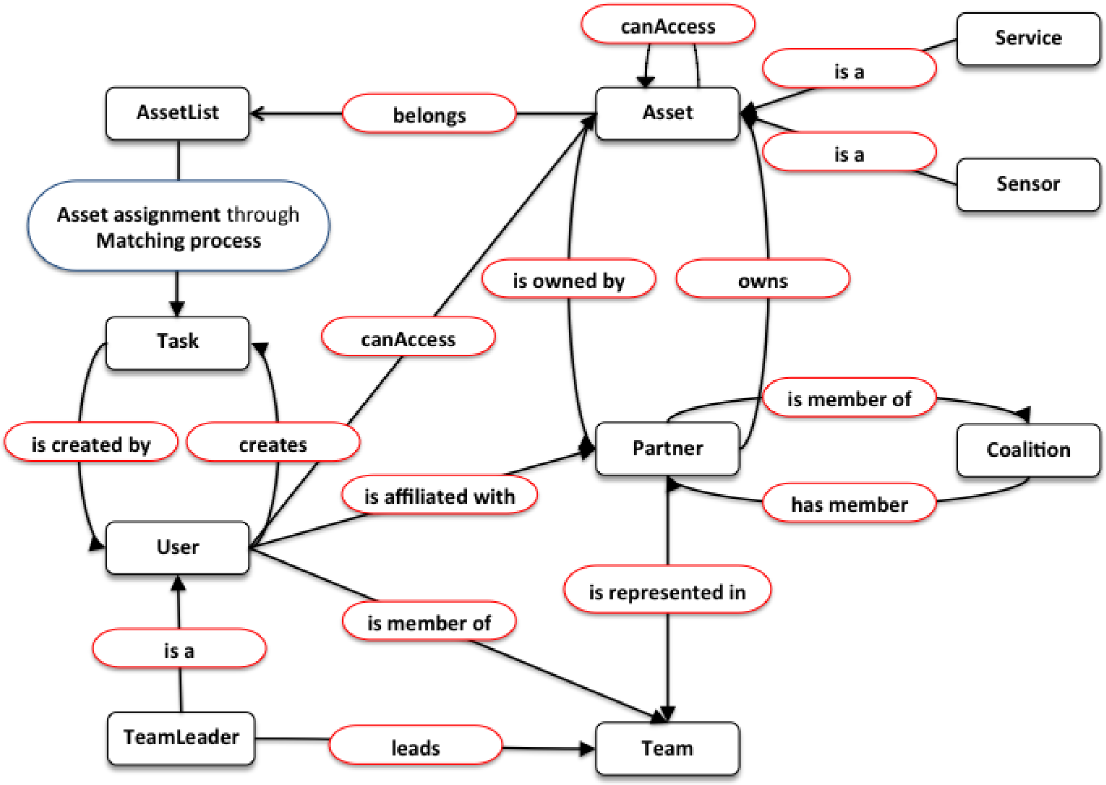

Figure 2. Coalition assets sharing ontology.

exclusive use of the owning partner, while the team-based model allows cross-partner users who participate in the same team to share assets freely. Therefore, team members have access to all assets owned by any coalition partner represented in the team.

With the following sample CE definitions we cover part of the ontology in Figure 2 while we present the basic capabilities and structure of CE as a domain concept developer.

To create a new object in the ontology we simple conceptualise it as follows:

```
conceptualise the assetList L.
```

To define concepts' properties there are two forms, which are semantically identical but allow the subsequent facts to be expressed in slightly different ways:

Verb singular form:

```
conceptualise the team M
  ~ is led by ~ the teamLeader D.
```

Functional noun:

```
conceptualise a ~ coalition ~ C that
  has the partner P as ~ member ~.
```

We can define any number of properties for a concept in a single CE sentence but we currently cannot mix *verb singular* and *functional noon* properties in a single conceptualise sentence, while we can write as many CE sentences as we like for a single concept. The CE Store will amalgamate all sentences for that concept into the model when it loads the sentences.

