

UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
ÁREA: CIÊNCIA DA COMPUTAÇÃO

**ESPECIFICAÇÃO DE UM SISTEMA MULTIAGENTE DE
RECOMENDAÇÃO DE AÇÕES EM CASO DE FALHAS
DE SISTEMAS DE AUTOMAÇÃO E CONTROLE
INDUSTRIAIS**

DISSERTAÇÃO DE MESTRADO

Aluno: Heider Cristian Moura Quintão

Orientadora: Prof^a. Dra. Rosário Girardi

São Luis, MA

Fevereiro de 2008

**ESPECIFICAÇÃO DE UM SISTEMA MULTIAGENTE DE
RECOMENDAÇÃO DE AÇÕES EM CASO DE FALHAS DE SISTEMAS DE
AUTOMAÇÃO E CONTROLE**

HEIDER CRISTIAN MOURA QUINTÃO

Dissertação de Mestrado apresentada à
Coordenação do Programa de Pós-
Graduação em Engenharia de
Eletricidade da Universidade Federal do
Maranhão como requisito parcial para a
obtenção do título de Mestre em
Engenharia de Eletricidade, na área de
Ciência da Computação.

Orientadora: Profa. Dra. Rosário Girardi

São Luis, MA
Fevereiro de 2008

Quintão, Heider Cristian Moura.

Especificação de um sistema multiagente de recomendação de ações em caso de falhas de sistema de automação e controle industriais / Heider Cristian Moura Quintão. – 2008.

154f.

Orientador: Rosario Girardi.

Impresso por computador (fotocópia).

Dissertação (Mestrado) – Universidade Federal do Maranhão, Programa de Pós-Graduação em Engenharia de Eletricidade , Área de concentração: Ciência da Computação , São Luís, 2008.

1.Sistemas multiagentes. 2. Automação industrial - falhas.
3. Ontologias. I. Girardi, Rosario. II. Título.

CDU 004.891

**ESPECIFICAÇÃO DE UM SISTEMA MULTIAGENTE DE
RECOMENDAÇÃO DE AÇÕES EM CASO DE FALHAS DE
SISTEMAS DE AUTOMAÇÃO E CONTROLE INDUSTRIAIS**

Heider Cristian Moura Quintão

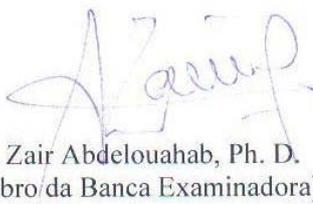
Dissertação aprovada em 15 de fevereiro de 2008.



Profa. Maria del Rosário Girardi, Ph. D.
(Orientadora)



Prof. Evandro de Barros Costa, Dr.
(Membro da Banca Examinadora)



Prof. Zair Abdelouahab, Ph. D.
(Membro da Banca Examinadora)

Aos meus pais e minha esposa.

AGRADECIMENTOS

Agradeço a todas as pessoas que de alguma forma me ajudaram a fazer dessa jornada uma fonte inestimável de aprendizado e experiências, que levarei comigo por toda vida:

A meus pais, Helton e Ana Maria, não só pelo carinho e exemplo de caráter, mas como também pelo incansável apoio e suporte que começou no jardim da infância, e continuou presente até minha colação de grau em engenharia e nos cursos de pós-graduação que fiz;

A Aline, minha esposa, pelo companheirismo, apoio e compreensão, principalmente nas minhas horas ausentes e nos momentos difíceis que passamos;

À Professora Rosário, por sempre ter mostrado com inabalável paciência a direção certa para continuar seguindo, mesmo quando eu insistia em ir para o lado contrário;

A toda Coordenação do Mestrado da UFMA, seus funcionários, professores e equipe do GESEC, pelos bons serviços oferecidos que foram fundamentais para a conclusão do mestrado;

Como o meu caminho no mestrado foi longo, agradeço também aos meus colegas e professores da UFMG, colegas de serviço da CVRD, UNICEUMA e também da ThyssenKrupp CSA, que sempre me apoiaram;

A meus amigos e amigas por compartilharem comigo da alegria desta conquista.

"Há um tempo em que é preciso abandonar as roupas usadas, que já tem a forma do nosso corpo, e esquecer os nossos caminhos, que nos levam sempre aos mesmos lugares. É o tempo da travessia: e, se não ousarmos fazê-la, teremos ficado, para sempre, à margem de nós mesmos."

Fernando Pessoa

RESUMO

Quando ocorrem falhas de equipamentos em plantas industriais complexas, o sistema de automação e controle gera uma grande quantidade de alarmes que podem confundir os operadores e induzi-los a tomar decisões erradas. O tempo para a tomada de decisão é muito curto e a quantidade de informação gerada é muito grande, sendo impossível que o operador consiga ler todas antes de tomar a decisão correta. Os novos sistemas industriais têm apresentado funcionalidades que buscam minimizar essa deficiência apresentando algum suporte ao usuário, mas ainda de forma ineficiente.

O presente trabalho apresenta como proposta um Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendação de Ações (SIGARA). É uma ferramenta baseada em conhecimento que objetiva suportar usuários de sistemas industriais de automação e controle, quando da ocorrência de alguma anomalia. O SIGARA é um sistema multiagente de recomendação de ações, modelado com base nas tarefas e fases descritas na ontologia ONTORMAS (*“Ontology for Reusing Multi-agent Software”*), conforme a metodologia MAAEM (*“Multi-Agent Application Engineering Methodology”*).

Além de buscar a solução de um problema do mundo real presente nas indústrias, o SIGARA proposto apresenta alguns diferenciais frente aos existentes no mercado, como o uso de técnicas de filtragem de informação em várias etapas do processamento das informações, e também a aplicação da MAAEM e ONTORMAS que ainda não haviam sido utilizadas nesse domínio.

Palavras Chaves: Gerenciamento de Alarmes, Gerenciamento de Condições Críticas, Engenharia de Software, Ontologias, Agentes, Sistemas Multiagentes, Sistemas de Recomendações.

ABSTRACT

When equipment failure occur in complex industrial plants, the automation and control system generates a great amount of alarms that can confuse the operators and lead them to take wrong decisions - the time for decision taking is very short and the amount of generated information is higher, being impossible for the operator read all of them before taking the correct decision. The new industrial systems have presented functionalities that try to minimize this deficiency presenting some support to the user, but still in an inefficient form.

This work presents a proposal of an Alarm Management System based on Action Recommendation - SIGARA, a knowledge-based tool which aims supporting users of industrial control systems, when abnormal events occur. SIGARA is an action recommender multi-agent system, shaped on the basis of the described tasks and phases of the ONTORMAS ontology and MAAEM methodology.

Beyond searching the solution of a problem of the real world in the industries, the proposed SIGARA presents some additional features not present on existing systems, as the application of information filtering techniques in different processing phases, and also the use of MAAEM and ONTORMAS in this new domain.

Keywords: Alarm Management System, Critical Conditions Management System, Software Engineering, Ontology, Agents, Multi-agent System, Recommender System.

SUMÁRIO

LISTA DE FIGURAS	12
LISTA DE TABELAS.....	14
LISTA DE EQUAÇÕES.....	15
ABREVIATURAS E SÍMBOLOS.....	16
1. INTRODUÇÃO.....	18
1.1 Motivação.....	18
1.2 Objetivos do Trabalho	19
1.2.1 Objetivo Geral.....	19
1.2.2 Objetivos Específicos	19
1.3 Organização da Dissertação	20
2. SISTEMAS DE INFORMAÇÃO APLICADOS À AUTOMAÇÃO INDUSTRIAL	22
2.1 Considerações Gerais sobre Sistemas de Automação Industrial	22
2.2 Exemplo de um Sistema de Automação Industrial	25
2.2.1 O Equipamento Virador de Vagões do TPPM.....	25
2.2.2 A automação do Virador de Vagões	27
2.3 Sistema Informatizado de Gerenciamento e Recomendação de Alarmes.....	30
2.3.1 Institutos de Pesquisa e de Desenvolvimento de Sistemas Informatizados de Gerenciamento de Alarmes e Sistemas de Automação	31
2.3.2 Sistemas Industriais de Gerenciamento de Alarmes.....	35
2.3.3 Sistemas de Gerenciamento de Condições Críticas	39
2.3.4 Empresas de Desenvolvimento de Sistemas Informatizados de Gerenciamento de Alarmes e Estudos de Casos	43
2.4 Considerações Finais	58
3. .PRINCIPAIS TÉCNICAS DE FILTRAGEM E RECOMENDAÇÃO	61
3.1 Métodos de Clusterização	61
3.1.1 Medição de Similaridade	64
3.2 Principais Técnicas de Filtragem e Recomendação.....	68
3.2.1 Filtragem e Recomendação Baseada em Conteúdo.....	69
3.2.2 Filtragem e Recomendação Colaborativa.....	71
3.3 Discussão da Aplicação de Clusterização e Filtragem em Grupos de Usuários.....	72
3.3.1 Estudo de Caso usando Filtragem Baseada em Conteúdo	73

3.3.2	Considerações sobre Técnicas de Filtragem e Recomendação Clássicas	78
3.4	Considerações Finais	79
4.	SISTEMAS MULTIAGENTES.....	81
4.1	Introdução a Sistemas Multiagente	81
4.1.1	Ontologias.....	81
4.1.2	Agentes	83
4.1.3	Sistemas Multiagentes	86
4.2	Metodologias e Ontologias para Sistemas Multiagente	87
4.2.1	A Metodologia MAAEM.....	88
4.2.2	A Ontologia ONTORMAS.....	91
4.3	Considerações Finais	93
5.	MODELAGEM E PROTOTIPAÇÃO DO SIGARA	95
5.1	Modelagem de Conceitos.....	97
5.2	Modelagem de Objetivos	101
5.3	Modelagem de Papéis	106
5.3.1	Modelo de Papéis - Modelagem e Classificação dos Usuários.....	107
5.3.2	Modelo de Papéis – Filtragem Baseada em Conteúdo.....	109
5.3.3	Modelo de Papéis – Avaliação dos Alarmes	111
5.3.4	Modelo de Papéis – Identificação da Causa do Alarme	113
5.4	Modelagem das Interações entre os Papéis	114
5.4.1	Modelo de interação entre os papéis da modelagem e classificação dos usuários.....	115
5.4.2	Modelo de interação entre papéis da filtragem baseada em conteúdo.....	116
5.4.3	Modelo de interação entre os papéis da avaliação dos alarmes	117
5.4.4	Modelo de interação entre papéis da identificação da causa do alarme	118
5.5	Prototipação da Interface do Usuário	119
5.5.1	Considerações Gerais sobre o Protótipo	119
5.5.2	Telas de cadastro da aplicação	121
5.5.3	Telas de seleção dos métodos da aplicação	131
5.5.4	Telas de consulta dos registros do SIGARA	133
5.5.5	Interface do SIGARA para seleção do modo de Exibição	136
5.6	Considerações Finais sobre a Análise e Especificação da Aplicação	141
6.	CONCLUSÃO DO TRABALHO.....	143
6.1	Resultados e Contribuições	144

6.2	Perspectivas Futuras.....	145
7.	REFERÊNCIAS BIBLIOGRÁFICAS.....	147

LISTA DE FIGURAS

Figura 1 – Foto do Virador de Vagões 01 da Vale em São Luis, em operação em Setembro de 2005.	25
Figura 2 – Tela sinóptica do Sistema de Supervisão e Controle dos Viradores de Vagões do TPPM da Vale em São Luis.	26
Figura 3 – Estrutura Simplificada de Automação e Controle do TPPM.....	28
Figura 4 – Leiaute do porto TPPM, referente ao plano diretor para produção de 85 milhões de toneladas/ano.....	30
Figura 5 – EEMUA – Mapa de Recomendações de Ações para o Operador quando da ocorrência de Eventos Pendentes ou Anormais.....	32
Figura 6 – EEMUA – Um alarme efetivo deve estar no ponto onde o operador deve tomar a ação [9]	33
Figura 7 – Camadas de Proteção de um SIGA em uma Planta Industrial Automatizada.....	40
Figura 8 – Funções Necessárias para o Gerenciamento de Condições Críticas - CCM.....	41
Figura 9 – Média de perdas em Milhões de Dólares causados pelos Maiores Acidentes Industriais.....	43
Figura 10 – Alarmes indesejados gerados de maneira repetitiva toda vez que ultrapassa limites.....	45
Figura 11 – Alarmes indesejados bloqueados com sistema oscilando por um grande tempo sem aviso ao operador.	45
Figura 12 – Comparação dos alarmes gerados com e sem o IMAS em operação.	47
Figura 13 – Estrutura lógica do <i>Toolkit</i> da <i>Control Art</i>	50
Figura 14 – Interface gráfica do software <i>AlarmAnalysis</i> do <i>Toolkit</i> da <i>Control Art</i>	51
Figura 15 – Interface gráfica do software <i>ManagerMain</i> do <i>Toolkit</i> da <i>Control Art</i>	52
Figura 16 – Interface gráfica do software <i>ManagerModify</i> do <i>Toolkit</i> da <i>Control Art</i>	53
Figura 17 – Interface gráfica do software <i>AssistantMain</i> do <i>Toolkit</i> da <i>Control Art</i>	54
Figura 18 – Modelo de um Sistema de Suporte a Decisões para Intervenção em Operações Anormais adotado pelo ASM.....	56
Figura 19 – Papéis Funcionais do AEGIS.....	57
Figura 20 – A correlação entre a Excelência Operacional e o Gerenciamento de Alarmes.....	59
Figura 21 – Clusterização de dados.	62
Figura 22 – Representação dos Documentos e Consultas por Vetores de Pesos.....	66
Figura 23 – Aplicação prática das Técnicas de Clusterização e Filtragem Baseada em Conteúdo... ..	74
Figura 24 – As interações de um agente genérico com seu ambiente.....	84
Figura 25 – A estrutura genérica de um agente.	84
Figura 26 – Exemplo de tela da ONTORMAS desenvolvido no <i>Protégé</i>	93
Figura 27 - Sistemas propostos inicialmente para o SIGARA, conforme objetivos específicos.....	96
Figura 28 – Modelo de Conceitos do SIGARA.....	101
Figura 29 – Objetivo Geral e Objetivos Específicos do SIGARA.....	103
Figura 30 – Modelo de Objetivos do SIGARA.....	105
Figura 31 – Modelo de Papéis do SIGARA - Modelagem e Classificação dos Usuários.....	109
Figura 32 – Modelo de Papéis do SIGARA - Filtragem Baseada em Conteúdo.....	111
Figura 33 – Modelo de Papéis do SIGARA – Avaliação dos Alarmes.....	112
Figura 34 – Modelo de Papéis do SIGARA – Identificação da Causa do Alarme.....	114
Figura 35 – Modelo de Interação entre Papéis – Modelagem e Classificação dos Usuários.....	115
Figura 36 – Modelo de Interação entre Papéis – Filtragem baseada em Conteúdo.....	117

Figura 37 – Modelo de Interação entre Papéis – Avaliação dos Alarmes	118
Figura 38 – Modelo de Interação entre Papéis – Identificação das causas do Alarme	119
Figura 39 – Tela do aplicativo NetBeans IDE 5.5.1 utilizado para desenvolvimento do protótipo da WebSIGARA	120
Figura 40 – Tela inicial de autenticação do usuário.....	122
Figura 41 – Tela com a lista das funções principais para usuário Operador	123
Figura 42 – Tela com lista das funções principais para o usuário Analista.....	124
Figura 43 – Tela com as Funções de Cadastro do usuário Analista	125
Figura 44 – Tela de Cadastro das Áreas de Responsabilidades.....	126
Figura 45 – Tela de Cadastro do Usuário em função da área de responsabilidade.....	127
Figura 46 – Tela de Cadastro de Anomalia Crítica.....	128
Figura 47 – Tela de Cadastro das Causas das Anomalias Críticas	129
Figura 48 – Tela de Cadastro das Informações e Conhecimento do Sistema.....	130
Figura 49 – Tela de Cadastro dos Arquivos de Registro	131
Figura 50 – Tela com as Funções de seleção dos métodos e algoritmos do SIGARA.....	132
Figura 51 – Tela de seleção dos Métodos para Análise de Similaridade.....	133
Figura 52 – Tela com as Função de consulta de todos os dados do SIGARA.....	134
Figura 53 – Tela de consulta do registro de alarmes e condições críticas, com a opção da apresentação gráfica da possível causa	135
Figura 54 – Tela de consulta do registro de ações recomendadas para as anomalias críticas	136
Figura 55 – Tela com a Seleção dos modos de exibição do SIGARA.....	137
Figura 56 – Tela do sistema de automação e controle industrial, com o modo de exibição ÍCONE do SIGARA.....	138
Figura 57 – Tela do sistema de automação e controle industrial, como modo de exibição BANNER do SIGARA.....	139
Figura 58 – Tela do sistema de automação e controle industrial, como modo de exibição BANNER do SIGARA, exibindo possíveis causas através do Diagrama de Ishikawa	140
Figura 59 – Tela do sistema de automação e controle industrial, como modo de exibição BANNER do SIGARA, exibindo possíveis causas através do FTA.....	141

LISTA DE TABELAS

Tabela 1 – EEMUA – Critério de ocorrência de Alarmes para Condições Normais de Operação em Sistemas de Automação Industrial.....	32
Tabela 2 – Comparação entre as Funções de um Sistema de Controle com um CCM.....	42
Tabela 3 – Configurações e Funções que devem estar presentes em um SIGARA.....	60
Tabela 4 – Tipos de Filtragem e suas principais características	73
Tabela 5 – Vetor de Pesos da Consulta.....	75
Tabela 6 – Trecho do Repositório de Dados.....	75
Tabela 7 – Vetor de Pesos do Documento	76
Tabela 8 – Vetor de Pesos da Consulta Q1	76
Tabela 9 – Vetor de Pesos do Documento D1	76
Tabela 10 - Conceitos de Modelagem da metodologia MAAEM	90
Tabela 11 - Fases, Tarefas e Produtos da MAAEM	92

LISTA DE EQUAÇÕES

Equação 1 – Distância Euclidiana.....	65
Equação 2 - Métrica Minkowski.....	65
Equação 3 – Distância Quadrada de Mahalanobis.....	65
Equação 4 - Fórmula de Similaridade Produto Interno.....	67
Equação 5 - Fórmula de Similaridade do Cosseno	68

ABREVIATURAS E SÍMBOLOS

AEGIS - Abnormal Event Guidance and Information System

AI - Inteligência Artificial

AMO-Rt - Alarm Management Optimization – Real-Time

ASM - The Abnormal Situation Management

ATP - Advanced Technology Program

CCO – Centro de Controle Operacional

CCM - Critical Condition Management

CLP's - Controladores Lógicos Programáveis

DCS - Discrete Control System

DDC - Digital Direct Control,

EEMUA - The British Engineering Equipment and Materials Users Association

FTA – Fault Tree Analysis

GESEC - Grupo de Pesquisa em Engenharia de Software e Engenharia do Conhecimento

HSE - The British Health & Safety Executive

IAMS - Sistema Inteligente de Gerenciamento de Alarmes

IEC - International Electro technical Commission

IHM's - Interface Homem Máquina

ISA -The Instrumentation, Systems, and Automation Society

MAAEM - Multi-Agent Application Engineering Methodology

MADEM - Multi-Agent Domain Engineering Methodology

NIST - U.S. National Institute of Standards and Technology

ONTORMAS - Ontology for Reusing Multi-agent Software

OSHA - Occupational Safety and Health Administration,

PAS - Process Automation Systems

PIMS - Plant Information Management System

ProSys - Process Systems Consultants

PSM - Process Safety Management,

ROCK - Robust Clustering using linkS.

SCADA - Supervisory Control and Data Acquisition,

SDCD's - Sistema Distribuído de Controle Digital

SIS - Safety Instrumented Systems

SIGA - Sistema Informatizado para Gerenciamento de Alarmes

SIGARA - Sistema Informatizado para Gerenciamento de Alarmes baseado na Recomendação de Ações

SOQA - SIRUP Ontology Query API

SMA - Sistema Multiagente

STING - STatistical INformation Grid-based method

TPPM - Terminal Portuário de Ponta da Madeira de São Luis-MA

1. INTRODUÇÃO

1.1 Motivação

Os sistemas automatizados de supervisão e controle utilizados em grandes complexos industriais são os responsáveis finais pelo desempenho da produção de todo o complexo. Desde 2000, não só o Brasil mas todo o mundo tem sido influenciado pelo milagre econômico Chinês, milagre esse que tem demandado grande volume de matérias primas, principalmente minério de ferro, gusa e placas de aço. O crescimento da demanda tem sido superior a 20% ao ano, ritmo esse superior ao incremento de produção que todas as empresas têm buscado. Assim, por maiores que sejam esses investimentos, a oferta desses bens continuará abaixo da demanda.

Uma forma de buscar aumento de produção, além do investimento em expansões e novos equipamentos, é a otimização dos ativos existentes. Entende-se por otimização dos ativos a busca pela excelência operacional, melhorando os sistemas produtivos existentes de modo a produzirem mais, com mais qualidade, mais regularidade, investindo em automação dos processos e treinamento das equipes. Dentro desse pacote de melhorias, têm-se os sistemas de recomendação, importante ferramenta no auxílio aos operadores e especialistas, ajudando tanto a reduzir o tempo de solução das falhas como meios para prevenir sua ocorrência.

Os sistemas de automação industrial atuais são operacionalmente eficientes, mas não ajudam os usuários a tomar decisões em caso de falhas [1]. Quando ocorrem falhas de equipamento, o sistema gera uma grande quantidade de eventos e alarmes que podem confundir os operadores e induzi-los a tomar decisões erradas – o tempo para tomada de decisão é muito curto e a quantidade de informação gerada é muito grande, sendo impossível que o operador consiga ler todas antes de tomar a decisão.

Por isso é de particular interesse a construção e operacionalização de um sistema que receba todos os eventos e alarmes gerado pelo sistema de automação industrial, realize uma filtragem baseada em conteúdo e, baseado no perfil dos usuários (manutenção e operação, por exemplo) e do conhecimento adquirido do sistema (armazenado em uma árvore de decisões, por exemplo), recomende as melhores ações.

O tema escolhido e proposto para buscar a solução desse problema presente nas indústrias é o objetivo principal dessa Dissertação de Mestrado: “Especificação de um Sistema Multiagente de Recomendação de Ações em caso de Falhas de Sistemas de Automação e Controle Industriais”. Irá consistir do estudo e modelagem de três sistemas, sendo um responsável por adquirir as informações, outro que irá explicitamente definir o perfil dos usuários e finalmente um que irá filtrar as informações realizando recomendações baseadas em conteúdo.

1.2 Objetivos do Trabalho

1.2.1 Objetivo Geral

O objetivo geral do presente trabalho é analisar e modelar um sistema multiagente de recomendações de ações com base nas fases e tarefas descritas na ontologia ONTORMAS, conforme a metodologia MAAEM, utilizando técnicas de filtragem de informações baseada em conteúdo. O sistema irá tratar alarmes e eventos provenientes do sistema de automação e controle industrial, apresentando apenas os alarmes mais críticos e relevantes, e para esses recomendar ações distintas para os vários usuários do sistema, como as equipes de operação e manutenção.

1.2.2 Objetivos Específicos

No sentido de alcançar o objetivo geral pretendido, buscar-se-á atingir os seguintes objetivos específicos:

- Capturar e especificar os requisitos de um subsistema para adquirir explicitamente as áreas de responsabilidade e o perfil dos usuários;
- Capturar e especificar os requisitos de um subsistema para adquirir e filtrar as informações provenientes do sistema de automação industrial, identificando os alarmes mais críticos e relevantes;

- Capturar e especificar os requisitos de um subsistema para armazenar o conhecimento do sistema de automação industrial, que permita recomendar ações aos usuários referentes aos alarmes mais críticos e relevantes;
- Aplicar as técnicas, metodologias e ferramentas desenvolvidas pelo grupo GESEC no detalhamento e desenvolvimento do trabalho, em particular, a ferramenta ONTORMAS (*“Ontology for Reusing Multi-agent Software”*) e a metodologia MAAEM (*“Multi-Agent Application Engineering Methodology”*).

1.3 Organização da Dissertação

A estrutura dessa dissertação compreende seis capítulos, sendo eles, além desta introdução, os seguintes.

No Capítulo 2 apresenta-se o estado da arte dos sistemas de informação aplicados à automação industrial, sistemas de controle e automação industrial, sistemas de gerenciamento de alarmes e de condições críticas. Para um melhor entendimento, apresenta-se também um exemplo real de sistema de automação industrial, bem como exemplos de aplicações de sistemas de gerenciamento de alarmes que foram pesquisados. Com essa pesquisa todos esses sistemas são devidamente identificados e seus principais conceitos detalhados, de modo que possam servir de referência para o desenvolvimento da nossa aplicação.

No Capítulo 3 descrevem-se os principais conceitos e técnicas da área de filtragem e recomendação de informações. São também desenvolvidos alguns estudos de casos para demonstrar melhor o desempenho das técnicas apresentadas e permitir um melhor discernimento quando da escolha das técnicas a serem utilizadas no SIGARA.

No Capítulo 4 apresenta-se a metodologia e as ferramentas que serão utilizadas no desenvolvimento do SIGARA, respectivamente, a MAAEM e a ONTORMAS.

No Capítulo 5 especifica-se a modelagem e prototipação do SIGARA conforme a ontologia ONTORMAS e a metodologia MAAEM apresentadas no Capítulo 4. Para essa modelagem, utilizam-se ainda os conceitos de sistemas de gerenciamento de alarmes e condições críticas apresentados no Capítulo 2 e as técnicas de filtragem e recomendação no Capítulo 3.

No Capítulo 6 apresentam-se os resultados obtidos, avaliando-se tanto a especificação do SIGARA, bem como a metodologia utilizada nesse desenvolvimento. Apresentam-se também propostas para novos trabalhos, visto que os produtos obtidos permitem refinamentos e o seu posterior reuso para outros domínios.

2. SISTEMAS DE INFORMAÇÃO APLICADOS À AUTOMAÇÃO INDUSTRIAL

2.1 Considerações Gerais sobre Sistemas de Automação Industrial

Automação é a substituição do trabalho humano ou animal por máquina. Automação é a operação de uma máquina ou de um sistema automaticamente ou por controle remoto, com a mínima interferência do operador humano. Automação é o controle de processos automáticos. Automático significa ter um mecanismo de atuação própria, que faça uma ação requerida em tempo determinado ou em resposta a certas condições [2].

O conceito de automação é muito vasto, e varia com o ambiente, cultura e experiência da pessoa envolvida. Para exemplificar, citam-se alguns exemplos de automação:

- Nas residências, para uma dona de casa, a máquina de lavar roupa é automática;
- Na indústria automobilística, para o empregado pode ser um robô;
- Em um shopping Center, para uma pessoa comum, pode ser o caixa eletrônico.

A partir desses exemplos, tem-se que o conceito de automação inclui a idéia de usar a potência elétrica ou mecânica para acionar algum tipo de máquina. Deve-se acrescentar à máquina algum tipo de inteligência, através de procedimentos ou programas, para que ela execute sua tarefa, tarefa essa pré-definida, de modo mais eficiente e com vantagens econômicas e de segurança.

Antes da definição atual de automação de sistemas, usava-se o termo controle automático de processo. Nessa época utilizava-se instrumentos com as funções de medir, transmitir, comparar e atuar no processo, para se conseguir um produto desejado com pequena ou nenhuma ajuda humana. A isto se denomina controle automático clássico.

