

White Paper



Policy Based Management and NEC

A key enabler for Network Enabled Capability

Author	J Johnson
Date	5 July 2004
Reference	NET040502
Issue	2

Abstract



Policy Based Management (PBM) is a rules-driven approach that can be used to automate pre-configurable system management tasks. It is usually employed in a network management context, for activities such as network security configuration or Quality of Service provisioning.

TRT (UK) are exploring the use of PBM as a widely applicable technique for communication system management, particularly for controlling context- or mission- specific systems and enabling the rapid deployment and dynamic use of coalition infrastructures. Rules-based approaches have the potential to play a significant role in reducing the equipment required in deployments, reducing the number of skilled personnel required to manage them, ensuring configuration reliability, and in bringing decision support to man-machine interactions.

Demonstrator programs at TRT (UK) have shown that PBM techniques could be a key element in the delivery of Network Enabled Capability and have potential for future combat and operational systems and C4ISR applications. The evolution of PBM in the commercial arena makes it a potential candidate for off the shelf use in military deployments, and this paper introduces applicable work in exploiting commercial tools and approaches.

Keywords

PBM (Policy Based Management), Rules-driven approach, NEC (Network Enabled Capability), Network Infrastructure, System Management, C4ISR

Thales

Thales is a world leader in mission-critical information systems covering three major markets: Aerospace and Space, Defence, and Security. We are present all along the value chain, providing equipment and systems, systems integration, prime contracting and services. Thales meets the communications, information and security needs of people in countries throughout the world with operations in more than 50 countries and 68,000 employees worldwide.

Thales Research and Technology (UK) Limited

Thales UK's Reading-based research & technology facility is the UK arm of the Thales corporate research centre. Its activities focus on providing solutions: Security and Communication Systems, Galileo and Position-Based Systems, and Enhanced Digital Environments. These are based on the key technologies of IP Networks and Network Security, Wireless Communications, Sensors and Signal Processing, and Navigation and Positioning. The facility offers a wide range of consultancy and development services to European Government Agencies and to industry throughout the world.

Thales Research and Technology (UK) Limited
Worton Drive, Worton Grange
Reading, Berkshire, RG2 0SB, UK

Company Registration No. 774298

<mailto:scs.trtuk@thalesgroup.com>

Opportunities

C2 Convergence

Computing and Communications in the consumer world are changing. Mobility and geography are no longer barriers to computing power or connectivity to remote services, and users are growing ever more comfortable with and reliant on this mobile world. 'Anytime – anywhere' computing is upon us already, and is progressing rapidly. This convergence enables a large number of potential applications and opportunities, but also invalidates some of the traditional approaches to information presentation and protection.

The military parallel

Naturally, this convergence of computing and communications infrastructures has parallel application in realising the visions for NEC (Network Enabled Capability) and C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) applications of various types. The broadest network-enabled visions would see ad hoc multinational joint forces coalitions plus civil deployment groups, seamlessly and securely connected to each other as required, with machine support and information filtering to ensure that each person has exactly the right information, at the right time, to fulfil their role.

Right time. Right place. Right information.

Employing COTS solutions

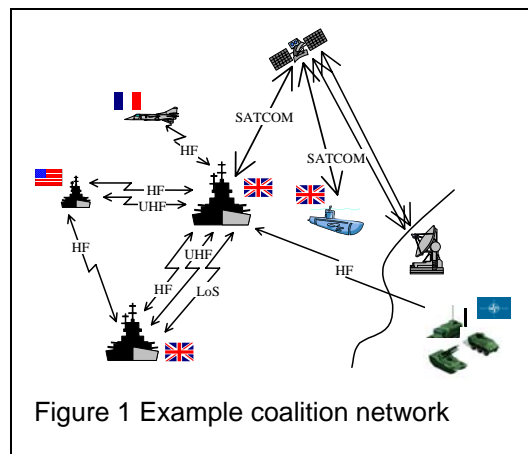
Increased implementation modularity (such as component-based approaches) brings many benefits to system architectures, including improved potential for the use of commercial-off-the-shelf (COTS) components. However, as systems become increasingly interconnected, and users increasingly mobile, 'system of systems' issues, such as scalability and interoperability, become crucial in realising the visions of commercial and military customers alike.

Business Drivers for Machine Support

Business reasons for delegating more tasks to the computing and communications infrastructure include: reducing equipment costs by employing re-configurable devices, reducing the amount of skilled management required by automating pre-defined configuration tasks, and improving response time and reliability by automating pre-defined reactions to detectable events. This gradual re-definition of man-machine interaction in decision support systems of various types also opens up opportunities for more advanced uses of the infrastructure, which may only be possible because of increased machine support.

