

2 Levantamento de Requisitos

Os requisitos foram levantados a partir dos estudos de caso elaborados pela Petrobras sobre os incidentes com a P-36 e a P-34. Eles foram utilizados para identificar os papéis e atributos das pessoas envolvidas em uma operação típica de gestão de desastre. Também foram realizadas entrevistas para identificar procedimentos e expectativas dos usuários com relação ao espaço de trabalho colaborativo. Nesse tipo de ambiente, é importante modelar as relações entre os usuários e identificar as principais características da colaboração que os usuários gostariam de ter à sua disposição.

Uma vez completada a fase de levantamento dos requisitos dos usuários, o passo seguinte foi definir os requisitos técnicos em termos de modelos de colaboração, simulações, espaços de trabalho globais e personalizados, visões sincronizadas, reprodução de vídeos, etc. O espaço de trabalho colaborativo deve ter nós distribuídos com interfaces personalizadas que representem as várias perspectivas dos usuários.

Realizamos a seguir um estudo dos principais sistemas comerciais de gestão de emergências disponíveis, de modo a relacionar suas principais características e identificar os principais aspectos ainda desenvolvidos de maneira insuficiente.

2.1. A Evolução da Gestão de Desastres na Petrobras

A Petrobras enfrentou recentemente dois grandes incidentes (P-36 e P-34). Esta seção resume esses incidentes no intuito de ilustrar a complexidade do problema em termos dos processos e grupos de pessoas envolvidos nessas situações de desastre. A partir desta discussão, veremos que a Petrobras tem melhorado continuamente seu programa de gestão de desastres.

Durante o acidente com a P-36, houve uma explosão mecânica e uma explosão química com fatalidades, o que dificultou a execução de ações rápidas no sentido de salvar a unidade. Já no desastre com a P-34 não houve nenhuma

explosão, o que permitiu às equipes reagirem rapidamente, ainda que a comunicação entre os membros pudesse ter sido melhor. Esta pesquisa visa dar o próximo passo na evolução desse processo, no sentido de empregar ICT (*Information and Communication Technology* – Tecnologia de Informação e Comunicação) para aperfeiçoar a colaboração entre aqueles envolvidos em ações de contingência.

No caso da P-36, a Petrobras identificou a necessidade de atualizar os procedimentos de emergência e executar as ações em um espaço de tempo mais curto, de modo a poder salvar a unidade. Esse caso levantou a necessidade de se investigar modelos colaborativos e de tomada de decisão capazes de ajudar equipes complexas a evitar maiores desastres.

No caso da P-34, já havia um modelo atualizado da unidade *offshore* e uma forma de trabalho distribuído que ajudou a equipe de resgate a agir com rapidez. Havia também um simulador estático que permitiu aos especialistas executar diferentes simulações. Ainda assim, a equipe não dispunha de um ambiente adequado para trabalhar na forma de uma equipe virtual, de modo a compartilhar conhecimentos, discutir conjuntamente possíveis planos de resgate e chegar rapidamente a um consenso.

Conseqüentemente, foi necessário que as pessoas se reunissem no mesmo local físico, o que provocou algum atraso no processo. Além disso, algumas das informações não estavam diretamente disponíveis para aqueles responsáveis por tomar as decisões. Esse incidente demonstrou a necessidade de se fortalecer a colaboração entre as equipes distribuídas, oferecendo melhor interação, simulação e discussão ao longo de toda a operação de salvamento.

2.2. Requisitos

A partir da análise dos desastres descritos, observamos a necessidade de ir além e desenvolver um paradigma de reação a situações de emergência que deve garantir, como característica essencial, a colaboração entre todos os participantes de cada cenário de contingência. Idealmente, cada nó participante desse ambiente distribuído deve poder compartilhar e discutir seus resultados com outros

participantes, além de ter acesso a todos os dados de que precisa para suas tarefas de simulação.

Discutiremos agora a natureza distribuída das equipes e dos recursos que precisam ser congregados no paradigma proposto para o espaço de trabalho colaborativo.

2.2.1.