Com a evolução das atividades industriais, ocorreu um aumento da complexidade dos processos, tamanho das plantas, exigências de produtividade, segurança e proteção do meio ambiente, além do controle automático do processo, aparecendo a necessidade de se monitorar o controle automático. A partir deste novo nível de instrumentos, com funções de monitoração, alarme e intertravamento, é que apareceu o termo sistema de automação. As funções predominantes neste nível são as de detecção, comparação, alarme e atuação lógica.

Os sistemas de automação industrial são sistemas de informação dedicados, que funcionam no chão de fábrica de uma empresa, com a responsabilidade de coletar informações de produção e do processo produtivo para fins de análises, além de controlarem e supervisionarem os equipamentos de produção. O termo chão de fábrica refere-se a todos os elementos que compõem o ambiente em volta dos equipamentos, ou seja, aspectos ligados diretamente à produção, tais como: os equipamentos, os operadores, os computadores que controlam as máquinas, etc.

Além dessas funções citadas, os sistemas de automação em alguns casos provêm o ajuste otimizado de um equipamento, o que equivale dizer que estes sistemas enviam informações para que esse equipamento possa produzir o material e/ou controlar algum processo. Ajuste é toda a preparação que o equipamento deve ter a fim de processar um material ou realizar alguma atividade.

De um modo geral, independentemente do mercado de atuação, as empresas estão investindo muito em sistemas de automação, indo desde sistemas para exames laboratoriais até sistemas para controle de grandes plantas industriais.

Principais Vantagens do Sistema de Automação [3]:

- Redução da intervenção humana: com os dados de configuração (ajuste/setup) chegando automaticamente diminui-se a interferência do operador no equipamento;
- Aumento da produtividade e eficiência: como toda a configuração do equipamento é feita mediante dados automáticos, há um ganho direto na produtividade e na eficiência, pois os erros são minimizados;
- Redução de papel: como todas as informações estão disponíveis em computadores ligados aos sistemas mencionados, os volumes de papel diminuem consideravelmente;
- Informações em tempo real: em outras palavras, a informação está disponível instantaneamente após um processo. Como exemplo poderia ser citado o fato de que, após a confirmação da colocação de um novo pedido para a fabricação de um produto, estas informações são enviadas diretamente para o equipamento, estando, assim disponíveis para o mesmo;

- Redução de custos: possibilidade de redução de operadores, uma vez que muitas das tarefas antes desempenhadas pelos mesmos foram automatizadas bem como redução de desperdício de matéria prima e de tempo ocioso dos equipamentos;
- Melhoria na qualidade: aumenta a confiabilidade das informações geradas no decorrer do processo, auxiliando também na qualidade dos produtos produzidos via o aprimoramento dos dados que irão configurar os equipamentos. Sistemas automatizados garantem um grau de repetibilidade maior, melhorando o controle de qualidade – obtêm-se menos desvios na produção;
- Criação de oportunidades: com a eliminação de alguns operadores (que realizavam atividades repetitivas e que pouco agregava à sua formação), há a oportunidade para que os operadores remanescentes se preocupem com outras questões importantes como a qualidade do produto.

Principais Desvantagens [3]:

- Dependência tecnológica: todo o processo produtivo depende do funcionamento dos sistemas, podendo causar prejuízos no caso de ocorrer uma parada inesperada do sistema;
- Acidentes: toda a automatização pode levar a um aumento de velocidade das tarefas que estão sendo corretamente realizadas, como também, acelerar e ampliar a ocorrência de problemas; ou pior, ocasionar acidentes devido a uma informação errada, por exemplo, um erro em “setup” (valores de ajuste do equipamento);
- Alto custo: como existe muita tecnologia envolvida, os valores a serem investidos inicialmente são altos. Deve-se fazer um estudo de viabilidade econômica para se avaliar as vantagens da automação em todos os casos.

A automação é um habilitador e uma alavanca para se obter produtividade em uma planta industrial. Em geral, em uma planta industrial, 75% dos ativos de produção estão sob influência do controle de processos.

Por outro lado, a própria automação muitas vezes é ela própria uma das causas das paradas de uma planta industrial. Os ativos de automação devem ter uma disponibilidade cerca de dez vezes maior que a dos ativos que ela controla [4]. Isto nem sempre acontece. Falhas humanas referentes à automação também constituem uma importante

causa de paradas e, portanto não se pode desvincular o fator humano do componente tecnológico.

Dentre os sistemas de informação dedicados que compõem o sistema de automação industrial, tem-se o sistema de diagnóstico, que faz parte do sistema supervisor na sala de controle, e deve ser capaz de indicar a causa da parada instantaneamente sem a necessidade de varrer e interpretar uma lista de alarmes.

2.2 Exemplo de um Sistema de Automação Industrial

2.2.1 O Equipamento Virador de Vagões do TPPM

O TPPM (terminal portuário de ponta da madeira de São Luis - MA, pertencente à Vale) tem uma instalação completa para recebimento de minério (viradores de vagões), manuseio (correias transportadoras, máquinas de empilhamento e recuperação de minério), classificação (planta industrial de peneiramento) e despacho (carregadores de navio), além de toda infra-estrutura necessária para garantir o perfeito funcionamento dos equipamentos acima.



Figura 1 – Foto do Virador de Vagões 01 da Vale em São Luis, em operação em Setembro de 2005.

Os viradores de vagões são equipamentos de grande porte, de forma tubular, que recebem simultaneamente dois vagões de minério de ferro, e realizam as suas viradas – giram em torno de um eixo central, conforme Figura 1 descarregando o minério em uma moega (estrutura metálica colocada logo abaixo do virador, que recebe o material), que irá coletar e encaminhar esse minério para as correias transportadoras e dessas para o pátio de estocagem, conforme Figura 2.

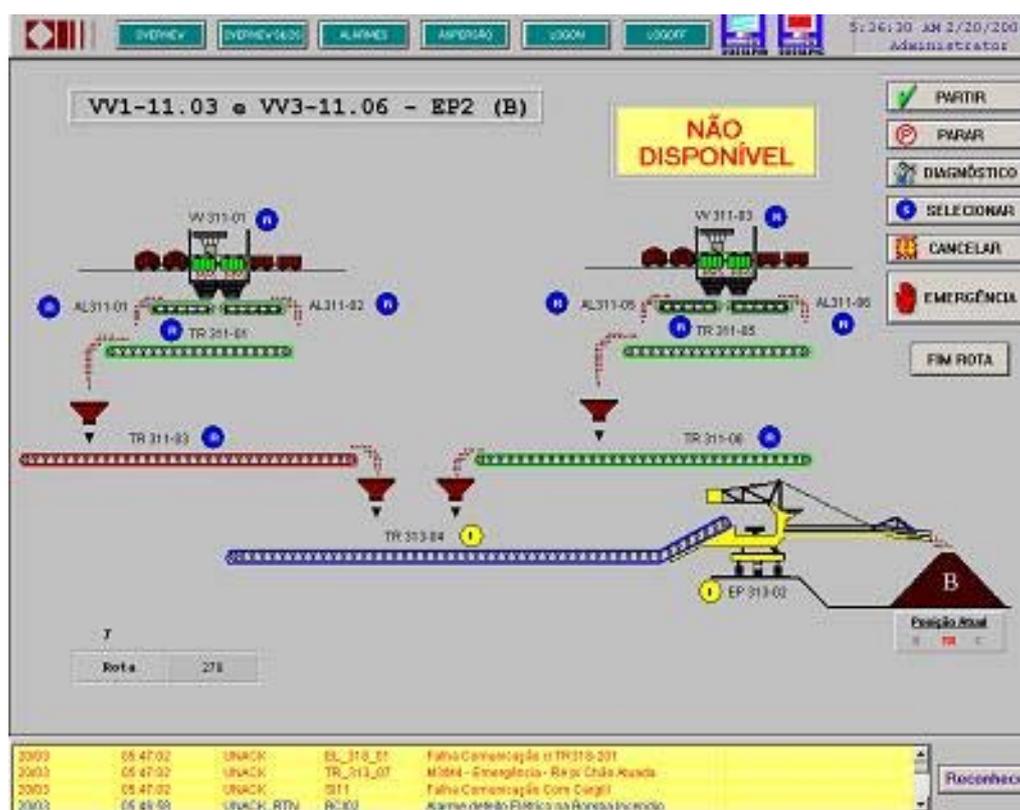


Figura 2 – Tela sinóptica do Sistema de Supervisão e Controle dos Viradores de Vagões do TPPM da Vale em São Luis.

Operacionalmente, o ciclo consiste de:

- Recebimento da composição composta por 102 ou 104 vagões carregados de minério de ferro, provenientes de Carajás;
- Posicionamento do primeiro par de vagões no virador de vagões, através de um empurrador de vagões (que pode ser elétrico ou hidráulico). Quando os vagões atingem a posição de giro dentro da “gaiola” são travados, e também os vagões que estão do lado de fora são travados no engate, por segurança;

- Com os vagões travados, é realizado o giro de 120 graus (manualmente pode chegar a 180 graus), descarregando o minério de ferro na moega;
- Cada virador de vagões possui os seguintes equipamentos, conforme pode ser visto na Figura 2: duas moegas (uma para cada vagão). Na parte inferior dessas moegas existem alimentadores que são correias de sapatas metálicas, equipamentos AL311-01 e AL311-02 do virador 01 - VV 311-01; que descarregam o minério nas correias transportadoras TR311-01 e TR 311-05; e essas encaminham o minério de ferro para o pátio de estocagem e manuseio, por exemplo, pátio B, usando para empilhar a máquina móvel EP 313k-02.

2.2.2 A automação do Virador de Vagões

Para garantir uma maior produtividade dos equipamentos instalados, toda a planta é automatizada garantindo maior confiabilidade, controle, segurança e produtividade.

A automação do TPPM é segmentada, sendo composta por quatro níveis de automação bem distintos, que trabalham em conjunto, sendo compostos conforme apresentado na Figura 3 [5] e descritos a seguir, de maneira estrutural em:

- Nível 0 – Aquisição de Dados - Equipamentos de campo como relés, medidores, disjuntores, inversores e componentes conectados a módulos de entrada e saída dos CLP's (controladores lógicos programáveis), localizados nas Subestações, Máquinas Móveis e diversos equipamentos distribuídos em todo o TPPM;
- Nível 1 – Funções de Automação, Intertravamento e Controle - CLP's (controladores lógicos programáveis) dos fabricantes GEFANUC e *Rockwell Automation*, localizados nas Subestações (para o plano diretor de 85 Mton/ano, são 26 subestações) e Máquinas Móveis (15 máquinas móveis, sendo 10 máquinas de empilhar e/ou recuperar minério localizadas nos pátios de matérias primas e 5 carregadores de navios, localizados nos píeres). O Virador de vagões possui CLP's do fabricante *Rockwell*, modelo SLC 500 nos VV01 e VV02 (viradores de vagões) e do fabricante GEFANUC modelo 90-30 no VV03, que realizam as funções de controle e intertravamento dos equipamentos;

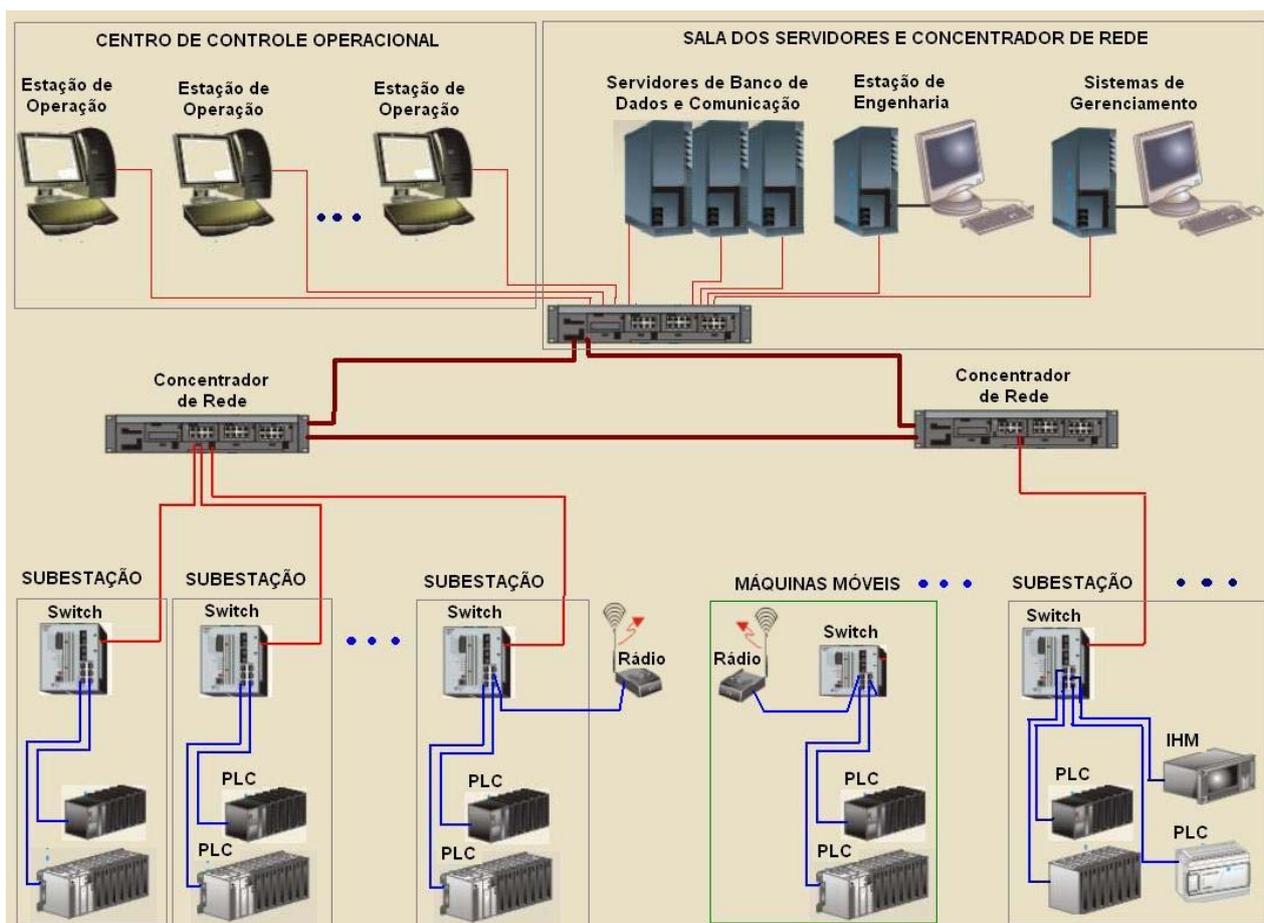


Figura 3 – Estrutura Simplificada de Automação e Controle do TPPM

- Nível 2 – Supervisão e Gerenciamento - Estações de operação (atualmente são 10 estações no CCO – Centro de Controle Operacional e outras 10 estações distribuídas na área) que utilizam software aplicativo INTOUCH da fabricante *Wonderware*, versões 8.0 e 9.0, possuindo “drivers OPC” e outros de comunicação com os CLP’s (controladores lógicos programáveis), e estações IHM’s (interface homem máquina) com aplicações dedicadas (atualmente são 16 IHM’s instaladas em máquinas móveis e subestações). Para os viradores de vagões, tem-se uma aplicação INTOUCH versão 8.0 do fabricante *Wonderware*, em três Estações de Operação dedicadas, aplicação esta que pode controlar simultaneamente ou individualmente os três viradores. Essas estações estão ligadas à rede de automação e supervisão, buscando informações através da rede de Automação dos CLP’s que controlam os equipamentos. Pela rede de Supervisão fornece informação para o Nível 3. Estas estações estão localizadas no CCO – Centro de

Controle Operacional. Além das estações de operação e controle dos viradores de vagões, o CCO possui ainda quatro Estações de Operação e Controle de Rotas que gerenciam e definem as rotas de descarga (minério recebido pelos viradores e empilhado no pátio) e embarque (minério recuperado dos pátios e carregado nos navios). Essas estações são clientes de dois servidores de comunicação, que também usam a plataforma INTOUCH. Esses servidores fazem a interface com todos os CLP's do campo, e disponibilizam esses dados para as estações clientes de rota e outras mais;

- Nível 3 – Sistema de Gerenciamento Integrado da Planta Industrial - PIMS (*Plant Information Management System*, que utiliza a plataforma *Infoplus* versão 6.0 da fabricante *Aspentech*) e Intranet, desenvolvida com a plataforma Visual Studio .Net. Composto por dois servidores de comunicação (os mesmos usados pelas estações de rota, sendo que esses servidores fornecem dados tanto para essas estações como para outros sistemas), e um Servidor PIMS que está ligado à rede de supervisão e rede corporativa da Vale. Esse servidor conecta-se aos servidores de comunicação para obter os dados operacionais de campo através da rede automação, disponibilizando esses dados aos clientes (mais de 350 usuários em Maio/2007] através da rede corporativa da Vale.

A planta industrial do TPPM está em franco crescimento, com capacidade atual (ano de 2006] de recebimento e carregamento de 77 Milhões de toneladas de minério de ferro (em transição do plano diretor de 70 Mton/ano para o de 85 Mton/ano), com investimentos e contratos aprovados para atingir 130 Milhões de toneladas de minério de ferro (plano diretor de 130 Mton/ano para 2010, dados de Maio/2007]. Com esses investimentos, o número de equipamentos instalados irá crescer novamente, e exigir novas técnicas que auxiliem a equipe de operação e manutenção da planta.

Atualmente, para o plano diretor de 85 Milhões de toneladas por ano, existem em operação três viradores de vagões automatizados, com projeto de um quarto virador de vagões para o plano diretor de 130 Milhões de toneladas por ano, conforme Figura 4 [5].

levar as plantas automatizadas para uma utilização máxima dos seus recursos, enquanto o impacto para a sociedade aumenta em níveis inaceitáveis. A redução da mão-de-obra experiente se acentua, a substituição de operadores e engenheiros experientes por recém-formados também, de modo que o risco de se operar uma planta industrial cresce cada vez mais. Devido a essa complexidade, devem-se fornecer informações mais precisas e no momento adequado às equipes de operação e manutenção, de modo que auxiliem suas tarefas.

No acidente químico ocorrido em *Bhopal* [7], devido a erros humanos e de projeto, aproximadamente duas mil pessoas morreram e outras 200 mil foram feridas. O desastre de Chernobyl foi causado por que engenheiros e gerentes realizaram atividades fora do controle automático, em modo manual. O maior desastre econômico dos EUA não ocorreu devido a causas naturais em 1989, e sim devido a falhas humanas, quando um acidente em uma planta petroquímica na cidade do Texas gerou um prejuízo de um bilhão e seiscentos milhões de dólares [1].

O mercado de gerenciamento de alarmes e produtos de racionalização está em franco desenvolvimento, apresentando desenvolvimento realizado por fabricantes de equipamentos de controle e empresas de desenvolvimento de soluções customizadas. Dessa forma, não existe hoje um padrão na área de gerenciamento de alarmes e racionalização aceito pelo mercado.

2.3.1 Institutos de Pesquisa e de Desenvolvimento de Sistemas Informatizados de Gerenciamento de Alarmes e Sistemas de Automação

Um dos padrões mais bem conhecidos é o da EEMUA (*"The British Engineering Equipment and Materials Users Association"*) [8], que publicou o guia *"Alarm Systems, a Guide to Design, Management and Procurement"* [9] conforme pode ser visto na Figura 5 [9]. Esse guia possui algumas métricas para o bom desempenho do sistema de alarmes. Dentre os 27 membros da EEMUA, que compartilham seus padrões e conhecimentos, vale citar ABB, BASF, BP, ExxonMobil, Phillips, Shell e Texaco.

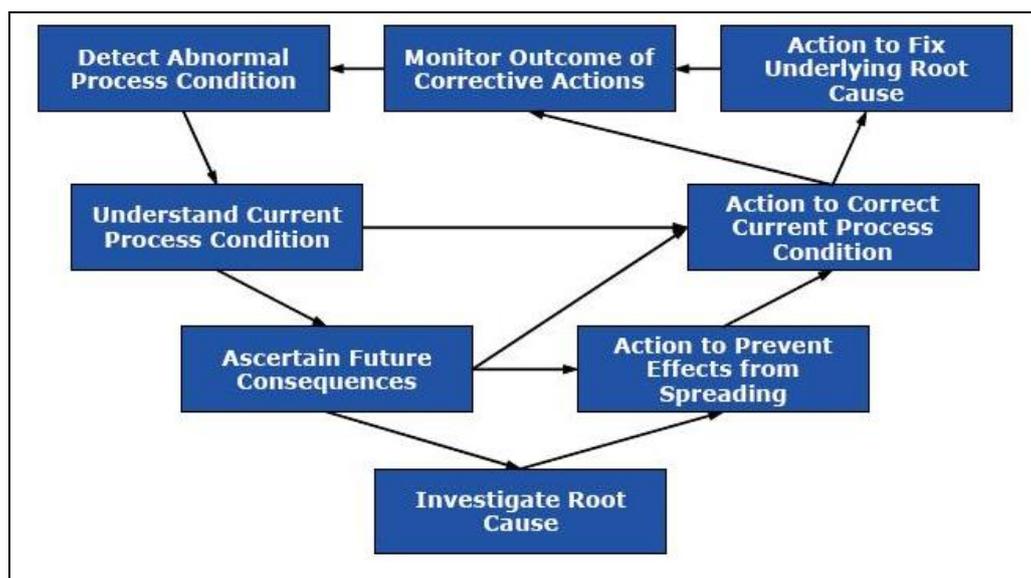


Figura 5 – EEMUA – Mapa de Recomendações de Ações para o Operador quando da ocorrência de Eventos Pendentes ou Anormais

A EEMUA define que um operador de DCS (“*Discrete Control System*”) pode efetivamente gerenciar até 150 alarmes em um dia, o que na média significa um alarme a cada dez minutos. Um alarme a cada cinco minutos ou 300 alarmes por dia ainda é considerado gerenciável, como apresenta a Tabela 1 [9]. Naturalmente, a realidade é muito diferente. Os alarmes típicos para uma grande refinaria podem atingir 14 mil ocorrências por dia [4].

Tabela 1 – EEMUA – Critério de ocorrência de Alarmes para Condições Normais de Operação em Sistemas de Automação Industrial

Long Term Average Alarm Rate in Steady Operation	Acceptability
More than 1 per minute	Very likely to be unacceptable
One per 2 minutes	Likely to be over-demanding
One per 5 minutes	Manageable
Less than one per 10 minutes	Very likely to be acceptable

EEMUA define que os alarmes devem ser ajustados no ponto onde o operador deve tomar alguma ação. Se os alarmes forem ajustados de forma conservadora, serão acionados durante operação normal – assim os alarmes não farão sentido, pois os usuários não terão nada a fazer. Agora, se os alarmes forem ajustados fora da faixa de

operação normal da planta, será tarde para o operador tomar a ação – a condição anormal que deveria ter sido alertada ao usuário já ocorreu, conforme mostra a Figura 6 [9].

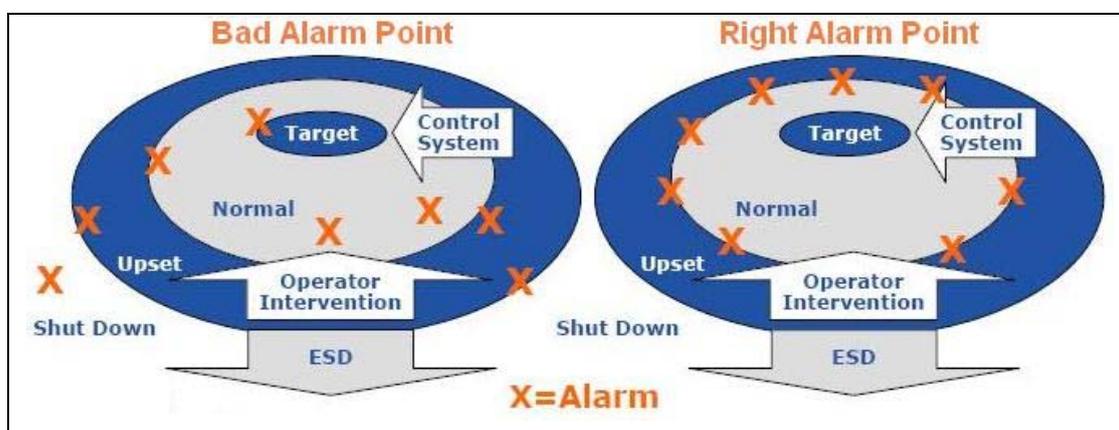


Figura 6 – EEMUA – Um alarme efetivo deve estar no ponto onde o operador deve tomar a ação [9]

O guia "*Alarm Systems, a Guide to Design, Management and Procurement*" da EEMUA [9] é reconhecida como sendo a melhor prática na gestão de alarmes, sendo considerada de fato por muitos como um padrão para projeto, gerenciamento e aquisição de sistemas de alarmes. É também reconhecido e considerado como uma “boa prática industrial” por OSHA [10]. Baseada no Reino Unido, a EEMUA é uma organização composta substancialmente por compradores e usuários de produtos de engenharia de várias indústrias, como indústrias de óleo, gás, energia, que buscam reduzir custos através do compartilhamento de conhecimentos e recursos. EEMUA não é uma entidade criadora de padrões, mas busca o desenvolvimento de padrões existentes compartilhando seu conhecimento com o resto do mundo [4].

Em 1970, foi criado nos Estados Unidos a OSHA [10] (“*Occupational Safety and Health Administration*”), como uma agência do departamento de trabalho. Sua missão é prevenir a ocorrência de ferimentos, doenças e mortes relacionadas ao trabalho, através do desenvolvimento de padrões e normas de segurança de trabalho. Em 1992, OSHA criou o PSM (“*Process Safety Management*”), como 29CFR1910.119 [11], com o objetivo de reduzir ou minimizar as conseqüências de uma catástrofe em grande escala com produtos químicos, tóxicos, inflamáveis ou reativos, como o ocorrido em Bhopal. O PSM contém

requisitos para o gerenciamento de risco associado a processos que utilizam produtos químicos de alto risco, com boa aceitação pelas indústrias petroquímicas.

A HSE (*"The British Health & Safety Executive"*) [12] possui também um guia que fornece alguma assistência, em *"Better Alarm Handling"* [13] e no documento de medidas técnicas *"Control Systems"* [12]. A HSE foi fundada há mais de 30 anos na Inglaterra, sendo responsável pela regulamentação de saúde e segurança no trabalho na indústria, mineração, hospitais, escolas e outras áreas de atividades.

A ISA (*"The Instrumentation, Systems, and Automation Society"*) [14] oferece o documento *"ISA TR91.00.02 - Criticality Classification Guideline"* [15] que é um guia que define características mínimas para equipamentos críticos de instrumentação industrial, utilizados na operação e também para sinalizarem emergências e alarmes; e também o *"ANSI/ISA S18.1 1992 - Annunciator Sequences and Specifications"* [16]. Esse documento teve a primeira versão em 1979, quando os sistemas eram discretos. Estabelece um padrão para a terminologia de anunciadores, define e apresenta seqüências, especificando e documentando os anunciadores. A função dos anunciadores é chamar a atenção para condições anormais no processo, através da simples iluminação ou emissão de algum som. Além desses padrões, ISA publicou também *"RP77.60.02-2000 Fossil Fuel Power Plant Human-Machine Interface"* [14] e *"ISA-SP18 Instrument Signals and Alarms"* [17].