Network challenges

Networks to support military operations can be characterised as similar to the naval example shown in Figure 1 - complex, dynamic networks, with multiple wireless communication links (such as line of sight radio or satellite relay) between otherwise autonomous groups and platforms. Particular challenges for this environment include the rationale that over-provisioning of bandwidth is unlikely to be possible, the characteristics and performance of the links will be changing as platforms and individuals move, and the structure is likely to be dynamic, having been constructed for a particular mission. These features make infrastructure management challenging and more sophisticated network management techniques will be needed to ensure the reliability and responsiveness required to support network-enabled features such as data sharing and fusion.



In addition, future networks are expected to feature even more network-enabled devices, and an even greater level of interconnection, between individuals, units, platforms, unmanned vehicles and sensors. This will demand yet more innovation in infrastructure management.

However, the infrastructures required to deliver Network Enabled Capability will actually need to meet many of the same challenges as those being explored in the consumer world. These include issues such as those shown below:

- How is identity determined and authenticated, and who is authorised to communicate with whom? Can this be managed at a group, organisational or national level as well as at an individual user level?
- How will limited communications resources, such as low bandwidth wireless links, be prioritised, allocated, and protected from attack or simply from over-subscription?
- How is a network rapidly set up, secured, and torn down again? This is particularly difficult when a high security level is required and when the parties have not communicated with each other before.
- How are such rapidly deployed networks integrated with any available or partially available fixed infrastructures?
- How is information filtered according to the current context or mission, to protect the operator or user from information overload? This issue exists in a multitude of domains, from distributed radar track fusion to location-based services such as building plans for emergency services. This is primarily an application issue, but computing and communications convergence raises questions such as whether information filtering should be related to available network bandwidth, particularly if that bandwidth is limited.
- What context information is public and what is privileged? Which individuals, organisations or states are entitled to share it? How is trust established, maintained, and revoked?

These considerations are indicative of the issues that need to be addressed to deliver the related visions of widely distributed systems, and machine support for managing and using them, and could apply to a wide range of battlespace applications, from sensor networks and combat management systems to logistics support.

Rules approaches

Benefits of Rules

The main tenet of rules-based approaches is to externalise the rules that drive a system, to separate them from both the hardware and the software that make up the system implementation. This 'late-binding' brings significant advantages whenever there is a need to make changes to those rules (for example, to suit a particular environment or mission, or to rapidly accommodate new requirements), or if there is a need to codify a pre-determined reaction to detectable conditions in the system.

As well as allowing the rules to be changed independently of the rest of the system, this separation also allows the rules to be expressed in a different language. What this means for systems of interest to Thales and its customers is that the rules no longer need to be written in a programming language, but can be expressed in natural language (e.g. English). Rules can therefore be created and edited by users skilled in the operational domain, rather than programmers or technical personnel.

PBNM

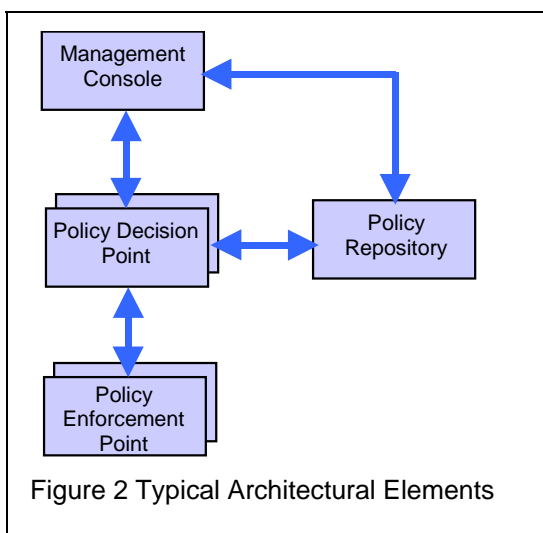
'Policy Based Network Management' (PBNM) has come to have many meanings, but is generally accepted to be a rules driven technique for managing network infrastructures. A 'policy' is a rule, of the general form if <conditions> then do <actions> that can be applied both to static device configuration and as an automatic response to dynamically changing conditions in the network.

IF <conditions> THEN DO <actions>

PBNM systems can automate actions that can be pre-defined, such as enabling access control for a set of users or allowing access to resources at certain times of day or under certain loading conditions. This can be used to reduce operator load and as a rapid response mechanism to allow a more dynamic utilisation of resources.