A Natureza Distribuída das Equipes

No caso particular da Petrobras, quando ocorre um acidente, a sede é imediatamente contatada e o Gerente Geral da unidade operacional fica responsável por gerenciar a crise. Todo o trabalho fica sob seu controle no espaço de trabalho decisório. O Departamento de Segurança, Meio Ambiente e Saúde inicia os procedimentos de emergência e, ao mesmo tempo, especialistas técnicos começam a agir. Esse espaço de trabalho técnico é constituído por engenheiros navais, engenheiros estruturais, analistas de *risers* e oceanógrafos. Quando eles trabalham juntos de forma colaborativa, em geral há os seguintes grupos distribuídos principais:

- uma equipe de alto nível com responsabilidade para tomar decisões na unidade operacional;
- um grupo de força-tarefa que coordena o processo de tomada de decisão:
 - na Unidade de Negócios (no Rio de Janeiro, para plataformas localizadas na Bacia de Campos) se a plataforma não foi seriamente prejudicada, com dois ou três operadores que permanecem dentro da unidade e realizam as operações necessárias; ou
 - em uma cidade que seja o local mais próximo do acidente em terra (Macaé, para as plataformas localizadas na Bacia de Campos), de onde os mergulhadores recebem orientações e realizam as únicas atividades possíveis quando a unidade está seriamente danificada ou tem problemas de segurança;
- uma equipe de suporte técnico na sede da empresa no Rio, na Unidade de Negócios e no centro de pesquisas;

- especialistas em trânsito, que podem estar em mar ou viajando e também precisam estar conectados.

Além desses grupos, e trabalhando em conjunto com eles, há equipes de segurança localizadas em unidades de resgate que se mobilizam rumo à região do acidente e oferecem assistência durante todo o tempo da crise.

2.2.2. A Natureza Distribuída dos Recursos

Não somente os especialistas, como também os recursos do sistema estão distribuídos nesse cenário:

- simuladores que requerem uso intenso de computadores precisam ser executados remotamente em um supercomputador ou em um aglomerado de computadores para obter resultados rápidos;
- o sistema computacional precisa ter acesso a bancos de dados remotos, que contêm modelos CAD e modelos de simulação da unidade;
- cada local envolvido na resolução da crise pode ter diferentes configurações, como um Centro de Realidade Virtual (RV), um computador *desktop* ligado à intranet e um *laptop* conectado à rede;
- os especialistas em trânsito podem se conectar por meio de tecnologias móveis;
- a conexão entre a unidade e as pessoas em terra pode variar. No melhor dos casos, a unidade é um dos nós da rede e, no pior, a comunicação entre os operadores somente pode ser feita por rádio ou telefone.

2.3. Sistemas Comerciais de Gestão de Emergências

Após determinar os requisitos do espaço de trabalho colaborativo para gestão de desastres, realizamos um estudo dos principais sistemas comerciais de gestão de emergências disponíveis, identificando suas características mais

importantes, as principais áreas abrangidas, os recursos de última geração e aqueles que ainda estão pouco desenvolvidos.

Durante a realização deste estudo, foram analisados os sistemas de gestão de emergências de alguns fabricantes além dos métodos de intervenção em caso de crise que estão sendo praticados em empresas como a Statoil, a Norsk Hydro, a Elf e a British Petroleum (BP). Os sistemas estudados estão resumidos nas próximas subseções.

2.3.1. Relatório de Comparação de Recursos do Departamento de Justiça dos EUA

O Departamento de Justiça dos Estados Unidos desenvolveu um Relatório de Comparação de Recursos (Hart, 2002) dos principais CIMS (*Crisis Information Management Software* – Software de Gestão de Informações sobre Crises) disponíveis comercialmente. Esse estudo produziu resultados importantes, dos quais listamos a seguir aqueles diretamente relacionados ao presente trabalho. O programa deve:

- permitir o acesso remoto de usuários autorizados localizados fora da LAN (*Local Area Network* – Rede de Área Local);
- estar de acordo com as normas e os padrões do ICS (*Incident Command System* – Sistema de Comando de Incidentes). O ICS é uma ferramenta para modelar comandos, controles e a coordenação de respostas, desenvolvida em torno de cinco atividades principais de gestão relativas a um incidente:
 - Comando;
 - Operações;
 - Planejamento;
 - Logística;
 - Finanças/administração;
- integrar outros sistemas, como de mapeamento, outros CIMS e sistemas de notificação telefônica;
- integrar o sistema de saúde pública à gestão de emergências;
- operar em uma variedade de configurações de redes;

- ter uma vasta gama de recursos consistentes com as quatro fases das operações de gestão de emergências: planejamento, mitigação, reação e recuperação.

O relatório também concluiu que não há um produto que seja o melhor ou que se adeqüe perfeitamente. O produto mais apropriado deve ser escolhido com base no orçamento, no ambiente de sistema, na dimensão da operação, na sofisticação da operação, na disciplina para sua implementação e em questões de ordem política.