O IEC (*"International Electro technical Commission"*) [18] tem os documentos *"IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems"* [19] e o *"IEC 61511 - Functional Safety: Safety Instrumented Systems for the Process Industry Sector"* [20] que relacionam segurança e sistemas de instrumentação, para aplicações que gerenciam os alarmes durante eventos críticos.

A ASM (*"The Abnormal Situation Management"*) [21], consórcio criado em 1992 com objetivo de definir melhorias e padrões no sistema de alarmes existentes, formado por grandes empresas (*BAW Architecture, BP, Celanese, Chevron, ConocoPhillips, ExxonMobil, Honeywell, Human Centered Solutions, Nanyang Technological University, Sasol, Shell, TTS Performance Systems, UCLA*) e universidades (*"Ohio State University - Department of Chemical Engineering e Purdue University School of Chemical Engineering"*) tem realizado considerável esforço no desenvolvimento de sistemas para

gerenciamento de situações anormais / críticas e gerado também um grande número de artigos.

ARC *Advisory Group* [22] foi fundada em 1986, sendo hoje a líder no fornecimento de serviços de suporte ao planejamento estratégico e tecnológico, para empresas de manufaturas, utilidades, fornecedores globais de logística, tão bem quanto empresas de software e fornecedores de soluções em todo o mundo. O objetivo da ARC é simples, e ainda crítico: melhorar o desempenho obtendo maior retorno dos ativos existentes, melhorando o desempenho operacional e reduzindo os custos de propriedade. Em outras palavras, buscar o nível correto de automação nos ativos existentes, de modo a produzir mais, obter maior ganho e lucro, com o menor custo possível.

Além dos institutos que buscam definir padrões para a gestão dos alarmes, tem-se os fornecedores de soluções, cujo mercado apresenta crescimento acelerado. Devido à grande variedade de fornecedores e soluções propostas, a busca pela melhor solução ainda depende da experiência e da análise da solução que mais se aproxima à sua necessidade.

Algumas das empresas que fornecem sistemas de gerenciamento de alarmes e produtos de racionalização dos alarmes são Chemtech [23], *Process Systems Consultants* [24], *Control Arts* [25], PAS ("*Process Automation Services*") [26], Exida [27], Honeywell [28], Matrikon [29], TiPS [30], *Rockwell*, *Wonderware*, GE Fanuc, Yokogawa e ABB.

Para melhor caracterizar a solução proposta, realizou-se um levantamento detalhado das ferramentas e métodos existentes. O mercado apresenta soluções que se caracterizam como Sistema de Gerenciamento de Alarmes, e também Sistemas de Gerenciamento de Condições Críticas, com algum enfoque na recomendação, e também sistemas voltados ao suporte à decisão e recomendação. A seguir será descrito e conceituado Sistemas Industriais de Gerenciamento de Alarmes e Sistemas de Gerenciamento de Condições Críticas, apresentando também uma pesquisa de soluções existentes no mercado.

2.3.2 Sistemas Industriais de Gerenciamento de Alarmes

Os sistemas de automação industriais atualmente concentram toda a supervisão e controle da planta industrial nas salas de controle, onde os operadores recebem uma quantidade muito grande de informação relacionada com alarmes e eventos dos sistemas

de controle. Além de serem geradas em grande número e com grande rapidez, estas informações muitas vezes não são claras e a ação imediata requerida do operador não é óbvia, pois não há uma correlação entre os vários alarmes acionados com a sua causa real.

Por definição, tem-se que os alarmes são um sinal ao operador, indicando que eles devem intervir na operação do processo para corrigir uma condição indesejada na planta, retornando o processo a um estado normal ou para impedir que o processo entre em condição anormal/insegura. É a primeira camada em uma estratégia de segurança composta por várias camadas, conforme Figura 7 [32]. Os operadores devem ver alarmes no contexto da operação da planta como um todo. Não faz nenhum sentido, por exemplo, que um operador tenha que responder a um alarme para o fluxo baixo quando a bomba que controla o fluxo é desligada para a manutenção. Alarmes que funcionam corretamente devem alertar o operador da ocorrência de uma mudança, informar o operador da natureza dessa mudança, e guiar o operador para realização de uma ação corretiva [4].

Sistemas Industriais de Gerenciamento de Alarmes tratam de forma inteligente as informações de alarme das plantas, organizando as mesmas para uma melhor compreensão do problema e para uma resposta mais rápida pelo lado dos operadores [31].

Sistemas de Automação de áreas críticas necessitam de um Sistema de Alarme, voltado exclusivamente para a redução de incidentes nas plantas industriais, auxiliando também na manutenção e no seu correto funcionamento. Um Sistema de Alarme eficiente direciona o operador aos pontos onde estão ocorrendo os desvios. Se mal configurado, pode confundir e sobrecarregar o operador com informações irrelevantes, atrasando suas ações. Isso acarreta perdas contínuas para o processo e, em caso de um evento crítico, pode ocasionar a parada da planta e/ou acidentes graves como uma explosão. Neste caso, o desenvolvimento de um programa de gerenciamento de alarmes representa ganho tanto para minimizar perdas e aperfeiçoar a produção, quanto para aumentar a confiabilidade e segurança do processo.

O principal sintoma que alerta para a existência de um problema quanto à configuração do sistema de alarmes é quando freqüentemente ocorrem muitos alarmes em curtos períodos de tempo [9], conforme já apresentado na Tabela 1. Mas este não é o único

indício de que é necessária uma revisão nos critérios de alarmes. Outros sintomas que podem ser destacados são [9]:

- Ocorrência de alarmes desnecessários - não necessitam de ações do operador;
- Existência de alarmes fixos - permanecem ativos por longos períodos ou aparecem repetidas vezes, sem que o operador tenha tido tempo para tomar uma ação;
- Alarmes que permanecem ativos mesmo após a situação da planta ter sido normalizada;
- Pequenas flutuações de variáveis geram um número significativo de alarmes sem que isso represente um desvio importante para o processo.

As melhores práticas para o gerenciamento de alarmes requerem distinções entre alarmes e alertas. Os alertas fornecem um mecanismo de advertência, mas não requerem necessariamente a ação imediata. Os alarmes devem nunca ser usados como um aviso, e devem sempre requerer a ação do operador [4].

Atualmente, as plantas automatizadas – com instalação de SCADA (“*Supervisory Control And Data Acquisition*”), DDC (“*Digital Direct Control*”), DCS (“*Discrete Control System*”) e SDCD’s (Sistema Distribuído de Controle Digital) – possuem sistemas de controle programados com vários tipos de alarmes. Nesses sistemas, devido à facilidade para inserir pontos de alarme, a configuração é feita sem análise e planejamento adequado, associando a programação de alarmes com os riscos operacionais. A consequência dessa falta de planejamento para as indústrias foi o acúmulo de alarmes desnecessários e espúrios.

Algumas ações simples podem racionalizar o número de alarmes. O primeiro ponto é um estudo prévio em relação às variáveis que realmente precisam gerar alarmes que necessitem de uma ação do operador. Em segundo lugar, o ajuste das faixas para que os alarmes disparem é de fundamental importância. Quando flutuações normais do processo geram alarmes, é sinal que deve ser feita uma revisão quanto à configuração. Esses alarmes tornam-se um incômodo ao operador e são quase sempre ignorados ou desligados.

Um alarme é efetivo quando este marca o ponto onde o operador deve agir, conforme apresentado na Figura 6. Os ajustes efetuados no sistema de alarme devem ser sistematicamente documentados em qualquer fase de configuração.

A racionalização é uma etapa importante do programa de gerenciamento de alarmes. Nela, a aplicação de um software de gerenciamento de alarmes reduz consideravelmente o tempo gasto para identificar os alarmes espúrios, alarmes associados a um determinado evento e alarme que ocorre com maior frequência.

Quando ocorre um evento que gera uma seqüência de alarmes, sem uma definição de prioridade e associação entre variáveis, há uma sobrecarga de informações para o operador. Com isso, informações relevantes podem ser mascaradas fazendo com que ocorra uma demora para a resposta. Desta forma, muitas vezes o problema só será percebido quando a planta se desvia perigosamente de sua operação normal.

A eficiência de um sistema de alarmes não está na quantidade de alarmes e sim na qualidade da informação que eles transmitem e na capacidade dos mesmos de orientar a ação do operador, conforme apresentado na Tabela 1, que apresenta os níveis aceitáveis de alarmes para um operador analisar.

Quando um alarme espúrio é removido, o operador fica focado apenas naqueles que têm importância, e para os quais se espera uma ação. Quando o operador não tem como distinguir uma prioridade entre vários alarmes ocorrendo simultaneamente, e qual efetivamente é o problema, pode haver uma demora para se tomar uma ação corretiva ou preventiva dentro de um cenário de risco operacional.

Gerenciamento de alarmes é um conjunto de procedimentos e ferramentas para a avaliação e monitoramento de alarmes. Não é uma ação de curto prazo, mas uma prática contínua que visa obter melhor desempenho operacional da planta industrial. Um programa de avaliação do sistema de alarmes envolve diversas áreas, como operação, engenharia básica, acompanhamento de processos e controle. Neste contexto, o software de gerenciamento de alarmes é uma ferramenta de análise e diagnóstico que serve como base para um programa amplo dentro da indústria de processos.

As abordagens mais antigas de gerenciamento de alarmes são baseadas apenas em análises estatísticas capazes de identificar os alarmes que ocorrem com maior frequência e fazer uma associação entre variáveis que geralmente estão associadas a um mesmo evento. Em abordagens mais recentes, as características definidas para um sistema inteligente de gerenciamento de alarmes incluem [4].

- Identificar alarmes espúrios, falsos e repetitivos;

- Priorizar importância de alarmes através da avaliação de riscos e suprimir alarmes que sejam consequências diretas de outros alarmes;
- Guiar o operador às possíveis causas do alarme;
- Auxiliar o operador como responder ao alarme através de procedimentos em tempo-real.

2.3.3 Sistemas de Gerenciamento de Condições Críticas

Asish Ghosh define “Condição Crítica” [32] como um estado do processo de manufatura, o qual está além do estado normal, mas por pouco ainda não atingiu a situação de emergência. Define ainda que a função de gerenciamento da condição crítica – CCM (“*Critical Condition Management*”) deve estar sempre ativa sendo executada em background, para reduzir a possibilidade da transição do um estado normal para o estado crítico, no caso de ocorrer uma emergência, minimizando o seu efeito [32].

Condições críticas são usualmente causadas por uma combinação de eventos que normalmente não se espera que ocorram simultaneamente. Intertravamentos de segurança e lógicas de exceção em sistemas de controle convencionais não estão adequados para essa combinação de eventos, e o operador tem pouca experiência para lidar com eles. No acidente de Bhopal, por exemplo, a quantidade de *Methyl Isocyanate* armazenado estava abaixo do limite, o sensor do limite de temperatura estava desligado, a leitura do medidor de pressão estava incorreto e sendo ignorado, e os operadores tinham pouca experiência e nenhum guia para lidar com condições críticas que ocorressem de maneira inesperada [1]. Todos esses itens levaram à ocorrência do acidente.

A boa notícia é que as condições mais críticas não levam a situações de catástrofes, explosões e incêndios. Elas, entretanto, levam a outros sérios impactos negativos no desempenho e rentabilidade da planta, causando [1]:

- Produtos fora da especificação;
- Paralisações não planejadas da planta
- Danos aos equipamentos
- Atrasos em cronogramas
- Problemas ambientais e de segurança

- Baixa utilização dos recursos

Os eventos mais críticos usualmente fazem parte da categoria referenciada como "incidentes levam a perdas" [32]. Esses eventos críticos podem levar a uma categoria maior de perda de desempenho, outras vezes conhecida como paradas não programadas, ou simplesmente perdas. Nas indústrias de processo, paradas não programadas comprometem em média de dois a cinco por cento da produção. Analisando somente as indústrias químicas, a média de perdas por falhas é de aproximadamente 19 milhões de dólares por ano [32].

Um dos pontos citados que tem aumentado a condição crítica são:

- Aumento da complexidade da automação;
- Operação de plantas e equipamentos próximos do seu limite;
- Maior consciência ambiental;
- Aumento das restrições ambientais;
- Carência de pessoal treinado e capacitado;

Uma planta de processo automatizada deve possuir múltiplas camadas protetoras, conforme apresentado na Figura 7 [32].

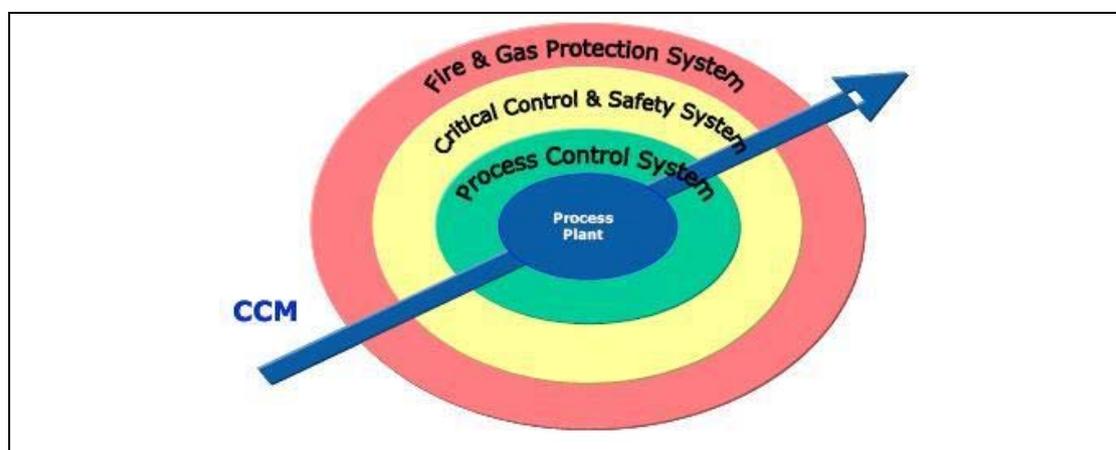


Figura 7 – Camadas de Proteção de um SIGA em uma Planta Industrial Automatizada

A primeira camada, o núcleo, é o processo de controle do sistema. Sua função primária é assegurar uma operação previsível e segura para o processo. A segunda camada deve ser provida de um sistema de segurança, cuja função primária é garantir uma paralisação de maneira ordenada quando o sistema de controle for incapaz de fazê-lo de uma forma previsível. Em alguns casos, tem-se uma terceira camada com sistema de proteção

contra fogo e gases. Esse sistema opera de maneira reativa e fornece um guia de ações para o operador. A função CCM deve trabalhar de forma preventiva nessas camadas de proteção, provendo orientações e ações para mitigação dos problemas, em caso de uma situação crítica.

As funções necessárias para o gerenciamento das condições críticas são apresentadas na Figura 8 [1].

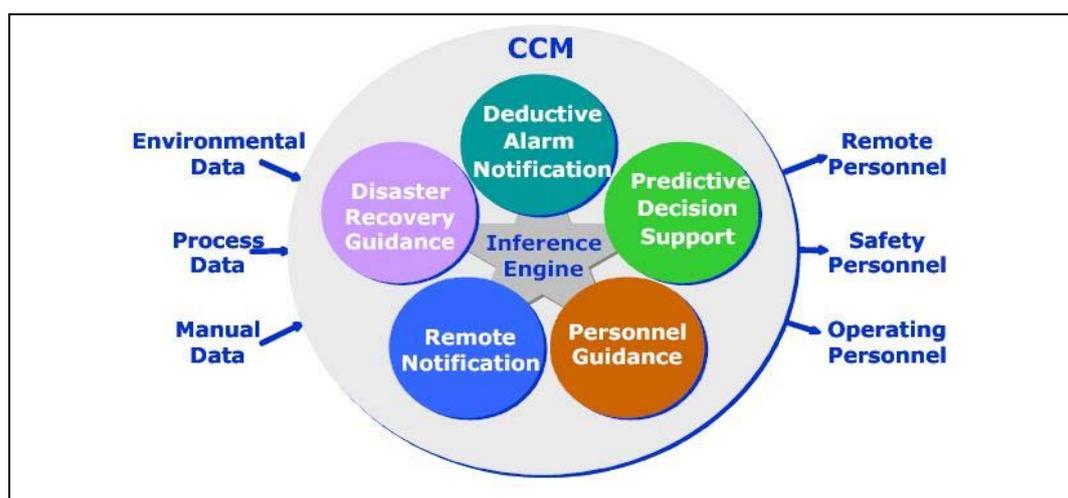


Figura 8 – Funções Necessárias para o Gerenciamento de Condições Críticas - CCM

Observando essas funções, *Asish Ghosh* apresenta a Tabela 2 [1], que compara as Funções de um Sistema de Controle tradicional com um CCM – Sistema de Gerenciamento de Condições Críticas.

Uma estratégia de alarme efetiva possui um papel crítico no CCM. Uma boa referência é o padrão EEMUA 191 [9], que serve como uma boa base para racionalização de alarmes. *Asish Ghosh* [32] afirma que a melhor prática para desenvolver uma boa estratégia de alarmes é criar uma equipe com o melhor operador e o melhor engenheiro de controle para o projeto. A definição de cada alarme requer de 5 a 10 minutos, e com o uso dos mais experientes, a ação é mais efetiva.

CCM prove benefícios econômicos significantes para indústrias. Um ganho típico de otimização de processo em uma grande indústria de processo contínuo, como uma refinaria ou uma planta petroquímica é em torno de três por cento, enquanto uma aplicação de CCM pode adicionar cinco por cento ou mais de rendimento detectando e evitando condições críticas antes que elas ocorram, reduzindo a necessidade de paradas

de produção em emergência, economizando milhões de dólares, conforme Figura 9 [32].

Outros benefícios obtidos com CCM são [1]:

- Detecção preditiva dos alarmes;
- Guia Operacional;
- Redução significativa das paradas de produção não planejadas;
- Melhor utilização dos recursos.

Tabela 2 – Comparação entre as Funções de um Sistema de Controle com um CCM.

Função	Sistema de Controle	Sistema de Gerenciamento de Condições Críticas
Entradas	Várias através de sensores e equipamentos	Através de sensores, equipamentos e entradas manuais
Ações Corretivas	Automática	Ação Manual
Utilizado por	Pessoal Operacional	Pessoal de Segurança e Operacional
Detecção de Alarmes	Reativa	Preditiva
Gerenciamento de Alarmes	Não Dedutiva	Notificação Dedutiva
Guia Operacional	Pequeno	Significante
Guia para Segurança Pessoal	Não	Significante
Notificação para autoridades locais	Não	Significante
Guia para recuperação de desastres	Não	Significante

Asish Ghosh [32] recomenda que CCM deva ser considerado em processos importantes de plantas industriais, onde há riscos consideráveis para a saúde humana e também de grandes perdas monetárias. CCM geralmente é um sistema de recomendação, e não substitui um conjunto bem projetado de segurança em camadas, incluindo uma racionalização dos alarmes estratégicos. Quando se projeta uma aplicação CCM, deve-se sempre integrar uma estratégia de validação automática, para eliminar alarmes falsos, os quais podem causar um incidente em vez de evitar acidentes.

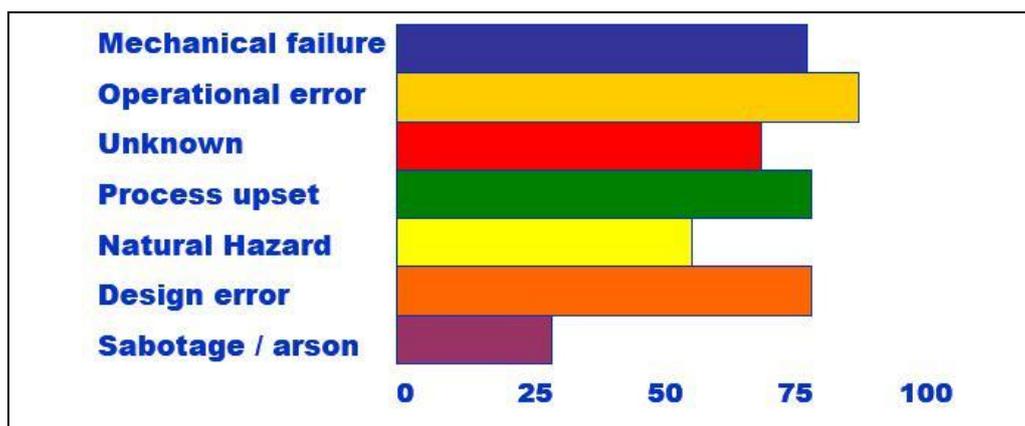


Figura 9 – Média de perdas em Milhões de Dólares causados pelos Maiores Acidentes Industriais

2.3.4 Empresas de Desenvolvimento de Sistemas Informatizados de Gerenciamento de Alarmes e Estudos de Casos

2.3.4.1 . HSE – Refinaria Milford Haven da Texaco

HSE realizou o estudo levantando fatores que levaram ao acidente da Refinaria *Milford Haven* da Texaco, em 1994 [7]. Esse estudo identifica três fatores principais, que acidentou vinte seis pessoas e trouxe um prejuízo de 48 milhões de libras, são eles:

- Havia muitos alarmes e eles eram priorizados de maneira ineficiente;
- As telas da sala de controle não ajudaram os operadores a entender o que estava acontecendo;
- O treinamento foi inadequado para os operadores lidarem com casos operacionais críticos na planta.

Além dos fatores acima, nos últimos onze minutos antes do acidente, dois operadores receberam 275 alarmes para tratar, reconhecer e agir [7].

Conforme estudos realizados pela EEMUA, presentes no “*EEMUA Guide*” [9] têm como desejável “No máximo um alarme a cada dez minutos de operação normal, e não mais do que dez alarmes apresentados nos dez primeiros minutos após a ocorrência operacional mais crítica”.

Para o correto funcionamento, deve-se priorizar de maneira efetiva os alarmes [9]:

- Definir regras de priorização e aplicá-las de maneira consistente em cada alarme de cada sistema;

- Usar aproximadamente três prioridades apenas;
- Basear as prioridades nos efeitos que podem acontecer caso o operador falhe ao responder/reconhecer a falha;
- Priorizar proporcionalmente, alocando, por exemplo, 5% dos alarmes como alta prioridade, 15% como média prioridade e 80% como baixa prioridade.

Os estudos da HSE apresentam que um correto manuseio dos alarmes pode ter um efeito significativo na segurança do negócio. Uma melhoria realizada na gestão dos alarmes pode trazer um controle de qualidade mais apurado, melhoria no diagnóstico e gerenciamento mais efetivo da planta pelos operadores. Os estudos apresentam um número grande de técnicas rápidas e fáceis de programar, que podem trazer benefícios imediatos. Atividades planejadas de médio e longo prazo podem trazer benefícios também mais duradouros.

2.3.4.2 National University of Singapore – Refinaria de Singapura

Pesquisadores da Universidade de Singapura desenvolveram um Sistema Inteligente de Gerenciamento de Alarmes – IAMS [33], que tem como objetivo inibir alarmes que não sejam críticos, como alarmes causados por falhas de equipamentos de medição, por exemplo – quando um valor de medição de uma variável está fora de faixa, em um nível que pode causar uma explosão ou dano a vidas e equipamentos, o operador deve agir; mas se o valor estiver sendo medido erroneamente, devido à falha de equipamento, a ação não necessita ser imediata.

O projeto do IAMS baseou-se em estudos apresentados pela HSE [7] e outros artigos dos próprios autores. O sistema foi projetado para ser implantado na Refinaria de Singapura. Antes da implantação do IAMS, o sistema de automação da refinaria gerava um alarme a cada 50 segundos durante operação normal, e um alarme a cada 10 segundos em casos de falhas operacionais e/ou de equipamentos [33]. O IAMS foi implantado inicialmente para reduzir o número de alarmes apresentados aos operadores, do elevado nível atual a um nível mais gerenciável.

Após implantar o IAMS e reduzir a geração de alarmes indesejados, o sistema passou a gerar informações que aconselham ações para o operador.

Os principais tipos de alarmes indesejados são os alarmes repetidos, e alarmes gerados por condições de valores fixos fora de faixa – enquanto esses valores permanecerem fora de faixa, alarmes continuam a serem registrados como pode ser visto na Figura 10. Em plantas típicas, esses alarmes correspondem a 50% dos alarmes [33].

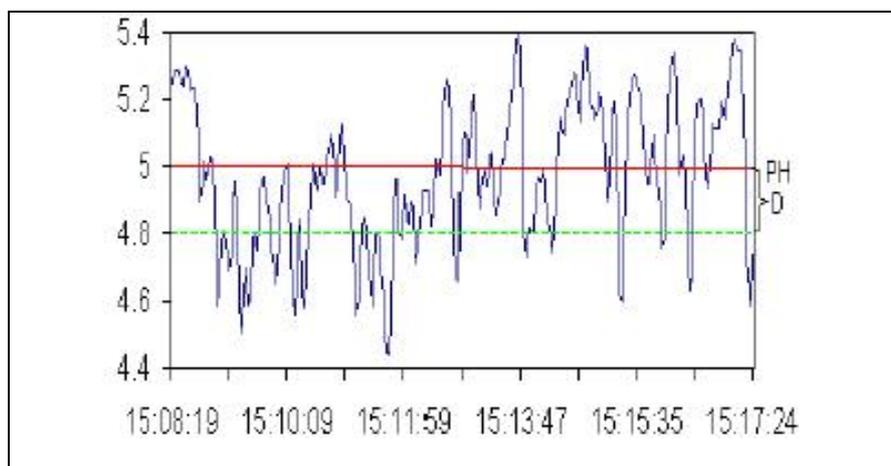


Figura 10 – Alarmes indesejados gerados de maneira repetitiva toda vez que ultrapassa limites.

Para os alarmes gerados fora de faixa, programa-se uma solução de banda morta, de modo que o alarme só é gerado quando ultrapassa o valor, e não o tempo todo em que estiver acima do valor desejado. A escolha do valor dessa banda morta é crítico, pois bandas mortas com valores grandes poderão deixar o processo oscilar fora de faixa sem notificar o operador, Figura 10 e Figura 11 [33].

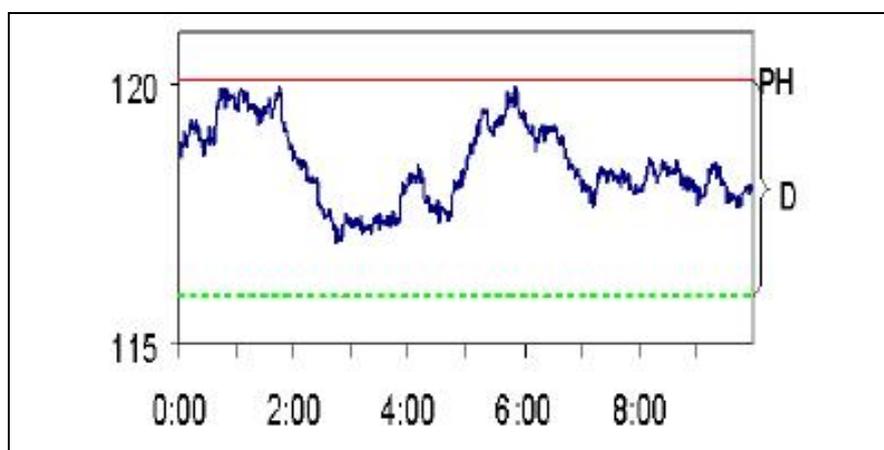


Figura 11 – Alarmes indesejados bloqueados com sistema oscilando por um grande tempo sem aviso ao operador.