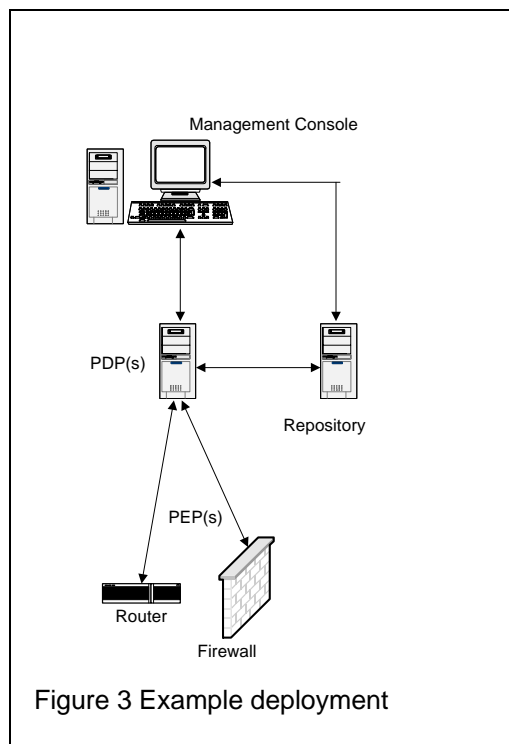
PBNM systems can also include refinement processes to turn high level specifications into low level commands, which can assist in abstracting the difficult task of network management and in allowing administrators to concentrate on *what* is required, not *how* it is achieved.

Usually, PBNM architectures include a console for creating rules and for controlling and monitoring their deployment, a repository for rules storage, 'policy decision points' for automatic decision-making according to detectable conditions (specified in the rules), and 'policy enforcement points' to enable any ensuing policy actions. Figure 2 illustrates this typical architecture, and Figure 3 shows a corresponding example deployment of those typical architecture elements for the control of a router and a firewall. Although not shown, it would also be necessary and usual to maintain an audit trail incorporating activities from each component.



There has been a substantial amount of academic and commercial research into policy management, for various types of devices and policies, and there are a number of activities aimed at standardising the protocols, programming interfaces, policy specification languages, models and schemas to

enable policy architectures. However, there is still no universally accepted approach, despite there being a large number of available commercial tools.



PBNM can be applied to the control of many network services. If the focus is on network security, a PBNM system can be used to configure firewalls, packet filters, access control, cryptographic parameters, and so on. If the focus is on quality of service provision or bandwidth management, then PBNM can be used to enable features such as priority queuing, differentiated services, and packet shaping. Other example applications include asset management, diagnostics, and monitoring systems.

It is possible to differentiate the underlying technologies from the policy based management of them, but in practice, PBNM can only enable the services that the underlying infrastructure can offer, so any use of PBNM needs to take account of that.

TRT (UK) Approaches

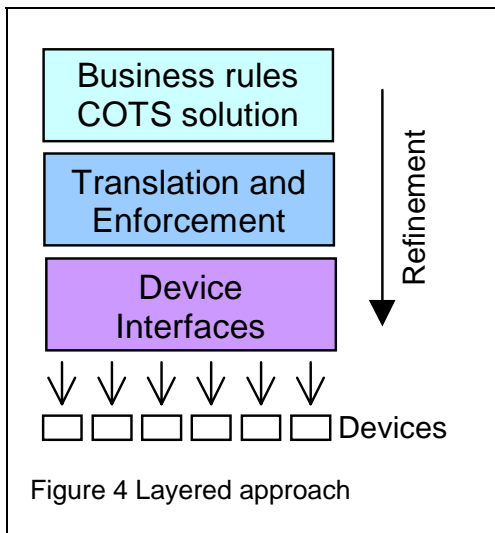
Researchers at TRT (UK) are taking a broad view of policy management as a technique, viewing it as an overlay to various technologies, applicable to systems as well as networks. Ideally, it will be driven from the highest level of abstraction –

business or operational goals, expressed in natural language.

Our work aims to take account of the difficult challenges being tackled by academic and industrial alliance groups (such as interoperability, sharing policies across different domains, resolving policy conflicts, etc.). In parallel, we consider developments in the commercial implementations of PBNM systems, although these tend to be less generic and focussed on specific domains, vendors or technologies. For network enabled capability, our work aims to allow doctrine and procedures to be expressed as rules, and for the system to provide a high level of machine support in converting these goals/rules into primitives that have meaning at the device level.

Unusually in the area of policy research, we employ a commercial rules engine for the creation and execution of the high level rules. The high level part of the architecture is therefore a COTS solution, with all the usual benefits of that, and the selected product allows rules to be written in natural language. The lowest level, at the device interface, is necessarily device manufacturer specific, and is driven from the infrastructure choices and the protocols and models required for the individual devices employed.