2.3.2. L-3 CRISIS *Command and Control System*

Uma das maiores fabricantes de sistemas de emergência é a Ship Analytics, com a qual a Petrobras já começou a estabelecer uma relação comercial. Um de seus principais produtos é o L-3 CRISIS *Command and Control System* (Sistema de Comando e Controle de Crise) (MPRI Ship Analytics, 2003), um dos sistemas computacionais comerciais considerados como padrão. Ele auxilia os coordenadores das ações de contingência, funcionando como a espinha dorsal durante a resposta a desastres e como ferramenta educativa em treinamentos para situações de emergência. Ele traz ainda simulações computacionais que permitem avaliar respostas alternativas, um sistema de planejamento para gestão de riscos e mitigação de danos ambientais, e um sistema de contabilidade para administrar ativos alternativos. Oferece também às equipes de gestão de incidentes um GIS (*Geographic Information System* – Sistema de Informações Geográficas) e SOP (*Standard Operating Procedures* – Procedimentos Padrão de Operação) para facilitar a reação a diferentes tipos de desastres, como enchentes, vendavais, vazamento de gases tóxicos, etc.

Do ponto de vista prático, os coordenadores de emergências consideram útil elaborar listas de verificação a partir do SOP para cada posição funcional relacionada a eventos específicos. As listas de verificação são desenvolvidas de modo a serem fáceis de ler e de implementar, e o L-3 CRISIS oferece um meio de automatizar a função de lista de verificação.

Quando necessário, são empregados *firewalls* para proteger informações confidenciais, permitindo aos usuários terem acesso às informações necessárias para realizarem suas tarefas. O sistema foi projetado para utilizar informações de entrada a partir de diversos equipamentos de detecção em tempo real, como sensores infravermelhos, imagens de satélite e bóias detectoras de hidrocarbonetos. O sistema é compatível com a Web, incorporando um navegador que permite aos usuários acessarem as informações mais atualizadas disponíveis na Internet, na Intranet e nas próprias bases de dados do sistema.

2.3.3.

Oil Spill Crisis Management Simulator

Um dos simuladores baseados no L-3 CRISIS é o *Oil Spill Crisis Management Simulator* (Simulador de Gestão de Crises de Derramamento de Óleo). Ele auxilia em todas as etapas da gestão de incidentes, desde a prevenção/mitigação, passando pela preparação e até a reação e a remediação. O programa funciona como um centro de treinamento completo para Equipes de Gestão de Incidentes, Comandantes e Executores no Local, capacitando-os a resolver diversos incidentes por meio da simulação de exercícios, planos de reação, procedimentos operacionais e listas de verificação.

O SMS (*Spill Management Simulator* – Simulador de Gestão de Vazamentos) incorpora modelos padrão de derramamento de óleo e de mitigação. Os participantes do exercício interagem com o cenário utilizando os módulos de reação do L-3 CRISIS, o qual traz uma interface com bancos de dados relacionais complexos, um Sistema de Informações Geográficas (GIS) e modelos científicos de destino e trajetória de vazamentos.

O SMS oferece ainda um repositório central que contém informações cruciais para a administração eficiente da resposta a crises, como os locais e as especificações dos equipamentos de resposta disponíveis, o pessoal disponível e dados ambientais e econômicos essenciais. O componente de simulação do sistema, que modela o destino e a trajetória físicos do óleo derramado e rastreia as embarcações e as operações simuladas de reação, armazena os dados de saída no banco de dados central.

Para simular um exercício, são criados bancos de dados de especialistas e equipamentos específicos para cada cenário associando-se todos ou um subconjunto dos bancos de dados da Central de Recursos a um determinado cenário. Quando o exercício está em andamento, os instrutores/operadores podem modificar e/ou adicionar registros de recursos específicos daquele cenário sem afetar os bancos de dados da Central. Os dados de recursos são utilizados pela Equipe de Gestão de Incidentes ou pelos Participantes do Exercício para alocar e rastrear equipamentos e pessoal.

Os cenários de vazamentos são desenvolvidos ou modificados antes da realização de um exercício por meio de um recurso de definição de cenários.

2.3.4.

Systems Requirements Document (SRD) do Automated Resource Management System (ARMS) dos EUA

Outro documento importante que também foi estudado é de autoria da Booz Allen Hamilton (2003), a qual foi encarregada de auxiliar a Divisão de Preparo da FEMA (*Federal Emergency Management Agency* – Agência Federal de Gestão de Emergências) do governo dos Estados Unidos na elaboração de um documento com requisitos para o ARMS (*Automated Resource Management System* – Sistema Automatizado de Gestão de Recursos). O SRD (*Systems Requirements Document* – Documento de Requisitos de Sistema) do ARMS traz uma especificação de alto nível dos requisitos desse sistema, identificando e definindo os dados correspondentes, as normas empresariais e os requisitos funcionais, operacionais e técnicos para um site da Web destinado a auxiliar os governos estaduais e municipais a melhorar sua capacidade de assistência mútua durante situações de emergência.