Muitos sistemas de automação já possuem uma banda morta para variáveis analógicas de 2%. Porém, esse ajuste geralmente é estático, e não varia conforme o processo. Foi desenvolvido no IAMS um algoritmo que, a partir do valor das variáveis do processo e da sua variabilidade, aumenta ou diminui as extremidades da banda morta. Com esse algoritmo, variáveis que geravam 53 alarmes no intervalo de 5 minutos reduziram para apenas três alarmes nesse mesmo intervalo [33].

Para os alarmes repetitivos, criou-se uma ferramenta com a qual o operador identifica que o alarme está repetitivo, e “congela” a sua geração de alarmes. O tempo para esse congelamento pode ser configurado, e o operador pode a qualquer momento “descongelar” o status e normalizar a geração dos alarmes.

O sistema inteligente de aconselhamento de ações foi desenvolvido para fornecer conselhos operacionais para os operadores quando encontram diferentes situações de alarme. Algumas das informações úteis para operadores e engenheiros das plantas são:

- Identificação de alarmes importantes;
- Aviso prévio para alarmes crescentes;
- Mudança de estado em malhas de controle que requerem atenção;
- Informações estatísticas;
- Visão geral do gerenciamento dos alarmes;
- Detecção de falha em sistemas;
- Relatórios para a manutenção.

O sistema implantado foi baseado em heurística a partir da experiência dos engenheiros da planta e estudos de diferentes alarmes da refinaria.

Com a implantação do IAMS em junho de 2000 observou-se uma redução de 30% a 50% na geração de alarmes em operação normal e em momentos críticos, conforme apresentado na Figura 12 [33].

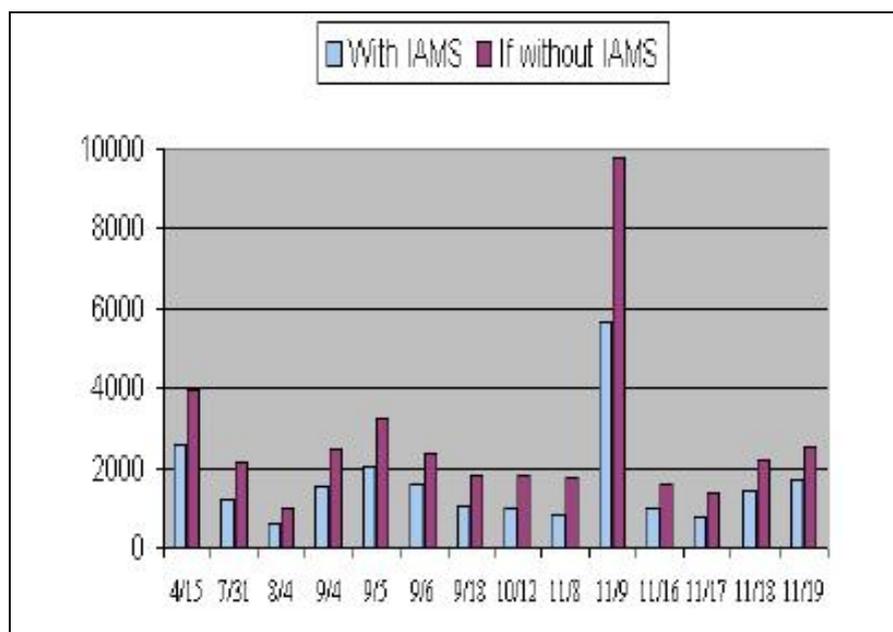


Figura 12 – Comparação dos alarmes gerados com e sem o IMAS em operação.

2.3.4.3 . Chemtech - Siemens

Qualquer não-conformidade na planta industrial que necessite de atenção por parte do operador, como variáveis fora da faixa normal de operação ou alteração brusca no comportamento do processo, são algumas situações que devem receber atenção do operador porque podem comprometer a segurança, o meio ambiente e a especificação de produtos. E para alertar o operador de uma anormalidade, plantas industriais contam com alarmes visuais e/ou sonoros que indicam que há algum problema no processo necessitando de uma ação.

Um das soluções existentes no mercado, criado pela Chemtech, trata o gerenciamento de alarmes, de modo que todos aqueles alarmes relacionados com determinados eventos são pré-configurados de forma a serem correlacionados durante um evento, filtrando as reais causas que serão apresentadas aos operadores [23].

A Chemtech utiliza uma tecnologia orientada a objeto, onde os equipamentos e as causas são correlacionados e as ações são sugeridas através da configuração de árvores de decisão e regras pré-configuradas. Vários relatórios podem ser também pré-configurados e disponibilizados através da web para o acompanhamento dos alarmes gerados pelos sistemas de controle. Toda a configuração é feita em cima de um diagrama do processo

(P&ID) e é implementada dentro do sistema. Essa solução foi implementada pela Chemtech com parceria com a holandesa *UReason* [34].

O OASYS-AM [35], software desenvolvido pela empresa holandesa *UReason* e representado no Brasil pela Chemtech em gerenciamento de alarmes, oferecem:

- Raciocínio baseado em modelos para traçar a origem de distúrbios ou para estimar as conseqüências de uma falha em um equipamento;
- Diagramas de causa-efeito para destacar os prováveis eventos futuros e ocultar a massa de alarmes que causam tal situação;
- Modelos multicamada para mostrar a interconectividade dos diferentes equipamentos;
- Identificação de estados para traçar o estado de uma unidade do processo, detectar componentes em mau-funcionamento;

O OASYS-AM permite tratar diferentes informações de alarme das plantas de forma inteligente, facilitando a compreensão do problema e a geração de uma resposta mais rápida pelo lado dos operadores. Com o gerenciamento, todos os alarmes relacionados com determinados eventos são pré-configurados de forma a serem correlacionados durante um evento, filtrando as reais causas que serão apresentadas aos operadores. A configuração é feita em cima de um diagrama do processo e é implementada dentro do sistema, assemelhando-se à representação de uma planta em um simulador.

A Chemtech programou soluções de gerenciamento de alarmes em várias indústrias. Plantas petroquímicas, de óleo, gás e usinas nucleares, presentes na Europa já contam com sistemas de gerenciamento de alarmes e representam casos bem sucedidos na área.

2.3.4.4 PROSYSINC - Process Systems Consultants

A ProSys (“*Process Systems Consultants*”) [24] desenvolveu o programa “*Alarm Dynamics*”, que atua no gerenciamento de alarmes. A motivação buscada pela ProSys para esse desenvolvimento deveu-se ao fato de que a maioria dos sistemas de configuração de alarmes são otimizados para um único estado do processo (sistema em funcionamento), deixando outros modos críticos de operação comprometidos, como sistema em desligamento e partida.

De fato, as mudanças de estado são as operações mais críticas em uma planta industrial, e muitos incidentes ocorrem na inicialização do sistema. Como resultado dessa atual configuração, os alarmes são freqüentemente apresentados aos operadores em um contexto diferente da realidade operacional. Nas mudanças dos estados operacionais uma grande quantidade de alarmes costuma ser gerado, tirando a atenção do operador nesse momento crítico.

A solução da ProSys – *Alarm Dynamics* fornece aos operadores uma interface de notificação de eventos de ações consistentes e reais, suportando suas atividades e garantindo segurança e eficiência na operação do sistema.

Esse sistema foi desenvolvido baseando-se em dois princípios:

- Todo alarme apresentado ao operador deve ter um significado claro e relevante;
- Todo alarme deve ter uma resposta definida.

Com esses princípios, tem-se que uma configuração ótima é uma onde a característica de desempenho do controle do processo, alarmes, e mensagens atingem os objetivos operacionais requeridos. Esse tipo de configuração deve [24]:

- Ajudar o operador a cumprir seus objetivos
- Não inibir o operador de tomar ações necessárias
- Não esconder informações ou condições necessárias
- Não apresentar informações ou condições desnecessárias.

2.3.4.5 Control Arts

O software “*Process Alarm Toolkit da Control Arts*” [25] fornece assistência no desenvolvimento de sistemas de alarmes, conforme apresentado na Figura 13 [25] a seguir.

O *Process Alarm Toolkit* consiste dos seguintes módulos [25]:

* *AlarmCapture* – automaticamente armazena os alarmes do DCS (“*Discrete Control System*”), ações do operador e mensagens do sistema em um banco de dados SQL (“*Structures Query Language*”). Funções adicionais permitem o agendamento de relatórios e envio de alarmes a outros usuários da planta.

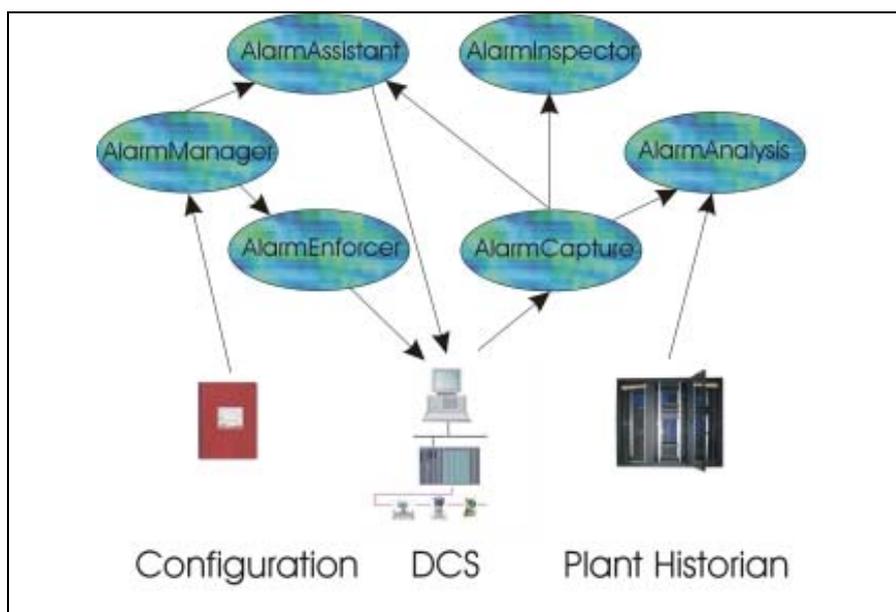


Figura 13 – Estrutura lógica do *Toolkit* da *Control Art*

* *AlarmAnalysis* – coleção sofisticada de testes gráficos e numéricos, baseado na mineração dos dados, que analisam a ocorrência dos alarmes.

O DCS gera milhares de alarmes e técnicas modernas de mineração de dados são necessárias para realçar a fonte do problema e áreas a serem cuidadas. Porém, observando um alarme individualmente não se tem dados suficientes para analisar a operação de todo um sistema. O *AlarmAnalysis* é um software que observa as ações do operador, medidas da planta, e controla as saídas para obter a melhor imagem, e a melhor técnica para seu sistema de alarmes, conforme apresentado na Figura 14.

Técnicas de análise:

- *Chattering/Frequent* – alarmes que oscilam e/ou ocorrem freqüentemente;
- *Redundancies/Subsets* – conjuntos de alarmes que ocorrem próximos no tempo, ou em uma parte do tempo;
- *Stale Alarms* – alarmes que se mantêm ativos por um tempo significativo;
- *Alarm Clusters* – grupos de alarmes que freqüentemente ocorrem juntos;
- *Alarm sequences* – alarmes que ocorrem geralmente em seqüência;
- *Time correlations* – alarmes que são impressos graficamente como uma função do tempo ou escala de operação;
- *Ignored Alarms* – alarmes que não são seguidos pelas operações dos operadores;

- *Alarm/Operator move correlations* – alarmes que se correlacionam com ações dos operadores;
- *Changed alarms* – parâmetros de alarmes que são alteados pelos operadores;
- *Trip point analysis* – determina se o ponto de acionamento do alarme está fora da faixa de operação e se a resposta dele no tempo está adequada;
- *Deadband analysis* – determina o melhor ajuste de banda morta baseado na frequência das respostas.

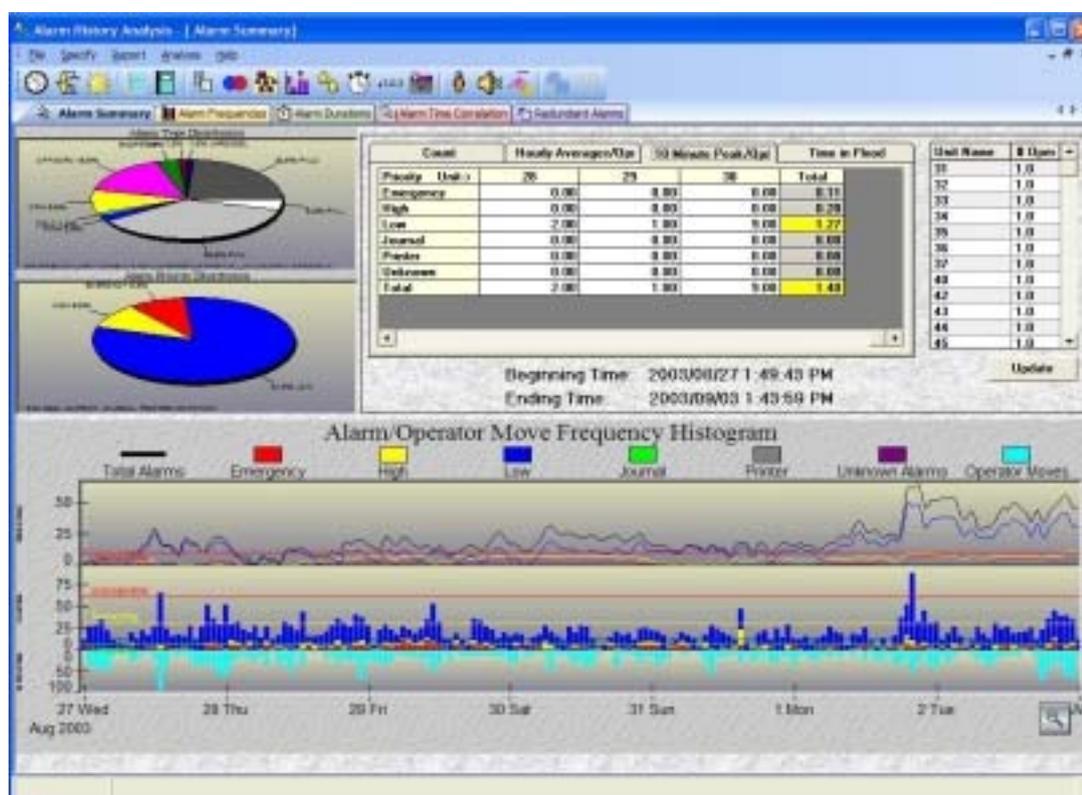


Figura 14 – Interface gráfica do software *AlarmAnalysis* do *Toolkit* da *Control Art*.

* *AlarmManager* – prove uma visão geral da configuração dos alarmes no DCS, e suporta o banco de dados de operações e gerencia as respostas do operador para cada alarme. Permite também a comparação da configuração atual com a projetada, de modo que se possa facilmente determinar as mudanças.

Uma importante parte de qualquer processo de racionalização dos alarmes é prover documentação para cada alarme.

O *Control Arts AlarmManager* prove uma interface limpa e de fácil gerenciamento de toda a configuração dos alarmes do DCS e uma tela de entrada de dados amigável para adicionar e/ou modificar alarmes, conforme apresentado na Figura 15 e Figura 16.

Tag		Design Values			TDC2000 Values			
Name	Parameter	Value	Priority	Rev. Date	Value	# Occurrences	Enable Status	Priority
ALF000	PALVAL	200	EMRGENC	1/26/99	200	246	ENABLED	EMRGENC
ALF000	PALVAL	250	HIGH	1/26/99	250	246	ENABLED	HIGH
ALP000	PARVAL	85.0	LOW	1/26/99	85.0	26	ENABLED	LOW
ALP000	PALVAL	95.0	HIGH	1/26/99	95.0	245	ENABLED	HIGH
ALT000	PARVAL	507	EMRGENC	1/26/99	507	2303	ENABLED	EMRGENC
ALT000	PALVAL	800	HIGH	1/26/99	800	321	ENABLED	HIGH
ALT000	PALVAL	810	HIGH	1/26/99	810	89	ENABLED	HIGH
ALF000	PALVAL	120	JOURNAL	1/26/99	120	44	ENABLED	JOURNAL
FC0000	PARVAL	2.5	LOW	1/26/99	2.5	258	DISABLED	LOW
FC0000	PALVAL	1.5	HIGH	1/26/99	1.5	2486	ENABLED	HIGH
FC0001	PARVAL	75.0	HIGH	1/26/99	75.0	112	ENABLED	HIGH
FC0001	PARVAL	70.0	HIGH	1/26/99	70.0	60	ENABLED	HIGH
FC0001	PALVAL	85.0	JOURNAL	1/26/99	85.0	1305	ENABLED	JOURNAL
FC0001	PALVAL	90.0	LOW	1/26/99	90.0	254	ENABLED	LOW
FCP112	PARVAL	2.0	HIGH	1/26/99	2.0	7	ENABLED	HIGH
FC0001	PARVAL	810	EMRGENC	1/26/99	810	32	ENABLED	EMRGENC
FC0001	PARVAL	800	HIGH	1/26/99	800	12	ENABLED	HIGH
FC0001	PALVAL	750	LOW	1/26/99	750	85	DISABLED	LOW
HC0000	PARVAL	2.3	LOW	1/26/99	2.3	118	ENABLED	LOW
HC0000	PARVAL	112	EMRGENC	1/26/99	112	304	DISABLED	EMRGENC
HC0000	PARVAL	110	JOURNAL	1/26/99	110	16	ENABLED	JOURNAL
HC0000	PARVAL	10000	HIGH	1/26/99	10000	7681	ENABLED	HIGH
HC0000	PALVAL	8000	HIGH	1/26/99	8000	23	ENABLED	HIGH
HC0000	PARVAL	1200	LOW	1/26/99	1200	3	ENABLED	LOW
HC0000	PARVAL	1100	LOW	1/26/99	1100	6	ENABLED	LOW
HC0001	PARVAL	800	LOW	1/26/99	800	2	DISABLED	LOW
HC0001	PALVAL	750	LOW	1/26/99	750	892	DISABLED	LOW

Figura 15 – Interface gráfica do software *ManagerMain* do *Toolkit* da *Control Art*.

Esse módulo armazena todos os documentos e configurações dos usuários em um banco de dados SQL, permitindo fácil acesso de qualquer um na planta.

O padrão EEMUA [9] recomenda configurações para os alarmes – uma distribuição de prioridades por equipamentos/funções e alarmes por controlador e por operador. Assim, é fácil checar quais sistemas atendem a essas recomendações, é fácil também determinar quais mudanças devem ter sido realizadas no sistema desde sua última configuração ajustada.

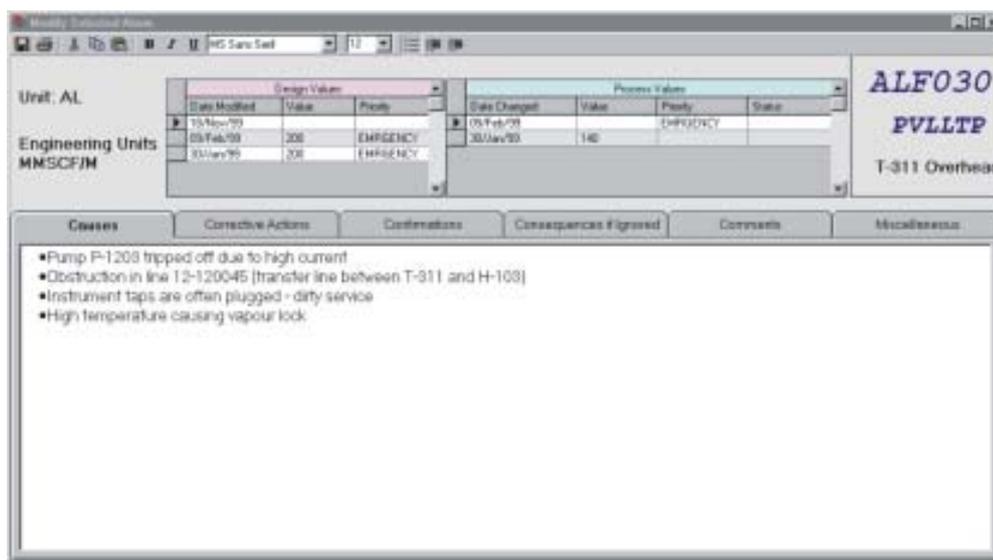


Figura 16 – Interface gráfica do software *ManagerModify* do *Toolkit* da *Control Art*.

* *AlarmAssistant* – sistema de apresentação dos alarmes que prove informações adicionais e configurações para o operador. Permite o acesso às configurações de projeto, seleção de alarmes, etc. tudo facilmente suportado.

Todo sistema DCS tem uma interface para apresentar alarmes, mas geralmente não é conectada a outras fontes de dados da planta – como documentação dos alarmes e suas medidas históricas. Tudo isso é apresentado em uma única interface, conforme apresentado na Figura 17.

A correta documentação possui valor inestimável durante falhas no sistema, mas também não ajuda se não estiver facilmente disponível para os operadores. O *AlarmAssistant* permite acesso imediato às documentações – um duplo clique em qualquer alarme e uma tela indicando as causas do alarme aparece, e também apresenta as ações corretivas, e qualquer outra informação que pode ser útil para o operador.

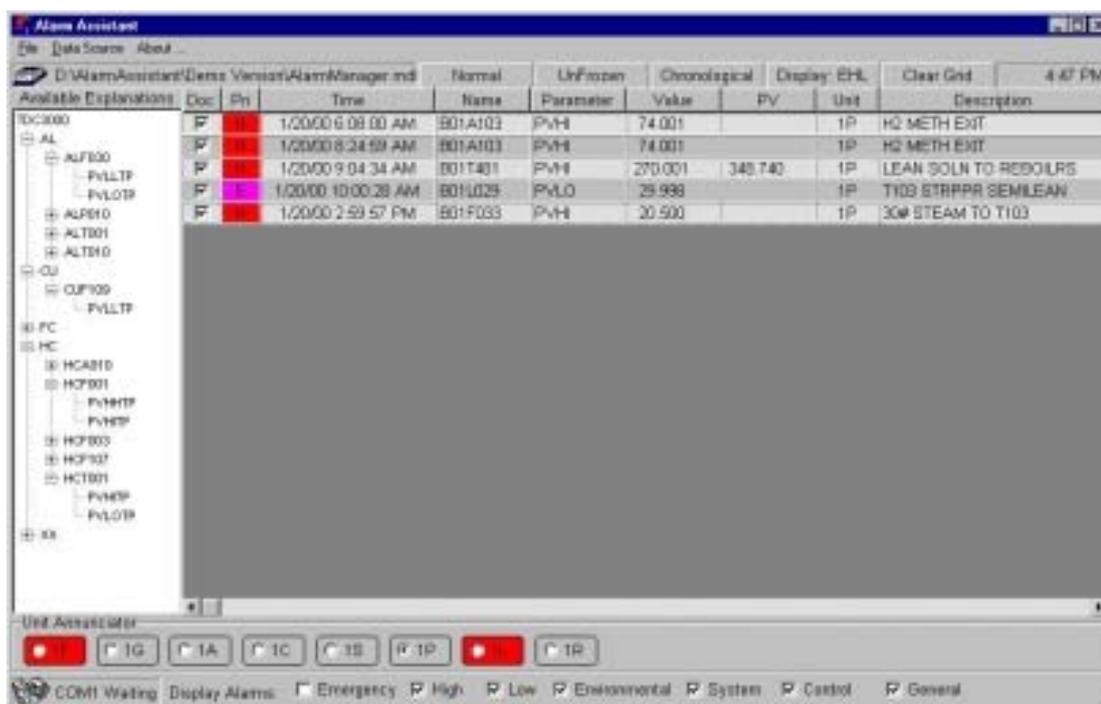


Figura 17 – Interface gráfica do software *AssistantMain* do *Toolkit* da *Control Art*.

* *AlarmInspector* – agenda relatórios das mudanças dos valores dos alarmes e de modificações ocorridas nesses alarmes.

* *AlarmEnforcer* – Mantêm o alarme em seu valor de projeto para longos períodos, e permite que o operador acerte sua configuração para atividades breves. Esse módulo compara a configuração corrente e a de projeto semanalmente, diariamente ou por escala de operação para assegurar que os alarmes nunca fiquem muito fora dos valores de projeto.

2.3.4.6 PAS - Process Automation Services

PAS [26] é uma empresa líder global em fornecimento de serviços de consultoria e desenvolvimento de softwares, localizada em Houston. Tem como grande cliente a Ameren – maior empresa de energia do Missouri e segunda maior de Illinois, que padronizou o *Alarm Management Optimization – Real-Time (AMO-Rt™)* nas suas mais de 30 plantas.

O software AMO-Rt inclui 7módulo para Análise de Alarmes e Eventos, Documentação e Racionalização, Auditoria e Manuseio de Alarmes. Somente esse software representou um crescimento de 124% nos seus negócios em 2006 [26].

2.3.4.7 EXIDA

EXIDA [27] foi fundada nos Estados Unidos com o objetivo de desenvolver sistemas de automação seguros e com alto nível de disponibilidade. Nos últimos anos, EXIDA tem desenvolvido pesquisas na área de sistemas seguros, publicando livros e artigos na área. Dentre esses livros, pode-se citar *Safety Integrity Levels* [36], esse livro foi escrito por parceiros da EXIDA, sendo publicado pela ISA. Descreve métodos sistematizados e técnicas para selecionar níveis de integridade de segurança para sistemas de instrumentos seguros (SIS - *Safety Instrumented Systems*). Descreve numerosos métodos utilizados pelas indústrias, enfatizando a camada de análise da proteção, que está tendo grande aceitação no mercado devido à fácil implementação com resultados bem precisos.

Com a evolução dos sistemas de controle distribuídos, um sistema de gerenciamento de alarmes tem se tornado cada vez mais importante nas plantas industriais, de modo a garantir que as metas de segurança e produtividades sejam atingidas.

O objetivo de sistemas de gerenciamento de alarmes eficientes é simples – efetivamente alarmar ou avisar o operador quando uma ação é requerida, segundo EXIDA.

Exida desenvolveu um sistema baseado em camadas para priorizar e racionalizar alarmes de processo, tendo como produto o *Alarm Management Solution*TM. Além de projetar um sistema eficiente, Exida apresenta indicativos de sistema de alarmes mal projetados, que são [27]:

- Pequenas paradas/interrupções geram grande número de alarmes;
- Alguns alarmes se mantêm ativos por longos períodos de tempo;
- Existem alarmes ativos quando nada está errado;
- Ocorrem alarmes que não requerem ação do operador;
- Operador não sabe o que fazer para certos tipos de alarmes.

2.3.4.8 HONEYWELL

Honeywell [28], empresa que participante do consórcio ASM [21] desenvolveu o AEGIS (*Abnormal Event Guidance and Information System*) [37], desenvolvido através do programa ATP (*Advanced Technology Program*) da NIST (*U.S. National Institute of Standards and Technology*) [38], voltado para indústrias petroquímicas. A Figura 18 [37] apresenta um modelo adotado pela ASM, que prove a descrição de como a equipe operacional de uma planta industrial responde intervindo em uma situação anormal [37].