The emphasis of the research work is therefore concentrated on the rigorous, enforceable translation of the domain-centric goals to the device-centric infrastructure, including the associated data modelling (which defines the objects and actions allowed in the rules). Despite



the benefits of this framework (illustrated in Figure 4), there are still many challenges to be addressed.

It is important to offer high level, abstracted rules, in a language that a non-specialist can use, whilst maintaining sufficient rigour to ensure correct translation into suitable low level, device-specific commands and correct enforcement in the devices. This is a difficult challenge but research under way in a number of programmes could enable benefits for a wide range of applications.

Pilot Programs in Security

In close collaboration, TRT (UK) and Thales eSecurity Ltd have produced a number of demonstrator systems to illustrate the application of these techniques to the very important area of network security configuration. Three demonstrations are of note:

1. Large Scale Centralised Device Configuration.
 This demonstration shows the power of policy based management in the large scale. A single system can configure all of the secure connections required between a number of IP encryptors (Thales e-Security Datacryptor® 2000 IP, referred to hereafter as 'Datacryptors') according to attributes associated with each Datacryptor installation, such as nationality or security level. This is an alternative to individual configuration, which could be time-consuming and error-prone in the large scale. This pilot uses accredited Datacryptors and illustrates a technique that is valid when an individual lead party has administrative responsibility for a large domain.

2. Platform-centric device Configuration.
 This demonstration illustrates that a policy based management system could be employed to configure many devices within an administrative domain or on a single platform (e.g. a ship), in a collaborative arrangement, with other platforms doing the same. This pilot also uses accredited Datacryptors (as well as

other network devices) and illustrates a technique which is valid for collaboration between independent administrative domains, where each can retain control over its own resources.

3. Ad hoc secure coalition configuration.

This pilot shows an innovation in Datacryptor functionality combining web services with policy based management. Web services provide a mechanism for dynamic discovery of secure communications services, and PBM controls automated authorisation activities - acceptance or rejection of requests for services, or referral to a human operator for undefined relationships. An important feature of this pilot is the ability to rapidly configure secure communications between agencies who may be communicating with each other for the first time. This demonstration uses a modified Datacryptor and is part of the UK 2004 JWID (Joint Warrior Interoperability Demonstration) demonstration.

Concluding Remarks

Any policy or doctrine that can be precisely expressed and can be followed 'rote-fashion' by a person could (in theory) be implemented using a policy based system instead. Policy based management is therefore a widely applicable labour-saving technology.

PBM is well suited as a network management delegation technology to enable the transparent, flexible, reactive infrastructure that is required to deliver network-enabled capabilities, and could also be applicable more generally for system management.

However, the potential benefits of policy based management are still not fully realised in commercial implementations, and there is challenging research and advanced development still to do to create scalable, rigorous and interoperable solutions that fully exploit its potential.

Policy based management is most suitable where there is a dynamic need of some type. This could include a wireless or dynamic network infrastructure, a context-specific application, or system developments where it is useful to isolate some of the behaviour to allow it to be easily changed.

It is expected that future-looking battlespace developments will include these requirements.

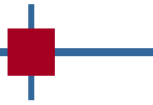
Related TRT (UK) work

Other research and advanced development activities at TRT (UK) include ad hoc networks, vision and surveillance architectures, predictive behaviour recognition, data mining, and data fusion. Combinations of these techniques have potential application to a number of areas, including combat management systems, operational planning tools, command and control systems, and network management.

Much of this research is conducted in close collaboration with Thales business units, and is aligned with future Thales group product offerings.

Further Information

- Networks@thalesgroup.com
- Internet Engineering Task Force (IETF) Policy Framework Working Group: <http://www.ietf.org/html.charters/policy-charter.html>
- Imperial College Policy Research Group Resources: <http://www-dse.doc.ic.ac.uk/Research/policies/resources.shtml>
- www.thalesgroup.com



THE INFORMATION IN THIS DOCUMENT IS SUPPLIED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ITS INFORMATION AND IN PARTICULAR WITHOUT ANY WARRANTY AS TO FITNESS OF SUCH INFORMATION FOR THE INTENDED PURPOSE.

THALES NOR ANY PERSON ACTING ON ITS BEHALF:-

- A) MAKES ANY WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, THAT THE USE OF THE INFORMATION IN THIS DOCUMENT MAY NOT INFRINGE THIRD PARTY RIGHTS;
- OR
- B) ASSUMES ANY LIABILITIES, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, WITH RESPECT TO THE USE OF, OR FOR DAMAGES RESULTING FROM THE USE OF ANY INFORMATION IN THIS DOCUMENT.

NO RIGHT OR LICENCE IS GRANTED TO THE RECIPIENT IN RELATION TO ANY INFORMATION IN THIS DOCUMENT.