O ARMS é definido como um “sistema automatizado que ajuda coordenadores de gestão de emergências a localizar recursos para melhorar sua resposta a emergências.” Entre seus recursos incluem-se pessoal, equipamentos e suprimentos. O ARMS é a faceta computadorizada da *National Mutual Aid and Resource Management Initiative* (Iniciativa Nacional de Ajuda Mútua e Gestão de Recursos) do governo dos EUA, e visa aperfeiçoar o processo de assistência mútua.

2.3.5. Análises do *Crisis Intervention and Operability* (CRIOP)

Outro documento importante que apresenta um método por meio de cenários para intervenções em crises e análises de operabilidade é o CRIOP (*Crisis Intervention and Operability* – Intervenção e Operabilidade em Crises) (Johnsen, 2004), elaborado em conjunto pela Scandpower, SINTEF, Statoil e NTNU, com ajuda da Norsk Hydro, Saga, Elf, NORSOK, BP, Safetec, DNV e Aker.

O CRIOP consiste de uma metodologia empregada para verificar e validar a capacidade de um centro de controle de lidar com segurança e eficiência com todos os modos de operação, incluindo iniciação, operação normal, manutenção e revisão, alterações no processo, situações críticas de segurança e finalização. Tal metodologia pode ser aplicada a salas de controle central, cabines de perfuração, guinchos e outros tipos de cabine, além de salas de controle *onshore*, *offshore* e de emergência.

Os elementos centrais do CRIOP são listas de verificação que abrangem áreas relevantes no projeto de Centros de Controle (CC), Análise de Cenário de alguns cenários chave e uma área de aprendizagem onde empregados de operações, projetistas e administradores podem se reunir e avaliar o melhor modelo de CC. As análises do CRIOP são iniciadas com uma fase de preparação e organização para identificar os participantes, coletar a documentação necessária, estabelecer grupos de análise e decidir quando a análise deve ser executada.

O método se concentra na interação entre as pessoas, a tecnologia e as organizações. Um dos princípios mais importantes do método CRIOP consiste em garantir que o foco permaneça nos fatores humanos importantes, no que diz respeito à operação e ao tratamento de situações anormais em centros de controle *offshore*, e em validar soluções e resultados.

2.3.6. Conclusões sobre os Sistemas de Emergência

Finalizando este levantamento sobre gestão de emergências, podemos observar que a maioria dos sistemas possui algumas características comuns, a saber:

- geralmente funcionam como ferramentas tanto de gestão de incidentes quanto de treinamento e planejamento;
- possuem grande capacidade de integração, não somente com bancos de dados e sistemas internos como também com sistemas públicos de gestão de emergências;
- geralmente têm uma arquitetura flexível em termos de integração com redes e software, integrando-se com um ou mais simuladores relacionados com o tipo de desastre que está sendo abordado;
- normalmente integram-se a um sistema gráfico, como um Sistema de Informações Geográficas (GIS), o qual é responsável por apresentar dados em tempo real do incidente em questão;
- são capazes de registrar e rastrear atividades e recursos, o que é importante não somente durante uma emergência real mas também como ferramenta para fins de treinamento;
- a maioria dos sistemas de emergência utiliza listas de verificação como um método eficiente e rápido para abordar os múltiplos requisitos simultâneos presentes em um cenário de emergência. A capacidade de oferecer meios de automatizar o máximo possível a função de lista de verificação pode ser um fator determinante na resolução rápida e segura de uma situação de emergência.

Apesar de todos os recursos listados acima, identificamos dois pontos negativos principais dos sistemas atuais de gestão de emergências:

1. Falta de integração adequada e completa dos simuladores com sistemas de visualização de alto desempenho;
2. Recursos de controle de acesso e segurança inadequados.

Este estudo demonstrou que, a despeito da integração que a maioria dos sistemas de gestão de emergências possui com simuladores, é preciso se desenvolver uma arquitetura de sistema capaz de suportar recursos distribuídos, particularmente simuladores distribuídos sendo executados em sistemas de visualização de *alto desempenho*. Tal arquitetura também deve fornecer comunicação síncrona entre diferentes equipamentos com co-localização virtual como uma de suas características.

A integração de simuladores com sistemas de visualização de alto desempenho em um ambiente distribuído sincronizado é o aspecto dos cenários de emergência no qual vamos nos concentrar. Como base para definir a arquitetura desse ambiente, foi elaborado um metamodelo. Desenvolvemos então um protótipo compatível com HLA como prova de conceito do metamodelo, tendo em conta que o HLA é um padrão para simulações de alto desempenho em tempo real.