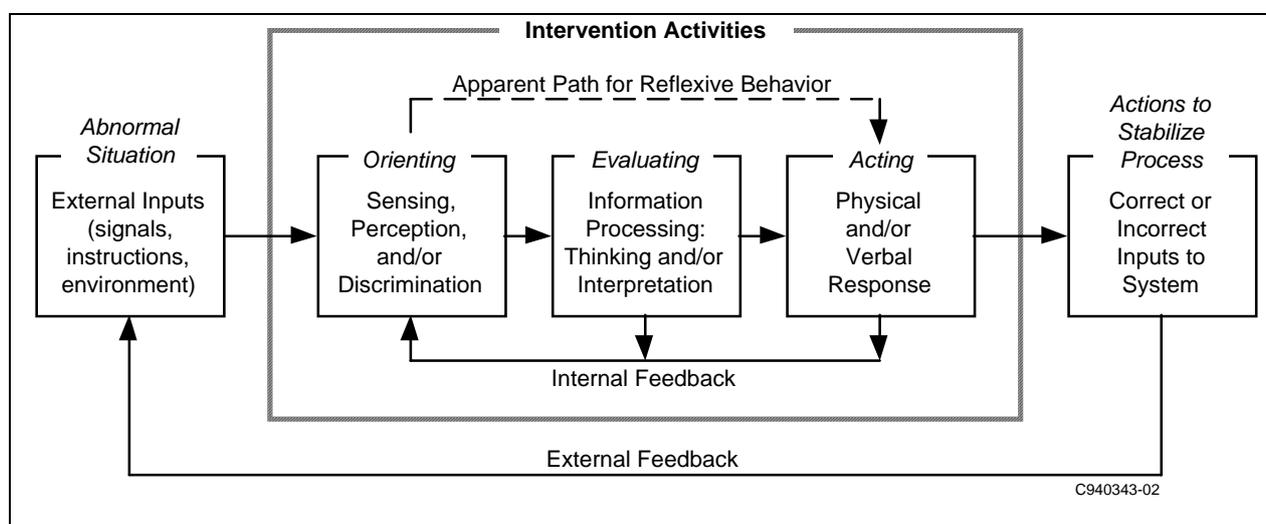


Figura 18 – Modelo de um Sistema de Suporte a Decisões para Intervenção em Operações Anormais adotado pelo ASM

O lado esquerdo representa a ocorrência de uma situação anormal externa, e a equipe representada pela caixa pontilhada, então intervêm para estabilizar o processo. Essa intervenção é dividida em três partes:

- Orientação – um distúrbio no processo é detectado;
- Avaliação – a equipe operacional desenvolve uma hipótese para a causa da condição anormal detectada, que pode ser pulada, para causas conhecidas;
- Ação – a equipe operacional realiza uma ação corretiva ou compensatória, incluindo ações que determinam se a hipótese está correta.

O propósito do AEGIS é suportar a equipe operacional da planta, de modo a atingirem os quatro objetivos definidos pelo ASM [37]:

- Manter o processo em operação normal;

- Falhando isso, restaurar o processo para operação normal;
- Falhando isso, trazer o processo para um estado ou condição segura;
- Falhando isso, minimizar a severidade de algum acidente ou perda de produção.

O AEGIS trabalha com seis papéis funcionais, conforme apresentado na visão da Figura 19 [37]. Esses papéis são:

- Estimador do Estado (*state estimator*) - fornece uma estimativa dinâmica e concisa do que esta acontecendo realmente na planta, incluindo informações de tendências que podem ser utilizadas para predizer os estados futuros;
- Apontador do objetivo (*goal setter*) - examina o resultado e propõe ações prioritizadas em função de objetivos que necessita perseguir;

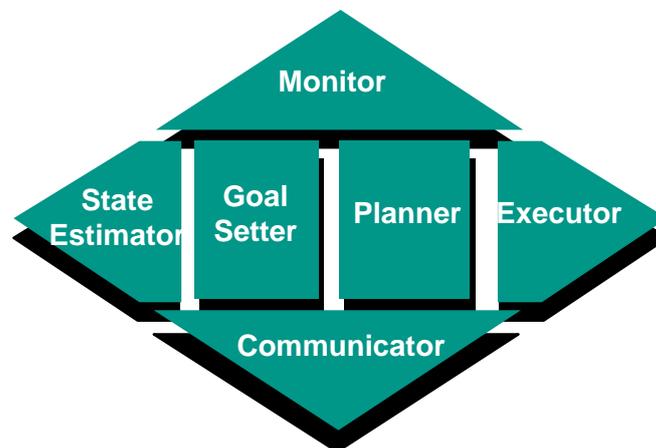


Figura 19 – Papéis Funcionais do AEGIS

- Planejador (*planner*) - cria um plano para conseguir atingir os objetivos, a partir do estado atual da planta;
- Executor (*executor*) – realiza o plano, assegurando-se de que cada etapa esteja sendo corretamente executada;
- Comunicador (*communicator*) - controla a relação entre os outros papéis e o pessoal de planta;
- Monitor (*monitor*) - examina a operação dos outros papéis e regula suas atividades.

O AEGIS foi desenvolvido e testado em quatro etapas distintas, usando uma arquitetura aberta de modo que suas principais funções (estimador de estados, interface com usuário, modelos, gerenciamento de dados...) podem ser facilmente incorporadas e/ou

interagir com sistemas existentes. O atual protótipo está em uso em plantas da Exxon, Mobil e Union Carbide Corporation.

2.3.4.9 UFCG (Universidade Federal de Campina Grande) e CHESF (Companhia Hidro Elétrica do São Francisco)

A UFCG em conjunto com a CHESF desenvolveu um sistema de software, baseado em técnicas de Inteligência Artificial, para o tratamento on-line de alarmes [39] [40]. Esse sistema realiza o diagnóstico das causas dos alarmes, avalia sua dimensão e localização, propondo um conjunto de ações a serem tomadas, no menor tempo possível. Para isso, utiliza-se técnicas de sistemas baseados em conhecimento para processar e recomendar ações.

O domínio de aplicação desse sistema refere-se a sistemas de distribuição de energia, e busca minimizar o impacto social e econômico quando da ocorrência de alguma anormalidade no sistema, reduzindo o tempo de solução do problema e retorno à condição segura.

Atualmente a UFCG está desenvolvendo um Sistema de Apoio à Decisão da Operação de Sistemas Elétricos -- SAD --, cujo objetivo é fornecer à operação, em tempo real, acesso fácil e rápido às informações que são relevantes aos fatores críticos de sucesso dos operadores. O SAD deverá cumprir os seguintes requisitos: o localizar, extrair e filtrar, de diversas fontes de dados, dados importantes para a atuação dos operadores em situações de contingência; apresentar a informação de forma concisa e relevante.

2.4 Considerações Finais

O grande avanço acontecido na automação das plantas industriais deveu-se ao impulso para alcançar a Excelência Operacional, criando a necessidade de uma gerência mais eficaz dos alarmes. As plantas estão operando cada vez mais perto de seus limites máximos, e os usuários estão procurando continuamente novas maneiras para obter a Excelência Operacional, aumentando a produtividade e reduzindo perdas operacionais. As estratégias eficazes para gerenciamento do alarme são componente chave na busca

destes objetivos, pois ajudam a minimizar perdas operacionais, oriundas de falhas em equipamentos sem diagnóstico, bem como assegurando um retorno mais rápido à condição operacional, reduzindo o tempo de parada. A Figura 20 [4] apresenta essa relação, apresentando junto com a função de gerenciamento de alarmes, ferramentas consagradas de otimização de processos, como Six Sigma e PDCA.

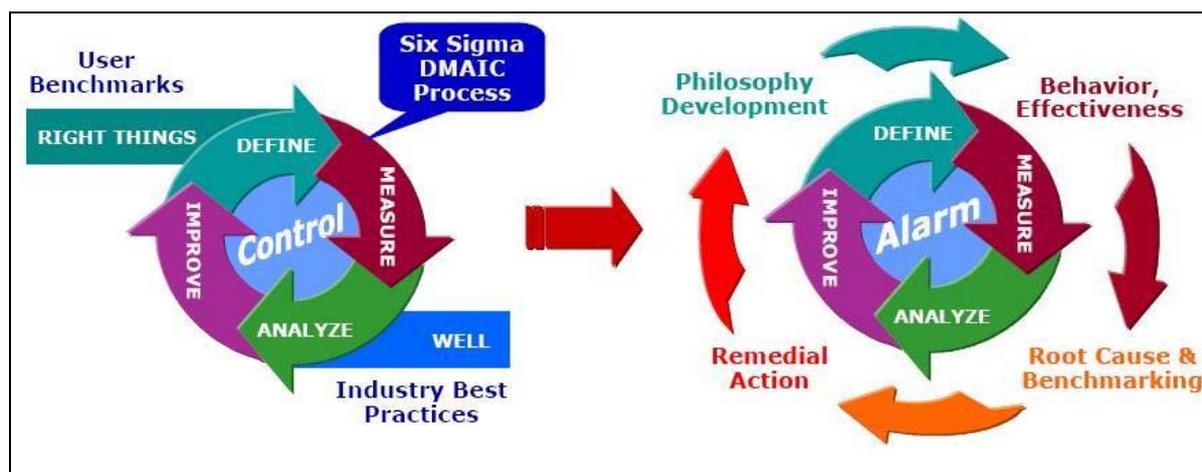


Figura 20 – A correlação entre a Excelência Operacional e o Gerenciamento de Alarmes

Na busca então da excelência operacional, propõem-se uma nova modelagem para Gerenciamento de Alarmes, baseando-se nos estudos apresentados. A partir de todos os princípios estudados, tem-se que uma configuração ótima é uma onde a característica de desempenho do controle do processo, alarmes, e mensagens atingem os objetivos operacionais requeridos.

Define-se primeiro que o sistema de Gerenciamento de Alarmes deve apresentar ao operador alarme com um significado claro e relevante, e que todo alarme deve ter uma resposta definida.

Além dessa característica, outras mais, incluindo funções e configurações também devem estar presentes, conforme se apresenta na Tabela 3, apresentada a seguir.

É claro que para cada planta industrial o sistema de gerenciamento de alarmes deve ser devidamente adequado às suas necessidades, mas os princípios e funções apresentados são considerados gerais, atendendo grande parte da necessidade dos sistemas conhecidos.

3. .PRINCIPAIS TÉCNICAS DE FILTRAGEM E RECOMENDAÇÃO

O objetivo geral desse capítulo é apresentar os principais métodos de clusterização, para aplicação em atividades de filtragem de informação, fornecendo assim embasamento para aplicar essas técnicas na determinação de grupos de modelos de usuários com interesses similares.

O capítulo está organizado em seções, sendo apresentados na Seção 3.1 métodos de clusterização, na Seção 3.2 as principais técnicas de filtragem e recomendação, apresentando filtragem e recomendação baseada em conteúdo e colaborativa. Na Seção 3.3 será realizada uma discussão da aplicação de técnicas de clusterização e filtragem em grupos de usuários, realizando-se um estudo de casos e finalmente na Seção 3.4 as considerações finais sobre esse capítulo.

3.1 Métodos de Clusterização

Sob o ponto de vista da mineração de dados, pode-se também conceituar Clusterização como a divisão dos dados em grupos de objetos similares. Cada grupo chamado cluster, consiste de objetos que são similares entre si e diferentes dos objetos dos outros grupos. Representando dados através de poucos clusters necessariamente perde-se precisão nos detalhes mais finos, mas atinge-se simplificação. Modelagem de dados coloca clusterização em uma perspectiva histórica próxima à matemática, estatística e análise numérica. Da perspectiva de aprendizagem de máquina, cluster corresponde aos padrões escondidos, a busca dos clusters é uma aprendizagem não supervisionada, e o sistema resultante representa um conceito de dados.

Entretanto, clusterização é uma aprendizagem não supervisionada de conceitos de dados escondidos. Mineração de dados lida com banco de dados extensos com atributos diversos, que impõem à análise da clusterização severos requerimentos computacionais adicionais [41].

A análise de dados é a razão principal de muitas aplicações de computação, tanto na fase de projeto como durante sua operação. Procedimentos de análise de dados podem ser opostos, exploratórios ou confirmatórios, baseados na disponibilidade de modelos

apropriados para a fonte de dados; mas um elemento chave em ambos os procedimentos (tanto para formação de hipóteses ou formação de opinião) é o grupo, ou a classificação das medidas baseadas no enunciado de um modelo adequado, ou em um agrupamento natural (clusterização) revelado através de análises.

Análise de cluster é a organização de uma coleção de padrões (usualmente representados como um vetor de medidas, ou um ponto em um espaço multidimensional) em clusters baseados na similaridade. Intuitivamente, padrões em clusters válidos são mais similares entre eles do que seriam se eles pertencessem a diferentes clusters. Na Figura 21 [42], tem-se os padrões de entrada na Figura 21 (a), e o cluster desejado na Figura 21 (b). Para os pontos que pertencem ao mesmo cluster associa-se o mesmo número.

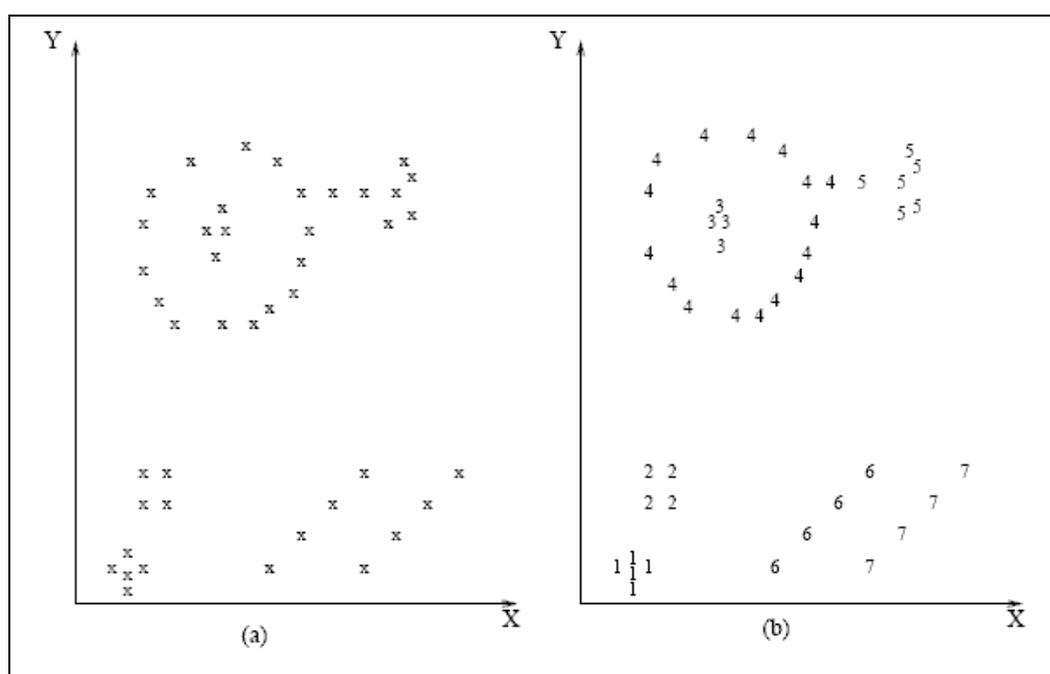


Figura 21 – Clusterização de dados.

A variedade de técnicas para representar dados, medições de proximidade (similaridade) entre elementos e agrupamento de elementos de dados tem produzido um rico e quase sempre confuso agrupamento de diferentes métodos de clusterização [43] [44].

É importante entender a diferença entre clusterização (classificação natural, não supervisionada) e análise discriminativa (classificação supervisionada). Em classificação supervisionada, pode-se fornecer uma coleção de padrões rotulados (pré-classificados); o

problema é rotular os padrões recentemente encontrados, ainda não rotulados. No caso de clusterização, o problema é agrupar uma coleção de padrões não rotulados dentro de clusters significativos. Rótulos são associados com Clusters também, mas rótulos de categorias são dados controlados, obtidos diretamente dos dados.

Clusterização é útil em vários padrões de análise exploratória, agrupamento, algoritmos para tomada de decisão, algoritmos para aprendizagem de máquina, incluindo mineração de dados, recuperação de documentos, segmentação de imagem, padrão de classificação, e principalmente para *Modelagem de Usuários*, *Filtragem Colaborativa* (Modelagem de Usuários) e *Filtragem Baseada em Conteúdo* (Modelos de Grupos de Documentos que satisfaçam um determinado perfil de usuários e/ou grupo de usuários).

Entretanto, em muitos problemas, a informação disponível sobre os dados é escassa (modelos estatísticos), e algoritmos tomadores de decisão têm que se basear em dados que considera verdadeiro, mesmo sem ter certeza. É baseado nessas restrições que métodos de clusterização são particularmente apropriados para exploração de relações entre pontos de dados fazendo um julgamento (talvez preliminar) da sua estrutura.

O termo “clusterização” é usado em muitas comunidades de pesquisa para descrever métodos para agrupamento de dados não rotulados. Essas comunidades possuem diferentes terminologias e avaliações para os componentes de um processo de clusterização e o contexto no qual o cluster é utilizado. Assim, para um melhor entendimento, os principais termos e técnicas que se irá abordar serão descritos e conceituados (sucintamente) nesse capítulo.

Uma das formas de se realizar a Filtragem da Informação em Sistemas de Recomendação é através da Clusterização, que permite agrupar a base de dados em clusters ou grupos com graus de similaridade conhecidos. Assim, obtendo-se o perfil do usuário, basta confrontá-lo com os clusters obtidos para se realizar a recomendação.

Atualmente se está presenciando o crescimento e a abundância desordenada de informação, surgindo a necessidade de se desenvolver sistemas que auxiliem o usuário a lidar com esta sobrecarga de informação. Sobrecarga de informação é definida como a dificuldade em se encontrar informação relevante em tempo hábil, dada a grande disponibilidade de informação minimamente organizada.

Sistemas de Filtragem de Informação ajudam os usuários a selecionar informações que realmente lhe sejam relevantes. Como os interesses dos usuários variam muito, estes

sistemas precisam ser altamente personalizados para satisfazer os interesses individuais de cada usuário.

Um sistema de filtragem de informação personalizado deve preencher as seguintes exigências: especialização, adaptação e exploração [45]. Um sistema é especializado quando é capaz de satisfazer os interesses específicos do usuário, selecionando a informação relevante e eliminando a irrelevante. A adaptação é necessária devido ao caráter dinâmico dos interesses do usuário, cabendo ao sistema notar esta mudança e adaptar seu comportamento em resposta a ela. Por fim, um sistema deve ser capaz de explorar novos domínios de informação com o objetivo de encontrar informação de potencial interesse para o usuário.

Os sistemas de filtragem de informação visam satisfazer as necessidades de informação de um usuário poupando-lhe tempo e esforço. Essas necessidades de informação, ou interesses dos usuários, constituem os chamados perfis (*profiles*). Estes perfis poderão ser usados por agentes do sistema de filtragem com o intuito de garantir melhores resultados de busca por informação. Como os interesses dos usuários têm natureza dinâmica cabe aos agentes modificarem os perfis e se adaptarem às mudanças.

3.1.1 Medição de Similaridade

Desde que similaridade é fundamental para a definição de um cluster, a medida da similaridade entre dois desenhos de padrões de um mesmo atributo espacial é essencial para a maioria dos procedimentos de clusterização. Por causa da variedade de tipos e escalas de características, a medição da distância deve ser escolhida cuidadosamente. É muito comum calcular a falta de semelhança entre dois padrões usando a medida da distância definida em um espaço característico. Será focado as medições de distâncias bem conhecidas utilizadas para padrões para os quais os atributos são contínuos.

3.1.1.1 Distância Euclidiana

A métrica mais popular para “atributo contínuo” é a “Distância Euclidiana”:

$$d_2(\mathbf{x}_i, \mathbf{x}_j) = \left(\sum_{k=1}^d (x_{i,k} - x_{j,k})^2 \right)^{1/2} = \|\mathbf{x}_i - \mathbf{x}_j\|_2,$$

Equação 1 – Distância Euclidiana

A qual é um caso especial (onde se tem $p=2$) da métrica Minkowski.

$$d_p(\mathbf{x}_i, \mathbf{x}_j) = \left(\sum_{k=1}^d |x_{i,k} - x_{j,k}|^p \right)^{1/p} = \|\mathbf{x}_i - \mathbf{x}_j\|_p.$$

Equação 2 - Métrica Minkowski

A distância Euclidiana apresentada na Equação 1 é mais intuitiva e é comumente utilizada para avaliar a proximidade de objetos em duas ou três dimensões espaciais. Trabalha bem quando os dados são clusters "compactos" ou "isolados". Métricas de Minkowski apresentada na Equação 2 são indicadas para atributos de grande escala que dominam as outras. Solução para esse problema inclui a normalização contínua de atributos (para uma faixa ou variação comum) ou outro esquema de atribuição de pesos.

Correlação linear entre características pode distorcer medidas de distância; essa distorção pode ser avaliada aplicando uma transformação dos dados ou utilizando a distância quadrada de Mahalanobis:

$$d_M(\mathbf{x}_i, \mathbf{x}_j) = (\mathbf{x}_i - \mathbf{x}_j) \Sigma^{-1} (\mathbf{x}_i - \mathbf{x}_j)^T,$$

Equação 3 – Distância Quadrada de Mahalanobis

Onde os padrões " x_i " e " x_j " são assumidos como vetores de linha, e Σ é a amostra da matriz de covariância dos padrões ou matriz de padrão de processos de geração; $d_M(,)$ atribui diferentes pesos para diferentes características baseadas nas suas variâncias e correlações. Aqui, assume-se implicitamente que as densidades condicionais das classes são uni modais e caracterizadas por densidade Gaussianas multivariadas. A distância regularizada de Mahalanobis foi usada por muitos outros autores para extrair clusters elipsoidais.

Alguns algoritmos de clusterização trabalham com uma matriz de valores aproximados ao invés do conjunto padrão originais. É útil para as situações que se tem que computar todos os pares de valores de distância $n(n-1)/2$, para os "n" padrões e armazenar eles em uma matriz simétrica. Computar a distância entre padrões com alguns ou todos os atributos sendo não contínuos é problemático, desde que diferentes tipos de características não são comparáveis e (como um exemplo extremo) a noção de proximidade é efetivamente em escala binária de características. Estudiosos desenvolveram medidas de proximidade para tipos heterogêneos de padrões. Um exemplo recente é Wilson e Marinez [46], que propuseram uma combinação de uma modificação da métrica de Minkowski para atributos contínuos e baseados na distância em contagens (população) para atributos nominais. Uma variedade de outras métricas tem sido reportada para computar similaridade entre padrões representados usando atributos tanto quantitativo quanto qualitativos.

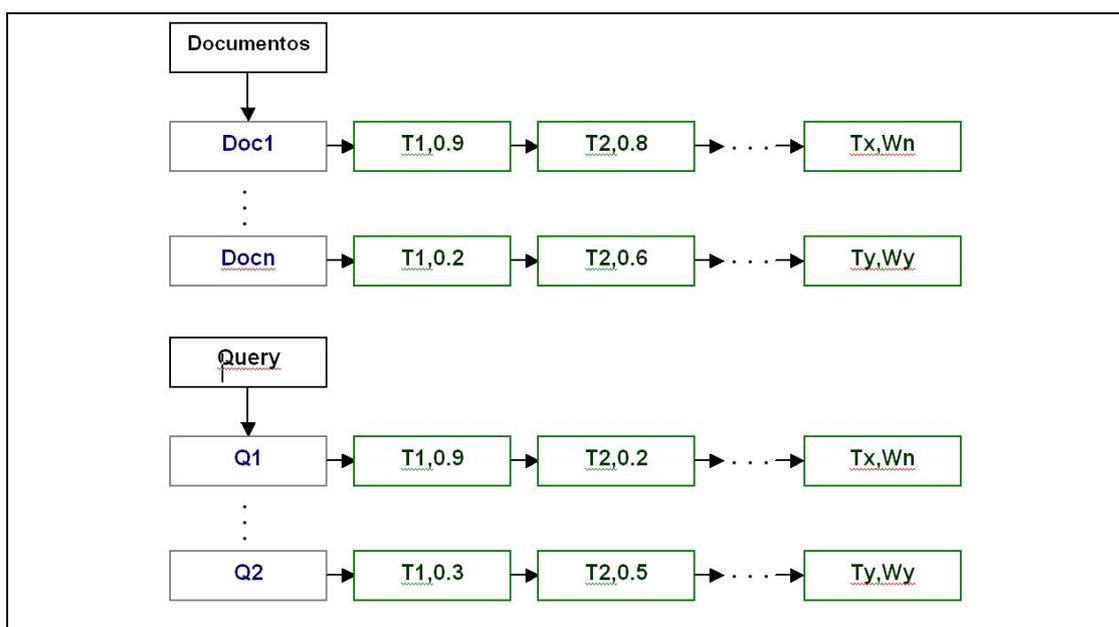


Figura 22 – Representação dos Documentos e Consultas por Vetores de Pesos.

3.1.1.2 Espaço Vetorial

Outra técnica de medição de similaridade é o modelo Espaço Vetorial, que foi desenvolvido por Geraldo Salton para ser utilizado no Sistema de Recuperação de Informação chamado SMART. Este modelo propõe um ambiente em que cada documento

é visto como um vetor de termos, e para cada termo associa-se um grau de importância (peso) deste no documento, ou seja, cada documento possui um vetor de pesos associados na seguinte forma: $(t_1, w_1), (t_2, w_2), \dots, (t_n, w_n)$, onde t é o termo e w é o seu peso do documento. As consulta do usuário também são representadas por vetores de termos $(t_1, W_{q1}), (t_2, W_{q2}), \dots, (t_n, W_{qn})$, conforme Figura 22 [47].

Desta forma o vetor dos documentos pode ser comparado com o vetor da consulta e o grau de similaridade entre cada um deles pode ser identificado. Será suposto neste trabalho que já estão definidos o vetor de pesos do documento e da consulta, e será então necessário encontrar a similaridade entre estes vetores.

Para esse trabalho irá se utilizar duas técnicas de similaridade: o **produto interno** e **cosseno**.

3.1.1.3 Produto Interno

O Produto Interno é dado pelas equações abaixo [47]:

$$\text{Similaridade}(Q, D) = \frac{\sum_{i=1}^n w_{qi} \cdot w_{di}}{dw}, \text{ sendo } dw = \sum_{i=1}^n w_{di}$$

Equação 4 - Fórmula de Similaridade Produto Interno

Onde se tem:

- Q= vetor de pesos da consulta
- D= vetor de pesos do documento
- W_{qi} = peso da consulta.
- W_{di} = peso do documento.

3.1.1.4 Cosseno

O cosseno é baseado em medida angular [47]:

$$\text{Similaridade de}(Q, D) = \frac{\sum_{i=1}^n w_{qi} \cdot w_{di}}{\sqrt{\sum_{i=1}^n (w_{qi})^2} \sqrt{\sum_{i=1}^n (w_{di})^2}}$$

Equação 5 - Fórmula de Similaridade do Cosseno

Onde se tem:

- Q= vetor de pesos da consulta
- D= vetor de pesos do documento
- W_{qi} = peso da consulta.
- W_{di} = peso do documento.