To define a property with a *textual value* rather than a relationship to another instance we use the word "value" as below:

```
conceptualise an ~ asset ~ A that
  has the value S as ~ scarcity ~ and
  has the value B as ~ sensorType ~ and
  has the value R as ~ serviceType ~ and
  has the value L as ~ capability ~.
```

The following examples declare that a sensor and a teamLeader are subtypes of pre-existing concepts, asset and user respectively. Sub-concepts have inheritance in the normal way, so if we define a property on a parent concept all children inherit that property.

```
conceptualise a ~ sensor ~ R that
  is an asset.

conceptualise a ~ teamLeader ~ D that
  is a user.
```

Once the conceptual model is defined, the next step is the models instantiation through fact sentences. Below we present instantiation examples of some of the objects, properties and relationships represented in ontology of Figure 2.

```
there is a partner named UK.
there is a partner named US.

the partner UK
  is represented in the team t1 and
  owns the asset a1 and
  is member of the coalition US-UK.
the partner US
  is represented in the team t2 and
  owns the asset a2 and
  is member of the coalition US-UK.

there is a user named u1 that
  has 'uid1' as userId and
  has 'intel1' as expertise.
there is a user named u2 that
  has 'uid2' as userId and
  has 'intel3' as expertise.
```

Note that when specifying a value (...has 'intel1' as expertise...) we do not need to say "has the value" but can leave it out for readability. Once we have defined and instantiated the ontology then we can develop and execute rules on it as it shown in Section 4 through the interface provided by CE Store.

4. CE POLICY RULES

In this section we develop high-level, attribute-based authorisation policies expressed in CE. Our goal is to verify whether CE is expressive enough to capture a variety of sharing rules. We experiment with different levels of access to resources and we show the flexibility of CE as a sharing policy representation.

Research and development in policy technologies within International Technology Alliance[††] (ITA) project has as consequence the development of the Policy Management Toolkit.[18] This toolkit was developed to perform a variety of management functions on sets of policies applicable to sensors, sensor platforms, and networks.[19] The developed policies regulate aspects including platform control, sensor and system control, sensor information access control and information flow protection. In this paper we focus on authorisation policies that regulate users-assets access control in the context of a coalition operation. Such policies should take into account several factors including user's partner membership, user's membership of cross-partner team and user's echelon and expertise. As far as the assets are concerned authorisation policies should take into account factors such as asset's partner ownership, asset's scarcity and intelligence capabilities. In addition, given that the scenarios that we are dealing with are time critical ones, CE-based rules must be able to consider and capture also spatio-temporal parameters in terms of asset sharing.

Thus, we develop different types of high-level access control rules using each time as building blocks different attributes of the concepts defined in the ontology of Figure 2. Attributes are sets of properties that are used in the ontology to describe concepts. Each rule consists of three grammatical blocks, a Subject, which is either a user or an asset (i.e. service), which wants to access an asset; an Object, which is an asset and an Action that the Subject wants to perform on the Object (i.e. can/cannot access). In order to test the expressive ability of CE as a policy language we develop policies for sharing different sets of assets (e.g. a specific asset to or all the assets owned by a specific partner) with different sets of users (e.g. a specific user or all the users who are members of a team) including those based on a traditional asset ownership model, and those defining team-based asset sharing across a coalition.

Suppose U is a user, A is an asset, P is a coalition partner, T is a team and C is the coalition and additionally the properties B as an asset capability, E which is a user expertise and the asset location C we have the predicates:

canAccess(U, A) == true if user U can access asset A
isAffiliated(U, P) == true if user U is affiliated with partner P
owns(P, A) == true if partner P owns asset A
member(U, T) == true if user U is member of team T OR
member(P, C) == true if partner P is member of coalition C
isRepresented(P, T) == true if partner P is represented in team T
capability(A, B) == true if asset A has B as capability
expertise(U, E) == true if user U has E as expertise
location(A, C) == true if asset A has C as location.

In order to help the readers to understand the developed rules we express each of them ("Rule 1" - "Rule 4") in three different ways: a plain text description, a formal definition rule using the above predicates and a CE-based representation. We start with simpler rules and we make them gradually more complex.

Rule 1
If User U is affiliated with partner P they can access the asset A, which is owned by partner P (i.e. traditional asset ownership model).

canAccess(U, A) **iff**
    isAffiliated(U, P) $\wedge$ *owns*(P, A)

[††] `https://www.usukitacs.com/`

```
if
  ( the asset A is owned by the partner P ) and
  ( the user U is affiliated with the partner P )
then
  ( the user U canAccess the asset A )
.
```

Rule 2
If User U is member of team T they can access asset A if it is owned by partners P and partner P is represented in team T (i.e. team-based asset sharing).