Padrões podem ser representados usando textos ou estrutura de árvore [48]. Textos são usados em clusterização sintática. Uma comparação das abordagens sintáticas e estatísticas para reconhecimento de padrões utilizando vários critérios é apresentada por Tanaka [49], e a conclusão foi que o método sintático é inferior em todos os aspectos.

3.2 Principais Técnicas de Filtragem e Recomendação

A Filtragem de Informação é o nome usado para descrever uma área de pesquisa que oferece técnicas para separar informações relevantes e irrelevantes, e a sua entrega para pessoas que precisem delas. A necessidade dessas informações pelas pessoas é de longo prazo. A filtragem é baseada na descrição de preferências de indivíduos ou grupos, denominado de *perfil*.

Os perfis podem ser adquiridos tanto de forma *explícita*, fornecido pelo usuário, como *implícita*, automaticamente através da captura do comportamento do usuário.

As principais características dos sistemas de filtragem de informação [50]:

- Um sistema de filtragem de informação é um sistema de informação projetado para fonte de informações dinâmicas. Ao contrário das tradicionais aplicações de banco de dados que trabalham com dados estruturados, tais como registros (funcionários, clientes, produtos etc.) com campos contendo tipos de dados com significados bem definidos.

- Sistemas de filtragem trabalham primariamente com informação textual. Dados textuais são usados como um sinônimo para dados não estruturados. Eles são mais gerais e incluem outros tipos de dados como imagens, voz e vídeo que são parte de sistemas de informação multimídia. Esses tipos de dados têm significados difíceis de representar e não são bem tratados por sistemas de banco de dados convencionais.
- Sistemas de filtragem envolvem grandes quantidades de dados. As aplicações lidam com grandes volumes de textos disponíveis em fontes diversas.
- Aplicações de filtragem envolvem tipicamente fluxos de dados *incoming* (dados que estão chegando), ou sendo transmitidos por fontes remotas (tais como serviços *newswire*) ou enviados diretamente por outras fontes (correio eletrônico). Filtragem descreve também o processo de acessar e recuperar informação de bases de dados remotas, neste caso os dados *incoming* são o resultado das buscas às bases de dados.
- Filtragem é baseada em descrições de preferências de informação de indivíduos ou grupos, freqüentemente denominados perfis. Tais perfis representam interesses *long-term* (são os termos que representam o interesse do usuário).
- Filtragem freqüentemente significa a remoção dos dados de um fluxo de entrada de dados, ao invés de encontrar dados nesse fluxo. No primeiro caso, os usuários do sistema vêem o que é deixado depois que os dados são removidos; no outro caso, eles vêem os dados que foram extraídos.

As principais técnicas de filtragem de informação são a Filtragem baseada no Conteúdo e a Filtragem Colaborativa, as quais serão apresentadas detalhadamente a seguir.

A aplicação da clusterização e das filtragens já apresentadas, tem como objetivo suportar sistemas de recomendação. Têm-se dois sistemas principais de recomendação, que são o Baseado em Conteúdo e Colaborativos. Serão apresentados agora os pontos fortes e as fraquezas e deficiências de cada técnica.

3.2.1 Filtragem e Recomendação Baseada em Conteúdo

A Filtragem Baseada em Conteúdo [51] baseia-se em informações obtidas através da análise do conteúdo dos itens de informação pelos quais o usuário demonstrou

preferência no passado, ou seja, um item será recomendado se este item é similar a outro que o usuário preferiu no passado.

Para fazer a recomendação os sistemas que utilizam essa abordagem inicialmente tentam “entender” padrões de preferências existentes nos itens previamente avaliados pelo próprio usuário, criando assim um perfil.

Um perfil é composto por termos ou palavras-chave e pesos associados. O peso indica a maior “importância” de uma palavra na recomendação. De maneira semelhante, para cada item de informação são configurados perfis de representação, contendo os termos considerados mais importantes destes itens.

Faz-se então um *matching* entre o perfil do usuário e os documentos, ou seja, através da análise de similaridade entre os documentos com o perfil do usuário e então os mais similares são recomendados.

A filtragem Baseada em Conteúdo é muito utilizada na recomendação de textos, como artigos, notícias, etc.

A técnica de sistemas de recomendação baseados no conteúdo tem suas raízes na comunidade de Recuperação de Informação, e aplicam-se muitas das mesmas técnicas. Documentos de texto são recomendados baseados em uma comparação entre seu conteúdo e o perfil do usuário. Estruturas de dados de ambos são criadas utilizando-se atributos extraídos do documento de texto. Frequentemente alguns esquemas de pesos são utilizados de forma a discriminar algumas palavras – evidenciando as palavras chaves e as que ocorrem com mais frequência. Quando se apresentar uma página para um usuário, pode-se ter um retorno sobre suas preferências [52]. Se o usuário gostar da página, pesos para as palavras extraídas dela podem ser adicionados para as palavras correspondentes de seu perfil. Esse processo é conhecido como retorno de relevâncias. Além de ser simples e rápido, sabe-se empiricamente que melhora os resultados em ajustes de recuperação de informação [53].

Aplicações industriais e acadêmicas comparam os sistemas de recomendação Baseados em Conteúdo e Colaborativos. Para uma melhor comparação tem-se que definir de maneira clara os sistemas. Considera-se um sistema de recomendações baseado em conteúdo “puro” quando a recomendação é feita baseando-se somente no perfil construído através da análise de conteúdo dos itens que o usuário avaliou no passado – cada usuário é tratado em separado. Exemplos de sistemas com esses atributos são

InfoFinder [54], NewsWeeder [55] e sistemas desenvolvidos para tarefas de roteamento da conferência TREC [56].

Um sistema de recomendação baseado em conteúdo puro possui diversas falhas. Em geral, somente uma análise superficial de certos tipos de conteúdos pode ser fornecida. Em alguns domínios os itens do conteúdo não são compatíveis com as técnicas de extração mais modernas. Mesmo para documentos de textos a captura de representações ocorre somente para certos aspectos, e existem muitos outros que poderiam influenciar a experiência do usuário. Tem-se o problema da super especialização. Quando o sistema recomenda somente itens ranqueados de acordo com o perfil do usuário, o usuário é restringido a ver somente itens semelhantes aos já avaliados por ele. Finalmente, avaliação de documentos é uma tarefa onerosa para o usuário, então quanto menos avaliação melhor. Em sistemas de recomendação baseada em conteúdo puro a avaliação do usuário é o único fator que influencia performances futuras, de modo que não se consegue ver como se pode reduzir a quantidade sem também reduzir o desempenho [52].

3.2.2 Filtragem e Recomendação Colaborativa

Filtragem Colaborativa [57] [58] [59] pode ser explicada a partir de Sistemas de Recomendação, utilizados em livrarias, lojas e sites da internet. Lojas em geral mantêm banco de dados com registro de quem comprou o que. Esses registros podem ser usados para prever as futuras compras que os clientes possam desejar. Essas predições não se limitam somente à compra, podem ser utilizados para indicação de filmes, CD's, comida, passeios, etc.

Esses sistemas de recomendação são geralmente baseados em Filtragem Colaborativa, desde que a seleção dos itens seja feita utilizando um método que a partir da colaboração de um indivíduo (que pertença a um grupo) possa fazer recomendações aos seus amigos (que pertençam ao mesmo grupo). Essa análise de cada compra realizada ou preferência permite, realmente, uma detalhada segmentação do mercado. Consumidores podem ser agrupados em grupos de cinco ou dez – ou mesmo individualmente, tendo seus gostos modelados, e o mercado customiza vendas para eles.

Problemas reais são mais complexos do que é sugerido por uma simples lista de filmes preferidos. Pessoas e filmes possuem atributos. Pessoas têm uma idade, um sexo, uma origem e nacionalidade. Filmes têm diretores e atores, os quais têm seus próprios atributos.

A abordagem para recomendação colaborativa é muito diferente da recomendação baseada em conteúdo: raramente se recomenda itens porque são similares aos itens que o usuário gostou no passado, recomendam-se itens que outros usuários similares gostaram no passado. Raramente computa-se a similaridade dos itens, e sim a similaridade dos usuários. Tipicamente, para cada usuário um conjunto de “vizinhos mais próximos” que são encontrados baseando-se nas avaliações passadas. Pontuações para itens ainda não vistos podem ser previstas baseados na combinação das pontuações dos vizinhos mais próximos [52].

Da mesma forma que se define um sistema de recomendação puro para sistemas baseados em conteúdo, far-se-á o mesmo para sistemas de recomendação colaborativos. Um sistema de recomendação colaborativo é um que não faz nenhuma análise geral no item diretamente. Recomendação para usuários é feita somente com base na similaridade com outros usuários. Exemplos desses sistemas são o “*GroupLens*” [60], “*the Bellcore video recommender*” [51] e “*Ringo*” [41].

3.3 Discussão da Aplicação de Clusterização e Filtragem em Grupos de Usuários

Das técnicas de Clusterização estudadas, citam-se algumas que se aplicam tanto a Filtragem Baseada em Conteúdo, como também em Filtragem Colaborativa. O ponto principal quando se fala de Clusterização é que não existe um método ou roteiro fixo para se realizar uma determinada clusterização. Para cada domínio tem-se que checar qual método é mais adequado, e conhecendo o domínio e o propósito, defini-se também se será Filtragem Baseada em Conteúdo ou Colaborativa.

A Tabela 4 apresenta os tipos de Filtragem, o que as caracteriza, seu objeto, vantagens e desvantagens e um exemplo, para melhor entendimento [51]:

Tabela 4 – Tipos de Filtragem e suas principais características

	Filtragem Baseada em Conteúdo	Filtragem Colaborativa
Objeto de Modelagem	Modelos de Grupo de Documentos que satisfazem o perfil de um Usuário ou de um Grupo de Usuários.	Modelagem de Usuário – gera modelos de grupos de usuários com interesses similares.
Técnicas de Recomendação baseadas na Modelagem mais utilizadas	<ul style="list-style-type: none"> • Clusterização; • Redes Bayesianas; • Árvores de Decisão; • Inteligência Artificial; • Redes Neurais. 	<ul style="list-style-type: none"> • Clusterização; • Redes Bayesianas; • Inteligência Artificial; • Redes Neurais; • Regressão Linear; • Modelos Probabilísticos.
Vantagens	<ul style="list-style-type: none"> • Precisão independente do número de usuários. • Possibilidade de recomendar itens novos. • Esparsividade não é problema. • Bons resultados para usuários incomuns. 	<ul style="list-style-type: none"> • Independência do conteúdo. • Baseado na qualidade e gostos. • Descoberta de novos relacionamentos entre usuários. • Recomendações de itens diretamente relacionados ao histórico.
Falhas /Limitações	<ul style="list-style-type: none"> • Formato do conteúdo. • Superespecialização. • Não distingue Qualidade e Gostos. • Novo usuário (perfil inicia vazio). • Dificuldade na definição da representação dos documentos. • Dificuldade na definição de um perfil efetivamente representativo em relação às preferências do usuário. 	<ul style="list-style-type: none"> • Novo Item. • Novo usuário (perfil inicia vazio). • Insuficiência de usuário. • Esparsividade. • Escalabilidade. • Ovelha negra.

3.3.1 Estudo de Caso usando Filtragem Baseada em Conteúdo

A partir das técnicas e métodos apresentados, serão aplicados os conhecimentos de Clusterização com Filtragem Baseada em Conteúdo, em um caso real.

O caso real consiste em um Sistema de Supervisão e Controle Automatizado dos Viradores de Vagões da Vale, planta de São Luis – Terminal Marítimo Ponta da Madeira, apresentado na Seção 2.2.

Esse sistema é composto por três estações de operação (além de dezenas de outros componentes, os quais não interessam para esse trabalho) que geram cada uma um arquivo de Eventos e Alarmes. O número de registros e as informações contidas neles são muito grande, o que gera dúvidas nos operadores principalmente em casos de pane, quando um grande volume de dados é gerado em um espaço de tempo muito curto, e o operador necessita tomar uma decisão.

A proposta desse trabalho pode ser vista na Figura 23, onde a partir de um arquivo de Eventos e Alarmes “consolidado” (essa consolidação deve ser realizada à parte, suprimindo os registros comuns), realizar uma Clusterização para uma Filtragem Baseada em Conteúdo desse repositório de dados, conforme descrito na Seção 3.2.1, cujas atividades são:

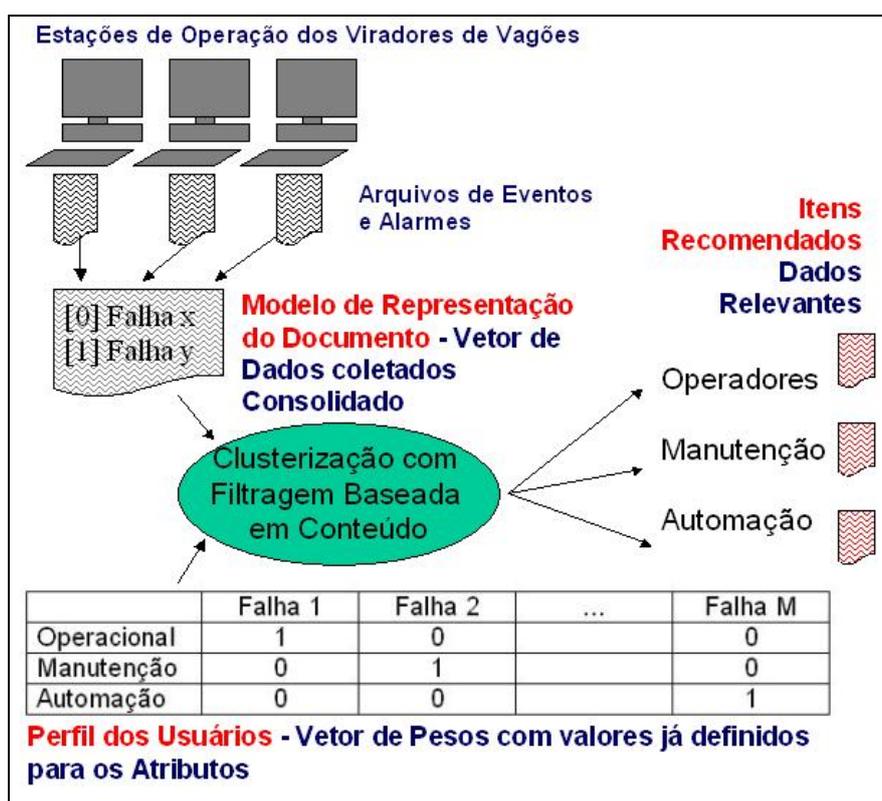


Figura 23 – Aplicação prática das Técnicas de Clusterização e Filtragem Baseada em Conteúdo.

- 1) Representação de padrões (incluem opcionalmente características de extração e/ou seleção);

- 2) Definição de padrões de medição de proximidade apropriados para os dados do domínio;
- 3) Clusterização e agrupamento;
- 4) Abstração de dados (se necessário);
- 5) Julgamento dos resultados (se necessário).

Desenvolvimento

A representação dos perfis será explícita, com o preenchimento de uma tabela, onde serão definidos pesos/valores para os atributos, que são apenas 6 (para análise nesse trabalho). Tem-se então o Vetor de Pesos da Consulta apresentado na Tabela 5.

Tabela 5 – Vetor de Pesos da Consulta

	Giro	Grampos	Braço	Seleção	Sirene	Status
Operacional	1	1	1	1	1	
Manutenção				1	1	1
Automação				1		1

Para o repositório de dados (arquivo de Eventos e Alarmes Consolidado) será montado um perfil com o vetor de pesos em função dos atributos escolhidos. Será obtido então parte do repositório de dados na Tabela 6.

Tabela 6 – Trecho do Repositório de Dados

18/07/06,12:24:00,33,ON,CMD - Giro do Virado
18/07/06,12:24:00,25,FUNZIONANDO,Grampos - STATUS LEI
18/07/06,12:24:01,33,OFF,CMD - Giro do Virador
18/07/06,12:24:02,26,LIGAR M28,Giro do Virador - CM
18/07/06,12:24:02,26,FUNZIONANDO,Ventilador Giro - ST
18/07/06,12:24:04,26,OFF,M28,Giro do Virador – CM

Atribuindo pesos em função da ocorrência dos atributos aos dados acima, tem-se o vetor de pesos do Documento apresentado na Tabela 7:

Tabela 7 – Vetor de Pesos do Documento

	Giro	Grampos	Braço	Seleção	Sirene	Status
18/07/06,12:24:00,33,ON, CMD - Giro do Virado	1					
18/07/06,12:24:00,25,FUNCIONANDO, Grampos - STATUS		1				1
18/07/06,12:24:01,33,OFF, CMD - Giro do Virador	1					
18/07/06,12:24:02,26,LIGAR M28, Giro do Virador - CM	1					
18/07/06,12:24:02,26,FUNCIONANDO, Ventilador Giro - STATUS	1					1

A técnica de medição de proximidade será a análise de Similaridade do Cosseno e do Produto Interno, para as quais serão comparadas as respostas. Para exemplificar, serão realizados os cálculos com o Vetor de Pesos da Consulta – Q1, representado na Tabela 8 e o Valor de Pesos dos Documentos – D1, representado na Tabela 9.

Tabela 8 – Vetor de Pesos da Consulta Q1

	Giro	Grampos	Braço	Seleção	Sirene	Status
Operacional	1	1	1	1	1	

Tabela 9 – Vetor de Pesos do Documento D1

	Giro	Grampos	Braço	Seleção	Sirene	Status
18/07/06,12:24:00,25, FUNCIONANDO, Grampos - STATUS		1				1

Calculando a similaridade entre o vetor de pesos da consulta e do documento (produto interno) conforme Equação 4, tem-se:

$$\text{Similaridade (Q,D)} = \frac{(1*0) + (1*1) + (1*0) + (1*0) + (1*0) + (0*1)}{0 + 1 + 0 + 0 + 0 + 1}$$

$$\text{Similaridade (Q,D)} = \frac{0 + 1 + 0 + 0 + 0 + 0}{2}$$

$$\text{Similaridade (Q,D)} = 0,5$$

Calculando a similaridade entre o vetor de pesos da consulta e do documento (Cosseno) conforme Equação 5, tem-se:

$$\text{Similaridade (Q,D)} = \frac{(1*0) + (1*1) + (1*0) + (1*0) + (1*0) + (0*1)}{\sqrt{(1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 0^2)} * \sqrt{(0^2 + 1^2 + 0^2 + 0^2 + 0^2 + 1^2)}}$$

$$\text{Similaridade (Q,D)} = \frac{0 + 1 + 0 + 0 + 0 + 0}{\sqrt{(1 + 1 + 1 + 1 + 1 + 0)} * \sqrt{(0 + 1 + 0 + 0 + 0 + 1)}}$$

$$\text{Similaridade (Q,D)} = \frac{1}{\sqrt{5} * \sqrt{2}}$$

$$\text{Similaridade (Q,D)} = 0,31622..$$

No exemplo mostrado, tem-se apenas um valor calculado. Realizando-se os mesmos cálculos para todos os registros de D, se obtêm uma lista ordenada (vetor) com seus respectivos graus de relevância para a consulta Q. Se for definido um valor mínimo para Similaridade (por exemplo, 0,5] e avaliado as técnicas, tem-se que para a técnica do Cosseno D1 não seria apresentado aos operadores, e para a técnica do Produto interno, D1 seria apresentado aos operadores.

Pseudocódigo - Para a correta implementação desse método, o Pseudocódigo utilizado nesse trabalho é:

- 1) Definir o universo de termos (atributos/falhas), $M = 6$.
- 2) Determinar as minhas entradas
 - a. Vetor de pesos dos atributos/falhas da consulta (tabela de pesos)
 - b. Vetor de pesos dos dados do documento (arquivo de eventos e alarmes consolidado).
- 3) Calcular a similaridade através do produto interno e co-seno.
- 4) Montar três listas ordenadas com falhas relevantes, apresentando-as para Operadores, Manutenção e Automação.

3.3.2 Considerações sobre Técnicas de Filtragem e Recomendação Clássicas

Clusterização é um processo de agrupamento de dados baseados na medida de similaridade, sendo um processo subjetivo: o mesmo conjunto de dados pode ser dividido de formas diferentes por diferentes aplicações. Essa subjetividade faz a clusterização ser de difícil execução. Isto porque um algoritmo ou técnica de clusterização não é adequado para resolver todos os problemas. Não existe nenhuma técnica de clusterização que seja universalmente aplicável para descobrir a variedade de estruturas presentes em um conjunto de dados multidimensionais. Por exemplo, considere os dados bidimensionais apresentados na Figura 21 (a). Nem todas as técnicas de clusterização podem descobrir todos os clusters presentes com igual facilidade, porque os algoritmos de clusterização freqüentemente contem suposições implícitas sobre a forma do cluster ou configuração básica de múltiplos clusters baseados em medições de similaridade e critérios de agrupamento utilizados.

Todas as técnicas de Filtragem e Recomendação estudadas apresentam vantagens e desvantagens, e a sua escolha deve ocorrer em função do domínio em que se deseja trabalhar.

Os sistemas de Recomendação [51] [61] [62] têm o objetivo de fornecer recomendações baseadas em informações registradas sobre as preferências dos usuários. As preferências dizem respeito a quaisquer itens de interesse do usuário como um livro, uma música, um restaurante ou um filme.

As preferências dos usuários são geralmente armazenadas através de perfis, representados por *avaliações* – explícitas ou implícitas – ou *palavras-chave* extraídas de textos lidos no passado.

Segundo Burke [61] um Sistema de Recomendação deve possuir:

- Dados de Background – que são os perfis de usuário;
- Dados de entrada – que são as ações executadas pelo usuário;
- Um Algoritmo – que faz a ligação entre os dados de entrada e o background.

Para isso, tais sistemas utilizam técnicas de Filtragem de Informação para processar informações e prover ao usuário itens potencialmente mais relevantes.

Filtragem de Informação é usada para atender necessidades de informação em *longo prazo* a partir de fontes de informação dinâmica e não estruturada [51] e apresenta

basicamente três abordagens, como apresentado anteriormente: Filtragem Baseada em Conteúdo, Filtragem Colaborativa ou social e Filtragem Híbrida.

Com a aplicação das técnicas de Clusterização e Filtragem baseada em Conteúdo em um caso real, utilizando o cálculo de similaridade do Cosseno e Produto Interno, pôde-se obter bons índices de relevância que recomendariam ou não um determinado item.

Assim sendo, conseguiu-se com esse trabalho apresentar uma abordagem bem geral de várias técnicas computacionais de Clusterização, Filtragem e Recomendação, mas a sua utilização de maneira eficaz dependerá sempre da análise que se fizer do domínio em questão, para escolha da ferramenta adequada.

Referente ao estudo de caso apresentado, conclui-se que as medidas de similaridade utilizadas não são indicadas para perfis com número elevado de atributos, pois a similaridade terá valores muito baixos podendo apresentar problemas de precisão. Para estudos futuros, poderá ser implementado esse sistema de recomendação com outras técnicas que sejam mais adequadas ao domínio.

3.4 Considerações Finais

Um SIGA bem projetado deve atender vários sistemas de automação, de modo que deve possuir recursos que permitam aos analistas avaliarem o melhor método de clusterização a ser utilizado. Conforme exemplo prático apresentado na Seção 3.3.1, para cada tipo de dados, um método apresenta resultados mais satisfatórios que o outro. Assim sendo, o SIGA deve permitir que o analista realize simulações, checando qual método é mais interessante para cada tipo de dados.

No estudo de caso apresentado na Seção 3.3.1 utilizou-se Filtragem Baseada em Conteúdo, que será também utilizada no SIGARA, por ser essa a técnica mais adequada aos dados e ao sistema que está sendo projetado. Para a função de filtrar os dados obtidos a partir dos repositórios de alarmes e eventos operacionais em função do perfil dos usuários, a Filtragem Baseada em Conteúdo é a indicada. Nestas técnicas são feitas comparações e cálculo de similaridade entre as representações dos itens de informação e os perfis de usuário. Os perfis dos usuários podem ser atualizados com base nas avaliações que o usuário fez de itens de informação no passado. A hipótese nesta

abordagem é que, se um usuário manifestou interesse por um item de informação no passado, ele tenderá a preferir itens com conteúdo similar no futuro.

Além de filtrar os alarmes e eventos críticos que o usuário final necessita tomar conhecimento, o SIGA proposto irá possuir também a função de Recomendação de Ações, tornado-se um SIGARA. Para essa função, SIGA projetados por outras empresas utilizam-se de Árvore de Decisão [63] [64] , como a Chemtech [23] e EXIDA [27]. Além dessa técnica, pode-se usar também Filtragem Colaborativa, desde que se consiga avaliar o resultado das últimas recomendações.

Detalhes de como será modelado o SIGARA será apresentado no próximo capítulo.

4. SISTEMAS MULTIAGENTES

A proposta desse trabalho prevê o uso de um sistema multiagente através de metodologias e ferramentas de Engenharia de Software. Mas antes da sua modelagem e prototipação que serão realizados no próximo capítulo, apresenta-se a seguir conceitos básicos que irão suportar todo o desenvolvimento desse trabalho fazendo uma introdução sobre o conceito de ontologias, agentes, sistemas multiagentes na Seção 4.1 e as ontologias e metodologias desenvolvidas pelo GESEC que serão aplicadas nesse trabalho na Seção 4.2, concluindo o assunto na Seção 4.3.

4.1 Introdução a Sistemas Multiagente

4.1.1 Ontologias

Uma ontologia é um modelo de dados que representa um conjunto de conceitos dentro de um domínio e os relacionamentos entre estes. Uma ontologia é utilizada para realizar inferência sobre os objetos do domínio.

As ontologias de domínio [65] [66] são descrições formais de classes de conceitos e relacionamentos entre esses conceitos que descrevem um domínio de aplicação. Estruturas de representação de conhecimento baseadas em frames são geralmente utilizadas para representar ontologias de domínio, onde os conceitos são representados por frames e os relacionamentos entre conceitos como *slots* dos frames.

Ontologia pode ser então descrita como “A especificação explícita de uma conceitualização” [67]. Ontologia é uma forma de agrupar conceitos pertencentes a um mesmo domínio de conhecimento.

Ontologias são utilizadas em inteligência artificial, web semântica, engenharia de software e arquitetura da informação, como uma forma de representação de conhecimento sobre o mundo ou alguma parte deste. Ontologias geralmente descrevem:

- **Indivíduos:** são os componentes básicos de uma ontologia. Podem ser objetos concretos (pessoas, animais, carros...) ou abstratos (número, palavras, ..);

- Classes: são grupos abstratos, conjuntos ou coleções de objetos. Eles podem conter indivíduos, outras classes, ou uma combinação de ambos;
- Atributos: propriedades, características ou parâmetros que os objetos podem ter e compartilhar. Objetos em uma ontologia podem ser descritos através de atributos. Cada atributo tem pelo menos um nome e um valor, e é utilizado para armazenar informação que é específica para o objeto ligado a ele;
- Relacionamentos: as formas como os objetos podem se relacionar com outros objetos. Um uso importante dos atributos é a descrição de relacionamentos (também conhecidos como relações) entre objetos na ontologia. Geralmente, uma relação é um atributo cujo valor é outro objeto na ontologia. Muito do poder das ontologias vem da habilidade de descrever estas relações. O conjunto de todas as relações descreve a semântica do domínio. O tipo mais importante de relação é a relação de inclusão (é-superclasse-de, é-um, é-subtipo-de ou é-subclasse-de), que define quais objetos são membros de quais classes de objetos. Tem-se ainda a relação do tipo parte-de que representa como objetos se combinam para formar objetos compostos é-um e parte-de; as ontologias geralmente incluem outros tipos de relações que refinam ainda mais a semântica do modelo. Estas relações geralmente são específicas do domínio e são utilizadas para responder tipos particulares de questões.