$\mathit{canAccess}(\mathrm{U}, \mathrm{A})$ **iff**

$\mathit{member}(\mathrm{U}, \mathrm{T}) \wedge \mathit{isRepresented}(\mathrm{P}, \mathrm{T}) \wedge \mathit{owns}(\mathrm{P}, \mathrm{A})$

```
if
  ( the user U is member of the team T ) and
  ( the partner P is represented in the team T ) and
  ( the partner P owns the asset A )
then
  ( the user U canAccess the asset A)
.
```

Rule 3
If User U has intel1 as expertise E can access asset A if asset A has detect as capability B.

$\mathit{canAccess}(\mathrm{U}, \mathrm{A})$ **iff**

$\mathit{expertise}(\mathrm{U}, \mathrm{E}) \wedge \mathit{capability}(\mathrm{A}, \mathrm{B})$

```
if
  ( the user U has the value EX as expertise ) and
  ( the value EX = ’intel1’ ) and
  ( the asset A has the value CP as capability ) and
  ( the value AP = ’detect’ )
then
  ( the user U canAccess the asset A )
.
```

The policy examples above show that CE is able to express authorisation policy rules based on different sets of conditions derived from concepts' properties and relationships. In particular, CE can express policies that regulate access control of all possible subsets of users to all possible subsets of assets considering each time different sets of attributes of the defined ontology; and this in a hierarchical independent manner. For example, assets owned by partner A can be accessed by users affiliated with partner B and not accessed by users affiliated with partner A. In essence the properties of the ontology's concepts are the factors which set the limits of CE's expressiveness as a policy language. The more the properties of the concepts the more complex access control rules one can build by combining them. In addition, CE can also express policies taking into account factors such as temporal and territorial variables as shown in "Rule 4".

Rule 4
If User U is member of team T can access asset A if asset A is owned by partners P and partner P is represented in team T and asset A is located in Kunar.

$\mathit{canAccess}(\mathrm{U}, \mathrm{A})$ **iff**

$\mathit{member}(\mathrm{U}, \mathrm{T}) \wedge \mathit{isRepresented}(\mathrm{P}, \mathrm{T}) \wedge \mathit{owns}(\mathrm{P}, \mathrm{A}) \wedge \mathit{location}(\mathrm{A}, \mathrm{C})$

```
if
  ( the user U is member of the team T ) and
  ( the partner P is represented in the team T ) and
  ( the partner P owns the asset A ) and
  ( the asset A has the value L as location ) and
  ( the value L = 'Kunar' )
then
  ( the user U canAccess the asset A)
.
```

In section 3 we mentioned that when a CE rule is executed, a rationale which is a set of reasoning steps, each of which is defined as a "because" relation between conditions and the rules decision is automatically created. Below we present the created rationale after executing a simple rule on our ontology.

Rule 5

```
if
  ( the asset A is owned by the partner 'US' ) and
  ( the user U has the value EX as expertise ) and
  ( the value EX = 'intel1' )
then
  ( the user U canAccess the asset A )
.
```

Rationale

```
the user 'u1'
canAccess  the asset 'a2'
because
the constant 'intel1' = 'intel1' and
the user 'u1' has 'intel1' as expertise and
the asset 'a2' is owned by the partner 'US'
```

It is worth noting that the policy grammar that we apply here for the development of policy rules is a very simple one. It can be easily extended according to the ontology and/or the system parameters that the CE-based policy language needs to control. One of the most important weaknesses of CE as a policy language is the absence of an inherent mechanism to cope with policy conflicts. A policy conflict occurs when two policies are applied simultaneously and their resulting actions contradict each other. As a consequence the subject implementing the policy cannot determine which action to perform.[20] Other well-known policy languages cope with this issue using for example precedence relationship to decide which one of the conflicting policies should first apply.[21,22] Currently CE users can cope with policy conflicts either by defining "metapolicies" (i.e. policies, which regulate other policies).

5. CONCLUSION & FUTURE WORK

In this paper we used a CNL named CE as a means to define a high-level policy representation, which is both human-friendly and directly processable by policy-checking systems. We claim that a high-level policy representation will help non-technical users operating near or at the edge of an organisation to create new and negotiate with existing policies. We first defined a CE-based ontology to capture the entities of a multi-partner coalition operation where ISR assets are owned by different parties and can be reserved for the exclusive usage of the owning partner or shared with different subsets of users affiliated to other partners. Then we developed and executed on the ontology a variety of authorisation attribute-based policy rules. We showed that the limits of expressiveness and flexibility of CE as a policy language are defined by the properties, which describe the concepts of the ontology.