Uma ontologia de domínio (*domain ontology* ou *domain-specific ontology*) modela um domínio específico, ou parte do mundo. Ela representa os significados dos termos aplicados ao domínio em questão. Descreve os conceitos e relacionamentos que são importantes em um domínio particular, fornecendo um vocabulário para esse domínio tão bem quanto uma especificação com o significado dos termos mais importantes usados no vocabulário. Recentemente, as ontologias têm sido adotadas em muitos negócios e comunidades científicas como uma maneira de compartilhar, reutilizar e processar conhecimentos do domínio. Ontologia é agora parte central de muitas aplicações tais como portais científicos do conhecimento, sistemas do gerenciamento de informação e sistemas de integração e comércio eletrônico [68].

Em geral, as linguagens das ontologias são desenvolvidas para um propósito particular, e, portanto, variam muito na sintaxe e semântica. Muitos centros de pesquisa escolhem seu

“*Meta Model*”, como por exemplo, o SOQA - *SIRUP Ontology Query API* [69], desenvolvido pela SIRUP que busca se aproximar de uma integração semântica [70].

Em sistemas de informação atuais, as ontologias são usadas cada vez mais para representar explicitamente a semântica de palavras reais presentes em dados e serviços [71].

Para esse trabalho, partiu-se dos conhecimentos já desenvolvidos pelo GESEC [72] para a representação das ontologias, e utilizou-se como ferramenta o Protégé [68]. O Protégé é um software livre, com plataforma de código fonte aberto, que possui uma comunidade de usuários crescente com um conjunto de ferramentas para construção de modelos do domínio e aplicações baseadas em conhecimento com uso de ontologias. Em seu núcleo, o Protégé executa um conjunto rico de estruturas de modelagem de conhecimento e prove ações que suportam a criação, visualização e a manipulação das ontologias em vários formatos de representação.

4.1.2 Agentes

A área de Ciências da Computação tem buscado atualmente a construção de "agentes" que mostrem alguns aspectos da inteligência humana. Alguns pesquisadores mais extremistas, afirmam que agentes poderão vir a recriar o comportamento humano inteligente em sua totalidade. Por outro lado, uma visão mais conservadora sustenta ser possível a construção de agentes que possam exibir alguns aspectos do comportamento humano inteligente [73].

O desenvolvimento e a construção de agentes inteligentes é hoje o mais importante tópico de pesquisa em Inteligência Artificial, devido à grande variedade de aplicações nos mais variados domínios. Os agentes estão sendo usados nas aplicações mais diversas, desde administração de informação personalizada a processos comerciais e industriais complexos, e até mesmo em jogos de computador. Apesar desta proliferação, não existe ainda uma definição comum sobre esses agentes.

Um agente é uma entidade autônoma, composta de sensores e atuadores, capaz de agir de forma a alcançar resultados otimizados. O Agente interage com o mundo e com outros agentes que o rodeiam através de sensores, agindo sobre o mesmo com a utilização dos executores ou efetores. Por exemplo, nos agentes humanos, os olhos e ouvidos, são

sensores; as mãos e a boca são os executores ou efetores. A Figura 24 [74] ilustra as interações de um agente genérico com seu ambiente [74]. Quando se diz que um agente é uma entidade autônoma, se quer dizer que dentre outras coisas, ele deve aprender baseado na sua percepção e nos efeitos para cada ação que realiza.

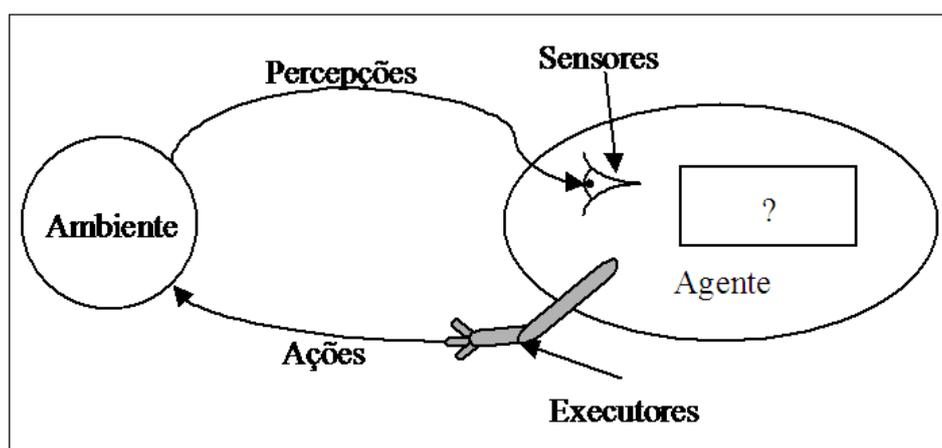


Figura 24 – As interações de um agente genérico com seu ambiente.

A representação da estrutura básica de um agente através de código é bem simples, conforme apresentado na Figura 25 [74]. O agente possui uma memória interna que irá atualizar-se com a chegada de novas percepções, sendo utilizada nos procedimentos de tomada de decisão, os quais irão gerar ações para serem executadas. De forma a manter um histórico do comportamento do agente, a memória do agente é também atualizada a partir da ação selecionada [65].

```

função Agente (percepção) retorna ação
  estática: memória {a memória que o agente possui do seu ambiente}
  memória ← Atualizar-Memória (memória, percepção)
  ação ← Escolher-Melhor-Ação (memória)
  memória ← Atualizar-Memória (memória, ação)
  retornar ação

```

Figura 25 – A estrutura genérica de um agente.

A autonomia é a característica principal dos agentes. Os agentes são capazes de atuar sem intervenção humana ou de outros sistemas através do controle que eles possuem do seu estado interno e do seu comportamento [65].

De uma forma geral, pode-se então definir Agentes como entidades (hardware ou software) que possuem as seguintes propriedades [73]:

- Autonomia - agentes operam sem intervenção humana direta, e possuem algum tipo de controle sobre suas ações e estados internos;
- Habilidade Social - agentes interagem com outros agentes (e possivelmente com seres humanos) através de alguma linguagem de comunicação própria dos agentes;
- Reatividade - agentes percebem seu ambiente, o qual pode ser o mundo físico, um usuário através de alguma interface, uma coleção de outros agentes, a Internet, ou talvez esses itens combinados; e também responde em função do que ocorre nesse ambiente;
- Pro - atividade - agentes fazem mais do que simplesmente agir em resposta ao ambiente, eles possuem habilidades para exibir um objetivo bem focado, através das ações que realiza.

Essa referência sobre agentes atende ao conceito de agentes da engenharia de software baseada em agentes, conforme definido por Genesereth e Ketchpel [75] os agentes se comunicam com seus pares através da troca de mensagens, usando uma linguagem de comunicação bastante expressiva dos agentes. Enquanto agentes podem ser simples como uma sub-rotina, tipicamente eles são entidades grandes com vários controles persistentes.

Além desses conceitos de Agentes, tem-se também outras definições consideradas mais fortes por pesquisadores da Inteligência Artificial – IA [73]. Esses pesquisadores geralmente conceituam um agente como um sistema computacional que, adicionando propriedades às que foram apresentadas anteriormente, são conceituados ou programados usando conceitos que geralmente se aplicam a seres humanos. Por exemplo, é comum na área de IA caracterizar um agente possuindo noções mentais, como conhecimento, convicção, intenção e obrigações [76]. Outros pesquisadores de IA vão mais além, e consideram que os agentes possuem emoções [77].

4.1.3 Sistemas Multiagentes

Um SMA - Sistema Multiagente, pode ser caracterizado como um grupo de agentes que atuam em conjunto no sentido de resolver problemas que estão além das suas habilidades individuais. Os agentes realizam interações entre eles de modo cooperativo para atingir uma meta [65]. Podem interagir entre si ou com outros sistemas de software para a resolução de um problema comum, que está além das suas capacidades individuais.

O Agente é uma entidade real ou abstrata que é capaz de agir sobre ela mesma e sobre seu ambiente, que dispõe de uma representação parcial deste ambiente que, em um universo multiagente, pode comunicar-se com outros agentes, e cujo comportamento é consequência de suas observações, de seu conhecimento e das interações com outros agentes [78].

A utilização da abordagem multiagente deve-se ao fato do poder de representação e adaptabilidade que os agentes possuem. O uso de sistemas multiagente utilizando os conhecimentos desenvolvidos no GESEC [72] facilita a sua padronização e o reuso – assim sendo, com essa abordagem proposta, a solução desse trabalho pode ser facilmente estendida e aplicada para outros sistemas de automação e controle industrial.

Usualmente, cada agente possui um conjunto de capacidades comportamentais que definem sua competência, um conjunto de objetivos, e a autonomia necessária para utilizar suas capacidades comportamentais a fim de alcançar seus objetivos. Um agente é uma entidade computacional com um comportamento autônomo que lhe permite decidir suas próprias ações [79]. A decisão de qual ação realizar é determinada pelo agente, que leva em consideração as mudanças acontecidas no ambiente em que atua e quais ações necessita realizar para alcançar seus objetivos. A idéia principal em um sistema multiagente é que se consiga obter um comportamento global inteligente, que pode ser alcançado a partir da soma dos comportamentos individuais dos agentes. Em um SMA não é necessário que cada agente seja individualmente inteligente, mas que o conjunto das ações desses agentes consiga alcançar um comportamento global inteligente.

Denomina-se interação entre agentes ou entre agente/ambiente uma troca de informações, que pode ser realizada de forma direta (comunicação explícita) ou de modo indireto (emissão de sinais através do ambiente). Uma organização define todas as

restrições aplicadas aos agentes pertencentes a uma determinada sociedade, ou seja, os meios através dos quais o projetista do sistema pode garantir que cada agente desejará e realizará a resolução dos problemas propostos.

A definição proposta acima se preocupa com os mecanismos internos para o tratamento de cada agente, não estabelecendo o tipo de comunicação possível nem a granularidade dos agentes. Em "*Boundaries, identity and aggregation: Plurality issues in multiagent systems*" [80] tem-se uma definição que ressalta o aspecto da identidade de cada agente, onde um agente é uma entidade à qual se pode associar uma identidade única, e que é capaz de realizar tarefas formalizadas. Um agente pode ser considerado como um meio que produz certo número de ações a partir dos conhecimentos e mecanismos internos que lhe são próprios.

Os SMA podem ser caracterizados didaticamente em duas classes, que são Sistemas Multiagente Reativos que trabalha com o desenvolvimento de sistemas que utilizam um grande número de agentes simples para a resolução de um determinado problema, e Sistemas Multiagente Cognitivos, que trabalha com poucos agentes que realizam tarefas mais complexas que os primeiros.

4.2 Metodologias e Ontologias para Sistemas Multiagente

A Engenharia de Domínio Multiagente [65] [81] [82] [83] [84] [85] e a Engenharia de Aplicações Multiagente [82] [86] [87] são processos complementares e interdependentes que possibilitam o reuso no desenvolvimento de software multiagente.

No contexto da Engenharia de Software Multiagente [65], a Engenharia de Domínio Multiagente se encarrega de desenvolver artefatos de software reutilizáveis orientados a agentes a partir do conhecimento acerca de um determinado domínio, e de requisitos comuns e variáveis de uma família de aplicações nesse domínio, considerando experiências passadas de desenvolvimento.

A Engenharia de Domínio Multiagente é um campo de pesquisa na Engenharia de Software Orientada a Agentes, baseando-se na prática da reutilização de software. Com essa prática, busca-se resolver os problemas de produtividade no desenvolvimento bem como de qualidade e manutenção dos produtos de software, através do reuso. A

Engenharia de Domínio Multiagente busca a construção de abstrações de software reutilizáveis que serão usados na criação de sistemas multiagente específicos na Engenharia de Aplicações Multiagente. Essas abstrações são os modelos de domínio, modelos de usuários, frameworks multiagente, padrões de análise, de projeto global e detalhado; e também modelo de agentes de software.

A MADEM (“*Multi-Agent Domain Engineering Methodology*”) [81] [85] [88] é uma metodologia para Engenharia de Domínio Multiagente [65] [81] baseada na abordagem de reuso composicional, na qual se produz componentes reutilizáveis para uma família de aplicações, e em ontologias, produzindo o vocabulário utilizado no domínio [85] [88].

A MAAEM (“*Multi-Agent Application Engineering Methodology*”) [66] [82] [86] [87] é uma metodologia para Engenharia de Aplicações Multiagente baseada na abordagem de reuso composicional, na qual se reusa componentes comuns a uma família de aplicações, e em ontologias, um vocabulário utilizado no domínio [86].

Os processos da Engenharia de Domínio Multiagente e da Engenharia de Aplicações Multiagente são apoiados em metodologias de desenvolvimento próprias, respectivamente MADEM e MAAEM. A metodologia MAAEM, utilizada nesse trabalho, será apresentada na próxima seção.

4.2.1 A Metodologia MAAEM

A MAAEM [66] [82] [86] [87] é uma metodologia para a análise, projeto e implementação de aplicações multiagente através da reutilização de artefatos de software produzidos na Engenharia de Domínio Multiagente, envolvendo a seleção, adaptação e composição de artefatos para a construção de uma aplicação específica, e cujo conhecimento é representado na ontologia ONTORMAS [66] [87], a qual representa artefatos de software na forma de conceitos e relações semânticas.

A MAAEM é uma metodologia que guia o desenvolvimento de aplicações multiagente, com suporte ao reuso, desde a especificação dos requisitos até a sua implementação [86]. Pode-se ter o desenvolvimento COM e PARA o reuso. O desenvolvimento PARA o reuso produz um conjunto de componentes comuns a um conjunto de aplicações de um mesmo domínio e o desenvolvimento COM reuso desenvolve várias aplicações reutilizando esses componentes. O processo inverso também é possível. Ao invés da

Engenharia de Aplicações reusar componentes genéricos da Engenharia de Domínio, esta pode reusar componentes específicos da Engenharia de Aplicações retirando as suas especificidades e tornando-o genérico para que as aplicações da família possam reusá-los.

Para realizar o desenvolvimento de artefatos de software a MAAEM recomenda que se realize um conjunto de tarefas agrupadas nas fases de Análise, Projeto, Implementação. Na fase de análise da aplicação pretende-se identificar e especificar os requisitos de uma determinada aplicação, partindo de modelos de domínio, elaborados na fase correspondente da Engenharia de Domínio Multiagente. Desse modo, a tarefa central do desenvolvedor é reusar um conjunto de requisitos da família em um domínio. Tais requisitos específicos da aplicação, quando provenientes da família, são levantados a partir da seleção dentre os requisitos comuns ou variáveis no domínio.

Na fase de Projeto da Aplicação o desenvolvedor irá reutilizar algumas soluções de projeto relacionadas a uma família de aplicações e adaptá-la aos requisitos específicos da aplicação em desenvolvimento. Essa fase consiste de três tarefas: Modelagem do Conhecimento da Sociedade Multiagente, a qual representa os conceitos compartilhados por todos os agentes em sua comunicação; o Projeto Arquitetural, que estabelece um modelo arquitetural da sociedade multiagente incluindo seus mecanismos de coordenação e cooperação; e o Projeto do Agente, que define o projeto interno de cada agente da sociedade, modelando sua estrutura de conhecimento e seus comportamentos. Na fase de Implementação da Aplicação, os agentes são identificados a partir do modelo de atividades da fase anterior, sendo associado a cada uma de suas responsabilidades comportamentos em uma determinada linguagem/plataforma de desenvolvimento de agentes, como o JADE. São ainda identificadas as interações entre agentes presentes no modelo de interações entre agentes, sendo estas mapeadas para uma determinada linguagem de comunicação entre agentes. O reuso, se dá através da complementação do código gerado, para a qual o programador utiliza agentes de software anteriormente implementados na fase de Implementação do Domínio. A seleção dos agentes ocorre conforme a semelhança de comportamentos e comunicações. A adaptação torna-se necessária em função dos detalhes que diferem de uma aplicação para outra.

Para cada uma dessas fases foram desenvolvidas técnicas que indicam as atividades a serem seguidos no sentido de se alcançar os objetivos de cada uma das fases. Assim sendo, para as fases abaixo foram desenvolvidas as seguintes técnicas:

- Análise de Aplicação - técnica SRAMO;
- Projeto de Aplicação - técnica ADEMÁS;
- Implementação de Aplicação - técnica AIMAS.

Os elementos de modelagem definidos pela MAAEM possuem um nome, uma descrição e um símbolo, conforme ilustrado na Tabela 10 [86].

Tabela 10 - Conceitos de Modelagem da metodologia MAAEM

Name	Description	Used by	Symbol
<i>Domain Concept</i>	<i>Representa qualquer conceito do domínio.</i>	<i>Concepts Model</i>	
		<i>Multi-agent Society Knowledge Model</i>	
<i>Responsibility</i>	<i>Representa uma responsabilidade a ser desempenhada por um Papel e/ou Agente.</i>	<i>Goal Model</i>	
		<i>Role Model</i>	
		<i>Multi-agent Society Model</i>	
<i>General Goal</i>	<i>Representa o Objetivo Geral do Sistema Multiagente.</i>	<i>Goal Model</i>	
<i>Specific Goal</i>	<i>Representa um Objetivo Específico do Sistema Multiagente.</i>	<i>Goal Model</i>	
<i>External Entity</i>	<i>Representa uma entidade externa ao Sistema com a qual o Papel ou Agente interage.</i>	<i>Goal Model</i>	
		<i>Role Model</i>	
		<i>Role Interaction Model</i>	
		<i>Multi-agent Society Model</i>	
		<i>Agent Interaction Model</i>	
<i>Role</i>	<i>Representa um Papel, uma entidade que terá uma ou mais responsabilidades necessárias para alcançar um objetivo específico.</i>	<i>Role Model</i>	
		<i>Role Interaction Model</i>	
<i>Knowledge</i>	<i>Representa conhecimento de domínio.</i>	<i>Role Model</i>	
		<i>Multi-agent Society Model</i>	
		<i>Agent Knowledge</i>	

		<i>and Activity Model</i>	
<i>Condition</i>	<i>Representa uma condição a ser satisfeita, previamente ou após a execução de uma responsabilidade.</i>	<i>Role Model</i>	
		<i>Multi-agent Society Model</i>	
		<i>Agent Knowledge and Activity Model</i>	
<i>Activity</i>	<i>Representa uma atividade a ser executada por um papel para o cumprimento de sua Responsabilidade.</i>	<i>Multi-agent Society Model</i>	
		<i>Agent Knowledge and Activity Model</i>	
<i>Skill</i>	<i>São habilidades ou conhecimentos necessários para a execução de alguma responsabilidade ou atividade específica.</i>	<i>Role Model</i>	
		<i>Multi-agent Society Model</i>	
		<i>Agent Knowledge and Activity Model</i>	
<i>Agent</i>	<i>É uma entidade de software com autonomia, responsável pela obtenção dos objetivos do Sistema através de uma ou mais tarefas.</i>	<i>Multi-agent Society Model</i>	
		<i>Agent Interaction Model</i>	
		<i>Agent Knowledge and Activity Model</i>	

Cada tarefa especificada pela metodologia MAAEM é responsável por produzir algum tipo de artefato. Essas tarefas e os artefatos produzidos estão resumidos na Tabela 11 [86].

4.2.2 A Ontologia ONTORMAS

A ONTORMAS (*Ontology for Reusing Multi-agent Software*) [87] é uma ferramenta e um repositório baseados no conhecimento que permite capturar e armazenar os produtos da Engenharia de Domínio e de Aplicações Multiagente. A ferramenta ONTORMAS é baseada em ontologias e permite realizar as tarefas de modelagem, tanto para a metodologia MADEM quanto a MAAEM. A ONTORMAS é integrada ao ambiente de desenvolvimento de ontologias *Protégé* [68], que fornece toda a infra-estrutura necessária para que qualquer ontologia seja criada, recuperada e integrada.

A proposta da ONTORMAS é facilitar a reutilização dos produtos, uma vez que os mesmos são representados como conceitos que possuem relações semânticas definidas. A partir dos conceitos básicos como Fases, Tarefas, Tipos de Modelos e Relacionamentos definidos na ONTORMAS no ambiente *Protégé*, consegue-se realizar a modelagem dos artefatos definidos pela MAAEM.

Tabela 11 - Fases, Tarefas e Produtos da MAAEM

Fases	Passos		Produtos			
Análise da Aplicação	Modelagem de Conceitos		Modelo de Conceitos		Especificação da Aplicação	
	Modelagem de Objetivos		Modelo de Objetivos			
	Modelagem de Papéis		Modelo de Papéis			
	Modelagem de Interações entre Papéis		Modelo de Interações entre Papéis			
	Prototipação da Interface com o Usuário		Protótipo da Interface com o Usuário			
Projeto da Aplicação	Modelagem do Conhecimento da Sociedade Multiagente		Modelo do Conhecimento da Sociedade Multiagente		Arquitetura da Aplicação	
	Projeto Arquitetural	Modelagem da Sociedade Multiagente	Modelo da Sociedade Multiagente			Modelo Arquitetural
		Modelagem das Interações entre Agentes	Modelo das Interações entre Agentes			
		Modelagem de Atividades	Modelo de Atividades			
	Projeto do Agente	Modelagem dos Mecanismos de Cooperação e Coordenação	Modelo dos Mecanismos de Cooperação e Coordenação			Modelo do Agente
		Modelagem do Conhecimento do Agente	Modelo do Conhecimento do Agente			
Modelagem do Estado do Agente		Modelo do Estado do Agente				
Implementação da Aplicação	Mapeamento de Agentes do Projeto para a Implementação e de Responsabilidades para Comportamentos		Modelo de Agentes e Comportamentos		Aplicação Multiagente	
	Mapeamento de Interações entre Agentes para Atos de Comunicação		Modelo de Agentes e Atos de Comunicação			
	Implementação do Agente		Agentes de Software Executáveis			

Na ONTORMAS existem três tipos de agrupamento de classes fundamentais que são:

- “*Modeling Concepts*” - estão definidos os conceitos fundamentais da metodologia como Papel, Agente, etc.
- “*Modeling Tasks*” - estão definidas as tarefas a serem realizadas em cada fase da MAAEM como, por exemplo, Modelagem de Conceitos, Modelagem de Objetivos, etc.
- “*Modeling Products*” - estão especificados os produtos de modelagem da MAAEM, onde também são definidos quais conceitos fazem parte de cada produto, por exemplo, o conceito papel é utilizado no modelo de papéis e no modelo de interações entre papéis.

Todas essas classes estão relacionadas entre si. Parte da estrutura hierárquica de classes da ONTORMAS desenvolvido no *Protégé* [68], apresentado na Seção 4.1.1. A partir da customização realizada no *Protégé* pelo GESEC [72], tem-se uma interface amigável para criação de seus modelos de conhecimento e ferramentas, gerando, por exemplo, as figuras dos modelos referentes às tarefas da MAAEM. A hierarquia de classes da ONTORMAS definida no *Protégé* está ilustrada na Figura 26.

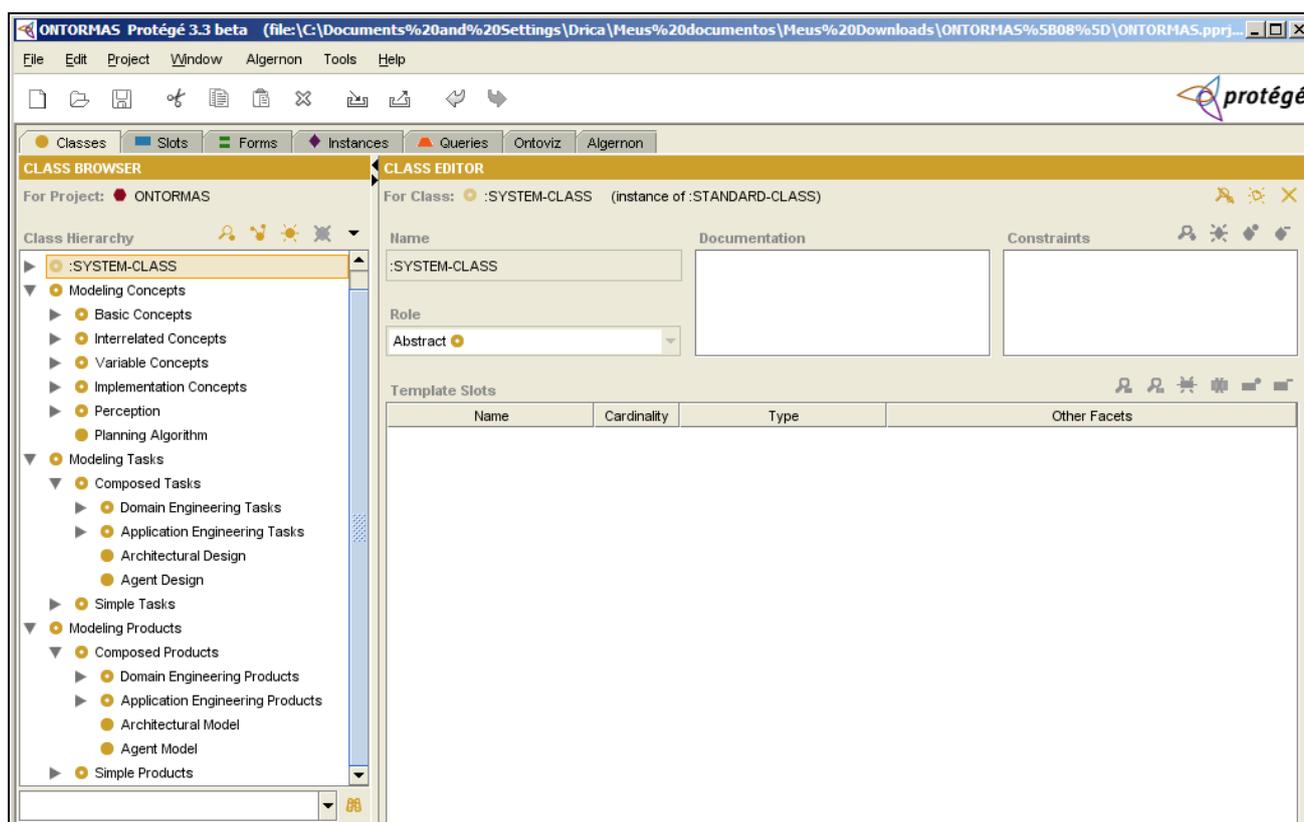


Figura 26 – Exemplo de tela da ONTORMAS desenvolvido no *Protégé*

4.3 Considerações Finais

O presente capítulo apresentou conceitos importantes da área de engenharia de software e do conhecimento, iniciando desde o conceito inicial das Ontologias [66] [87], Agentes e Sistemas Multiagentes [66] [73] [82] [87] [89] [90], até às metodologias e ferramentas que serão aplicadas no desenvolvimento do SIGARA.