A major aspect of policy-driven system's configuration is policy negotiation/relaxation when services are not implementable given the set of policies currently in force. A necessary prerequisite for a policy negotiation system is the creation of a mechanism for policy conflict detection. In terms of future work we plan to develop a mechanism for policy conflicts detection among policies expressed in CE. Moreover, we plan to integrate the CE-based policy language with other well-known policy enforcement models such as WPML through CE agents in order to test its effectiveness and efficiency in terms of usability and system performance.

ACKNOWLEDGMENTS

We thank Dave Braines and Christopher Gibson from IBM UK for their input and support in developing the CE-based policy representation, Jon Bakdash of the US Army Research Laboratory and Boleslaw Szymanski from Department of Computer Science, Rensselaer Polytechnic Institute for valuable discussions on the context for this work. This research was sponsored by the U.S.Army Research Laboratory and the U.K. Ministry of Defence and was accomplished under Agreement Number W911NF- 06-3-0001. The views and conclusions contained in this document are those of the author(s) and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defence or the U.K. Government. The U.S. and U.K. Governments are authorised to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

REFERENCES

1. J. Mahaffey and T. Skaar, "Observations on the dissemination of isr data employing network-enabled capabilities in the coalition environment," 2005.
2. S. Kraus and O. Shehory, "Coalition formation with uncertain heterogeneous information," 2003.
3. D. Alberts, R. Huber, and J. Moffat, "Nato nec c2 maturity model," *CCRP* , 2010.
4. D. Verma, T. Brown, and C. Ortega, "Management of coalition sensor networks," 2010.
5. R. Hayes and D. Alberts, "Power to the edge: Command and control in the information age," *CCRP* , 2003.
6. A. Simon and M. James, "The agile organization," *CCRP* , 2005.
7. D. Mott, "Summary of controlled english," *ITACS* , 2010.
8. R. Schwitter, "Controlled natural language as interface language to the semantic web," *Proceedings of the 2nd Indian International Conference on Artificial Intelligence, IICAI 2005* , pp. 1699–1718, 2005.
9. M. Tilbrook and R. Schwitter, "Controlled natural language meets the semantic web," in *Australasian Language Technology Workshop 2004*, **2**, 2004.
10. A. Bernstein and E. Kaufmann, "Gino - a guided input natural language ontology editor," 2006.
11. G. Hart, M. Johnson, and C. Dolbear, "Rabbit: Developing a control natural language for authoring ontologies," 2008.
12. T. Kuhn, "An evaluation framework for controlled natural languages," 2010.
13. T. Kuhn, "Acerules: Executing rules in controlled natural language," 2007.
14. A. Preece, D. Pizzocaro, D. Braines, and D. Mott, "Tasking and sharing sensing assets using controlled natural language," in *Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR III*, **SPIE Vol 8389**, 2012.
15. M. Gomez, A. Preece, M. Johnson, G. De Mel, W. Vasconcelos, C. Gibson, A. Bar-Noy, K. Borowiecki, T. La Porta, D. Pizzocaro, H. Rowaihy, G. Pearson, and T. Pham, "An ontology-centric approach to sensor-mission assignment," 2008.
16. P. Xue, D. Mott, D. Braines, S. Poteet, A. Kao, and C. Giammanco, "Information extraction using controlled english to support knowledge-sharing and decision-making," 2012.
17. D. Pizzocaro, A. Preece, F. Chen, T. La Porta, and A. Bar-Noy, "A distributed architecture for heterogeneous multi sensor-task allocation," 2011.
18. G. B. F. Pham, T. Pearson and S. Calo, "The ita sensor fabric and policy management toolkit," 2011.
19. G. Pham, T. Cirincione, "Sensor data and information sharing for coalition operations," 2012.

20. 3198 RFC, “Terminology for policy-based management,” *IETF Request for Comments 3198* , 2001.
21. E. C. Lupu and M. Sloman, “Conflicts in policy-based distributed systems management,” **25**(6), pp. 852–869, 1999.
22. D. Agrawal, J. Giles, K. W. Lee, and J. Lobo, “Policy ratification,” *6th IEEE International Workshop on Policies for Distributed Systems and Networks, POLICY 2005* **2005**, pp. 223–232.