A escolha da ONTORMAS [87] como ferramenta para desenvolvimento do SIGARA deveu-se à sua capacidade de capturar e armazenar os produtos da Engenharia de Domínio e de Aplicações Multiagente. A ferramenta ONTORMAS é baseada em ontologias e irá suportar as tarefas de modelagem conforme a metodologia MAAEM [66] [82] [86] [87] que é uma metodologia que guia o desenvolvimento de aplicações multiagente, com suporte ao reuso, desde a especificação dos requisitos até a sua implementação. Outra razão para a escolha da ONTORMAS é a sua integração ao ambiente de desenvolvimento de ontologias do *Protégé* [68], que fornece toda a infraestrutura necessária para que qualquer ontologia seja criada, recuperada e integrada. Espera-se assim, com o uso da MAAEM e da ONTORMAS facilitar a compreensão dos produtos, realizando-se a modelagem dos artefatos definidos pela MAAEM.

5. MODELAGEM E PROTOTIPAÇÃO DO SIGARA

Este capítulo apresenta a análise da aplicação SIGARA (Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendação de Ações), com a sua modelagem e prototipação, utilizando a ontologia ONTORMAS (*“Ontology for Reusing Multi-agent Software”*) [87] como ferramenta de modelagem, conforme a Metodologia MAAEM (*“Multi-Agent Application Engineering Methodology”*) [66] [82] [86] [87].

No Capítulo 2 foi realizado uma pesquisa e estudo dos sistemas informatizados de automação industrial existentes no mercado, buscando-se referências de sistemas informatizados de gerenciamento de alarmes e de condições críticas. Nessa pesquisa realizada encontrou-se vários sistemas desenvolvidos para diversos domínios, porém não foi encontrado nenhum padrão que suprisse totalmente a necessidade do mercado. Assim sendo, a razão de se estar modelando e prototipando um SIGARA ao invés de um SIGA deve-se ao fato desse sistema ser mais completo, contendo as funções e características realmente necessárias para os sistemas informatizados de automação industrial, suprimindo de maneira mais completa as necessidades do mercado.

O sistema multiagente de recomendação proposto é composto basicamente dos seguintes sistemas apresentados na Figura 27:

- Sistema para definir de forma explícita as áreas de responsabilidade e o perfil dos usuários. Os usuários do sistema de recomendação são principalmente formados pela equipe de operação e de manutenção corretiva do sistema de controle e automação. Como as funções e as necessidades são fixas por grupo, poderão ser definidos explicitamente perfis para filtragem e recomendação;
- Sistema para aquisição de Informações. Os dados de entrada do sistema são não estruturados, e gerados continuamente pelos sistemas de controle industrial. Será necessário definir padrões na criação dos textos de falhas presentes nos alarmes e eventos, de modo a aumentar a eficiência do processo de filtragem. Os dados são disponibilizados originalmente em arquivos texto. Será necessário então desenvolver um sistema para capturar as informações provenientes do sistema de automação industrial;

- Sistema para filtragem das informações realizando recomendações baseadas em conteúdo. A partir das informações adquiridas pelo sistema anterior e do perfil dos usuários do sistema inicial, será realizada a filtragem dessas informações, identificando os alarmes críticos e relevantes para esses usuários. Para recomendar as ações será utilizada uma árvore de decisão [63] [64], que em conjunto com a técnica de qualidade e confiabilidade FTA – *Fault Tree Analysis*, irão armazenar o conhecimento do sistema e complementar o processo de recomendação das ações.

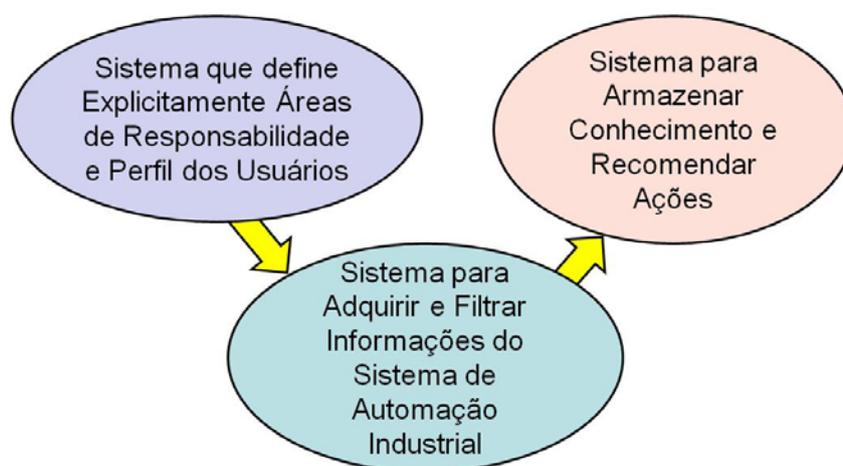


Figura 27 - Sistemas propostos inicialmente para o SIGARA, conforme objetivos específicos

Nas próximas seções são apresentados os modelos referentes à fase de análise da aplicação. Para o presente estudo será desenvolvido a especificação sem reuso de modelos do domínio. São definidos então os requisitos do SIGARA, conforme definido na metodologia MAAEM, obtendo como produto final dessa fase a especificação da aplicação, a qual é resultante das tarefas que irão compor esse capítulo, sendo descritas a seguir.

A primeira tarefa da fase de Análise da Aplicação é apresentada na Seção 5.1, onde se tem a modelagem de conceitos desenvolvendo uma rede semântica com os conceitos-chaves do domínio da aplicação. Na Seção 5.2 é descrita a modelagem de objetivos, onde se apresenta o objetivo principal da aplicação, seus objetivos específicos que representam os requisitos funcionais do sistema multiagente e os requisitos não-funcionais, que são associados a um ou mais objetivos. A modelagem de papéis é mostrada em seqüência na Seção 5.3, onde se irá determinar quem desempenhará as

responsabilidades para alcançar os objetivos específicos e, a partir da realização desses, atingir o objetivo geral. A partir do modelo de papéis da seção anterior, a Seção 5.4 apresenta a modelagem de interações entre esses papéis, onde são identificadas as interações entre os papéis e entre os papéis e as entidades externas através da análise de suas respectivas responsabilidades e atividades, junto com o conhecimento requerido e produzido. A Seção 5.5 mostra o protótipo da interface com o usuário onde se apresentam as possíveis interações de entidades externas, neste caso os usuários, com o sistema. Finalmente, na Seção 5.6 são realizadas as considerações finais sobre a análise e especificação da aplicação, avaliando as atividades realizadas neste capítulo através dos resultados obtidos com os modelos e o protótipo, e a eficácia das ontologias, metodologias e ferramentas utilizadas.

5.1 Modelagem de Conceitos

A tarefa de Modelagem de Conceitos tem como produto o Modelo de Conceitos, que é uma rede semântica com os conceitos-chaves do domínio da aplicação, conceitos esses que serão abordados a seguir, referenciando os estudos apresentados nos capítulos anteriores. Apresenta-se na Figura 28 o resultado dessa análise de requisitos preliminar, com a construção do Modelo de Conceitos proposto para o Sistema Informatizado de Gerenciamento de Alarmes baseado em Recomendação de Ações - SIGARA.

Parte-se inicialmente dos objetivos específicos definidos na Seção 1.2.2 do início deste trabalho, e também dos três sistemas propostos no início desse capítulo, como base para esse modelo. A seguir começa-se a definir os requisitos mínimos necessários para o SIGARA, o qual deve apresentar, ao operador, alarmes com um significado claro e relevante, e para as quais deve-se ter uma resposta definida [4]. É necessário também um sistema de detecção de condições anormais no sistema, conforme conceito "*Detect Abnormal Process Condition*" apresentado pela EEMUA na Figura 5 [9] da Subseção 2.3.1.

Para garantir que todo alarme a ser apresentado tenha relevância, deve-se aplicar várias das técnicas apresentadas na Seção 2.3, como a definição de alarme efetivo da EEMUA, presente na Figura 6 [9] que define que os alarmes sejam ajustados no ponto onde o operador deve tomar alguma ação. Além de ser relevante, o SIGARA deve avaliar também a condição operacional do sistema, através do conceito "*Understand Current*

Process Condition” da Figura 5 [9]. Outros conceitos interessantes que não podem faltar em nenhum SIGARA são *“Action to Correct Current Process Condition”* e *“Action to Fix Underlying Root Causes”*, conceitos esses que apresentam ações aos usuários, suportando-os na tomadas das decisões necessárias para corrigir a condição atual do sistema de automação, baseando-se para isso no conceito *“Investigate Root Cause”* que busca a identificação da causa da condição anormal, e somente após identificar a real causa, realizar a recomendação.

Na Figura 8 [1] da Subseção 2.3.3, tem-se as funções necessárias para o gerenciamento das condições críticas definidas pela ARC, que apresenta conceitos que também devem estar presentes no SIGARA, principalmente as funções *“Deductive alarm notification”* e *“Predictive decision support”*, que somados aos conceitos da Figura 5 [9] *“Detect Abnormal Process Condition”* e *“Investigate Root Cause”* se completam gerando um diagnóstico e uma análise da origem da falha mais completa para o alarme, e serão representados no modelo apresentado na Figura 28 pelos conceitos *“Alarm Evaluation”* e *“Alarm Cause Identification”*. Ao se adicionar funções de CCM ao SIGARA, a proposta fica ainda mais completa.

A função *“Personnel Guidance”* apresentada pela ARC na Figura 8 somada aos conceitos *“Action to Correct Current Process Condition”* e *“Action to Fix Underlying Root Causes”* da Figura 5 [9] também se complementam, garantindo uma orientação mais completa aos usuários das ações necessárias para evitar condições de perigo; problemas potenciais dos equipamentos e também para minimizar os efeitos de um desastre. Essas ações são representadas no modelo da Figura 28 pelo conceito, *“Action Recommender System”*. Assim, o SIGARA irá possuir funções que além de filtrar as recomendações em função do perfil dos usuários, irá possuir bases de dados diferenciadas, conforme necessidade.

Além desses conceitos definidos pela EEMUA [8] [9] e ARC [1] outros princípios são também necessários para que se tenha uma configuração ótima para o SIGARA, que se define sendo uma onde a característica de desempenho do controle do processo, gerenciamento de alarmes e mensagens ajude os operadores a atingirem os objetivos operacionais requeridos. Esse tipo de configuração deve:

- Ajudar os usuários dos sistemas (*“Users”*) que são os operadores, equipe da manutenção e engenharia, a cumprirem seus objetivos [1] [4] através do conceito *“Action Recommender System”*;

- Não inibir o operador de tomar ações necessárias [1]; não esconder informações ou condições necessárias [1] [4]; não apresentar ou bloquear informações ou condições desnecessárias, como alarmes ativos por longo período ou avisos [1] [9] [33]; inibir que pequenas flutuações de variáveis gerem um número significativo de alarmes, quando não forem devido a desvios importantes para o processo [4]; identificar alarmes espúrios, falsos e repetitivos e alarmes para os quais o operador não sabe o que fazer [9] [33] e em pequenas paradas/interrupções apresentar pequeno número de alarmes [9] através dos conceitos “*Alarm Evaluation*”;
- Priorizar a importância dos alarmes através da avaliação de riscos e suprimir alarmes que sejam conseqüências diretas de outros alarmes [4]; guiar o operador às possíveis causas do alarme [1] [15] [33], suportando tanto o operador quanto a equipe de manutenção na solução do problema, auxiliando o operador e a equipe de manutenção a responder ao alarme através de procedimentos em tempo-real [4] através do conceito “*Alarm Cause Identification*” e “*Action Recommender System*”.

O modelo de conceitos da Figura 28 é apresentado através de uma rede semântica, contendo os conceitos do domínio e os seus relacionamentos, obtidos a partir do refinamento progressivo em relação aos conceitos obtidos ao longo do levantamento de requisitos da aplicação. A seguir, são detalhados os conceitos e relacionamentos apresentados nessa figura:

- Sistema informatizado de recomendação de ações (“*Action Recommender System*”), que recomenda ações aos usuários (“*User*”), realizando (relacionamento “*performs*”) uma filtragem baseada em conteúdo (“*Content Based Alarm Filtering*”), que se caracteriza por recomendar uma ação se essa ação for similar a outras ações que o usuário avaliou como relevantes no passado. Para isso é necessário realizar a identificação da causa dos alarmes (“*Alarm Cause Identification*”) e a avaliação da criticidade dos alarmes (“*Alarm Evaluation*”);
- Os usuários (“*User*”) são os operadores e especialistas do sistema; pertencem a uma área de responsabilidade (“*Responsability Area*”), definida em função da sua atividade e nível de responsabilidade dentro da planta industrial, a qual ajuda a definir o perfil (“*User profile*”) que cada usuário possui;
- O modelo do usuário (“*User Model*”) representa o seu perfil (“*User profile*”), que é classificado dentro do conceito de grupo de itens relevantes para um perfil de usuário

(“*Groups of items relevant to a user profile*”). Com a definição dos usuários e do modelo dos usuários, garante-se que somente serão apresentados alarmes relevantes para esses usuários, poupando-os da tarefa de analisar alarmes que não são críticos ou são repetitivos;

- Os dados obtidos da filtragem baseada em conteúdo (“*Content Based Alarm Filtering*”), realizada baseando-se no modelo dos usuários (que define quais alarmes e ações irão interessar aos usuários), utilizam os itens de informação (“*Information Item*”) obtidos do sistema de automação industrial, que são os registros de eventos (“*Events Log*”), registro de estado operacional da planta (“*Operational Status Log*”) e registro de alarmes (“*Alarm Log*”);
- Esses itens de informação (“*Information Item*”) utilizados na filtragem baseada em conteúdo (“*Content Based Alarm Filter*”) são baseados no modelo do item de informação (“*Information Item Model*”), que é parte de um índice de itens de informação (“*Information Item Index*”) contido no grupo de itens relevantes para um perfil de usuário (“*Groups of items relevant to a user profile*”). Garante-se com essa filtragem que somente alarmes relevantes para esse perfil de usuários sejam apresentados;
- O conceito “*Alarm Evaluation*” representa a avaliação dos alarmes, realizando a classificação e análise de relevância dos elementos de informação de interesse dos usuários (“*Groups of items relevant to a user profile*”), a partir dos alarmes críticos (“*Critical Alarms*”) que servem para priorizar de maneira efetiva os alarmes [9], utilizando para isso os dados dos alarmes filtrados (“*Content Based Alarm Filtering*”), que estão incluídos no repositório de dados de alarmes críticos (“*Repository of Critical Alarms*”). Assim, dentre os alarmes que interessam ao perfil do usuário, filtra-se os que são realmente relevantes e críticos;
- O conceito “*Alarm Cause Identification*”, que representa a identificação da causa dos alarmes, é baseado no repositório de dados da árvore de análise de falhas (“*Repository of Fault Tree Analysis*”), que também é um tipo de item de informação (“*Information Item*”). Com esses conceitos, o SIGARA busca identificar e recomendar ações somente para os alarmes relevantes que já foram devidamente filtrados. Essas ações recomendadas serão então ações factíveis de serem realizadas pelos usuários, de modo que eles não perderão tempo com ações que não lhes dizem respeito.

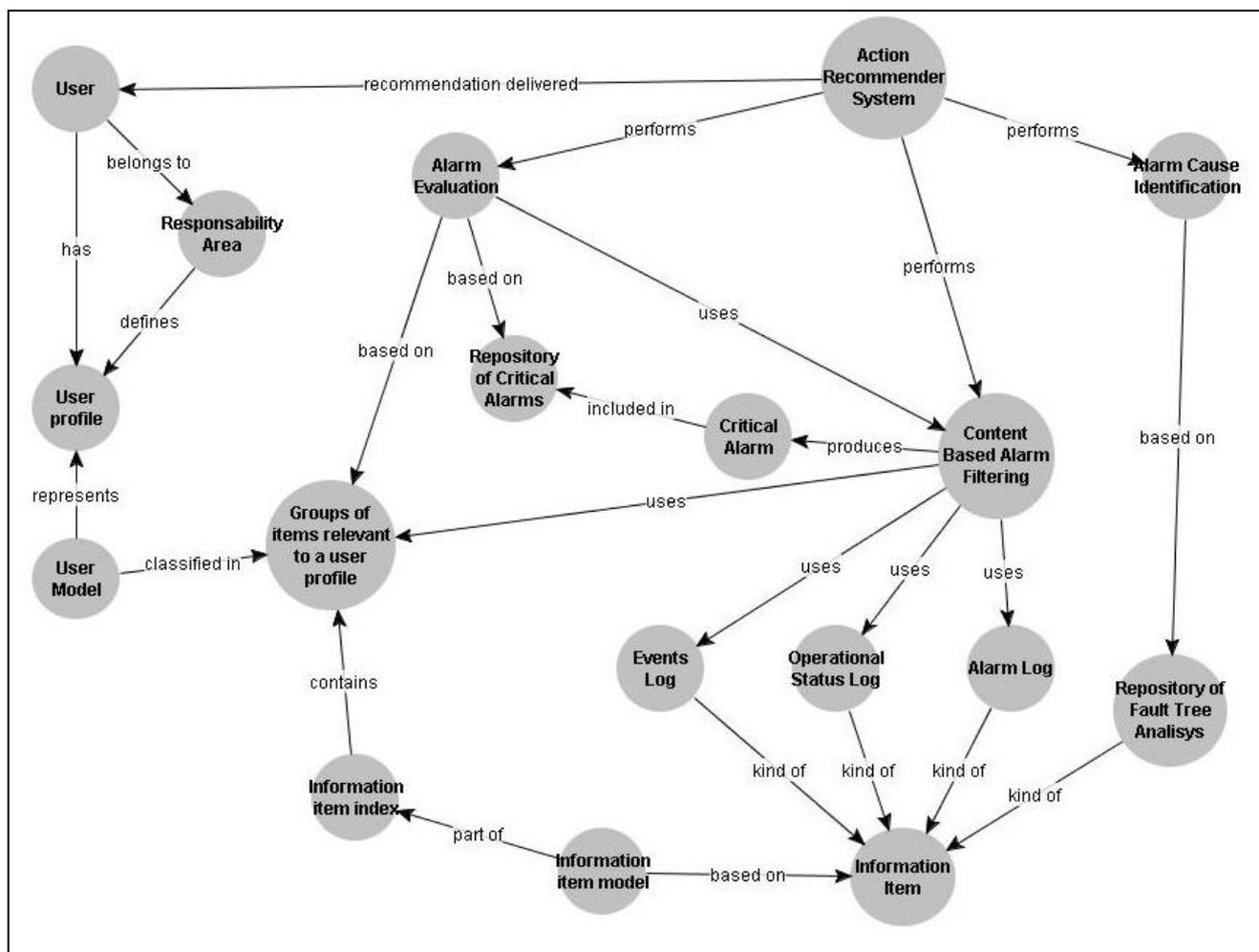


Figura 28 – Modelo de Conceitos do SIGARA

5.2 Modelagem de Objetivos

A partir do conhecimento obtido através da pesquisa realizada e do Modelo de Conceitos da Seção 5.1, desenvolveu-se o Modelo de Objetivos para o SIGARA, apresentado na Figura 30. Esse modelo apresenta o objetivo principal da aplicação, bem como seus objetivos específicos, que representam os requisitos funcionais do sistema multiagente e os requisitos não-funcionais, que são associados a um ou mais objetivos específicos. O Modelo de Objetivos relaciona uma hierarquia entre o objetivo principal, os objetivos específicos resultantes do mesmo, e as responsabilidades necessárias para alcançar esses objetivos. Apresenta-se também nesse modelo as entidades externas que interagem com a aplicação ao longo da sua utilização.

O Modelo de Objetivos definido pela MAAEM [66] [82] [87] [86] é composto por conceitos apresentados na Tabela 10 [86] que são:

- Objetivo geral, que representa o que se espera alcançar através do sistema;
- Objetivos específicos, que são metas a serem atingidas através do desempenho de responsabilidades, que e em conjunto, ajudam a atingir o objetivo geral;
- Responsabilidades, que estão associadas aos objetivos específicos pelo relacionamento semântico alcançar. Isso significa que um objetivo específico será alcançado através da execução de uma ou mais responsabilidades;
- Entidades externas, de onde o sistema obtém as informações necessárias para cumprir os objetivos, satisfazendo a necessidade dos usuários, que também são entidades externas que interagem com o modelo de objetivos.

A seguir, são descritos os objetivos do modelo apresentado na Figura 30:

- O objetivo geral *“Provide personalized action recommendation”* provê recomendação de ações personalizadas através da realização das responsabilidades dos objetivos específicos, tendo como referência o conhecimento adquirido da função *“Personnel Guidance”* para *“operating personnel”*, *“remote personnel”* e *“safety personnel”* apresentadas pela ARC na Figura 8e dos conceitos *“Action to Correct Current Process Condition”* e *“Action to Fix Underlying Root Causes”* definidos pela EEMUA na Figura 5 [9] também da Subseção 2.3.1; *“Goal Setter”* que examina o resultado da avaliação do estimador de estados *“State Estimator”* e propõe ações priorizadas em função de objetivos que necessita perseguir, conforme Figura 19 [37] e, finalmente, do modelo de suporte a decisões apresentado na Figura 18 [37]. Essas duas figuras são da Subseção 2.3.4.8;
- Os objetivos específicos *“Model and Classify User”*, *“Alarm Content Based Filter”*, *“Evaluate Alarm”* e *“Identify Alarm Cause”* são metas a serem atingidas através do desempenho de suas responsabilidades, que atuando em conjunto, ajudam o sistema a atingir o objetivo geral.

O objetivo geral e os objetivos específicos são apresentados de maneira resumida na Figura 29, que irão compor o modelo de objetivos.

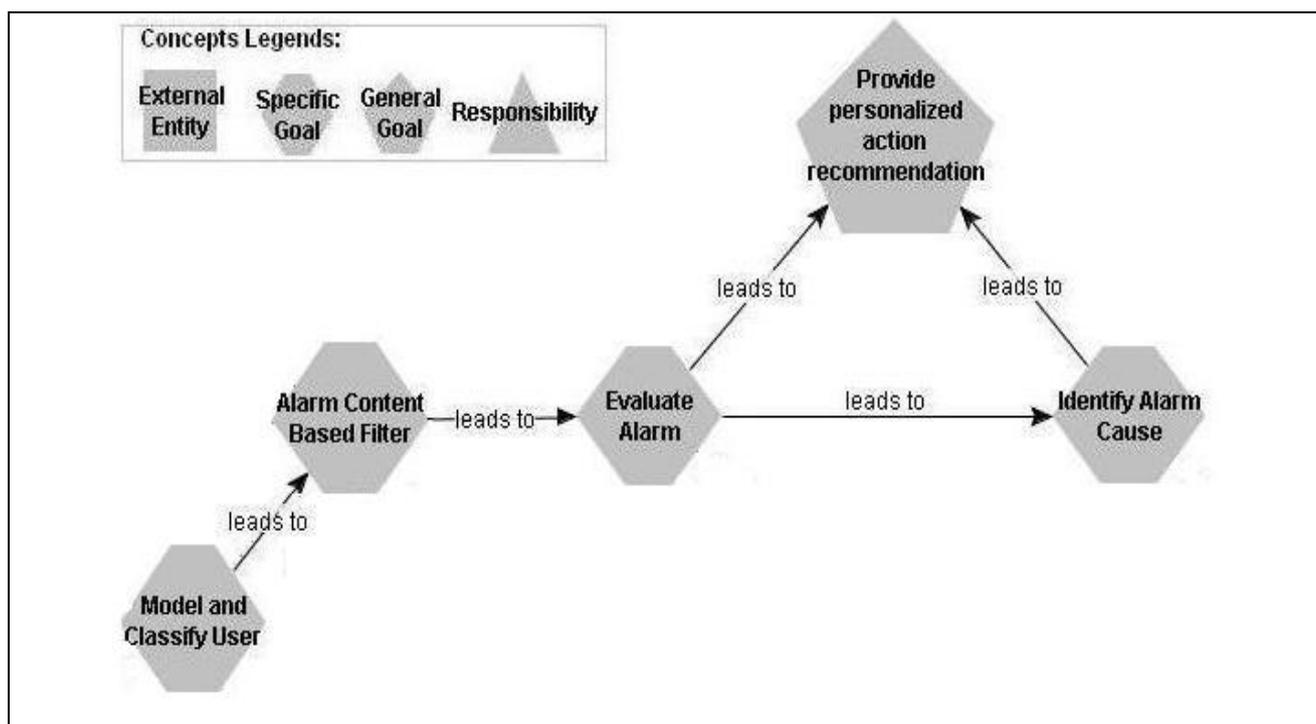


Figura 29 – Objetivo Geral e Objetivos Específicos do SIGARA

A seguir, para cada objetivo específico presente nesse modelo é descrito as responsabilidades necessárias para se cumprir a meta, bem como as entidades externas de onde são extraídas ou às quais são fornecidas as informações necessárias:

- *“Model and Classify User”*. Para atingir a meta de criação do modelo do usuário e classificação do usuário atual, é necessário executar as seguintes responsabilidades:
 - *“Area Creation”* para criar explicitamente as áreas de responsabilidades;
 - *“Explicit Profile Acquisition”* para capturar explicitamente o perfil do usuário;
 - *“User Model Creation”* para criar o modelo do usuário, a partir das informações obtidas das entidades externas *“User”* e *“Analyst”*, e das responsabilidades anteriores;
 - *“Classification of Current User”*, para classificar o usuário atual conforme os modelos de usuários criados.
- *“Alarm Content Based Filter”*. Para atingir a meta de filtragem baseada em conteúdo, esse objetivo específico necessita executar primeiro as seguintes responsabilidades:
 - *“Log Data Analysis”* que analisa os dados de alarmes gerados pelas entidades externas *“Repository of Events Log”*, *“Repository of Operational*

Status Log” e *Repository of Alarm Log*” que detecta a condição anormal do processo, conforme o conceito *“Detect Abnormal Process Conditions”* da Figura 5 [9];

- *“Similarity Analysis”*, que realiza a análise de similaridade baseada em conteúdo;
- *“Content Based Clustering”* que cria clusters dos log de dados que já foram analisados pela responsabilidade *“Log Data Analysis”*, realizando a clusterização a partir da análise de similaridade gerada pela responsabilidade *“Similarity Analysis”*.
- *“Evaluate Alarm”*. Este objetivo específico tem como meta realizar a avaliação dos alarmes, necessitando para isso executar as responsabilidades *“Critical Alarm Analysis”* e *“Critical Condition Analysis”* que analisam, respectivamente, se os alarmes gerados e já filtrados pela responsabilidade anterior, são alarmes críticos conforme os dados da entidade externa *“Repository of Critical Alarms”* ou se são condições críticas, conforme os dados da entidade externa *“Repository of Critical Conditions”*. Para avaliar a condição crítica, essa responsabilidade necessita buscar entender a condição atual do processo conforme *“Understand Current Process Condition”* da Figura 5 [9] ou estimar o estado operacional da planta industrial, conforme conceito *“State Estimator”* apresentado na Figura 19 [37].
- *“Identify Alarm Cause”*. Para atingir a meta de identificação da causa do alarme, esse objetivo específico necessita executar as responsabilidades:
 - *“Alarm Cause Analysis”* que analisa as possíveis causas dos alarmes já avaliados e filtrados pelos objetivos anteriores, a partir dos bancos de dados *“Repository of Alarm Causes”*, conforme conceito *“Investigate Root Cause”* da Figura 5 [9];
 - *“System Knowledge Analysis”*, que analisa as possíveis ações para as causas dos alarmes já avaliados e filtrados pelos objetivos anteriores, a partir dos bancos de dados *“Repository of System Knowledge”*, conforme conceito *“Investigate Root Cause”* da Figura 5 [9].

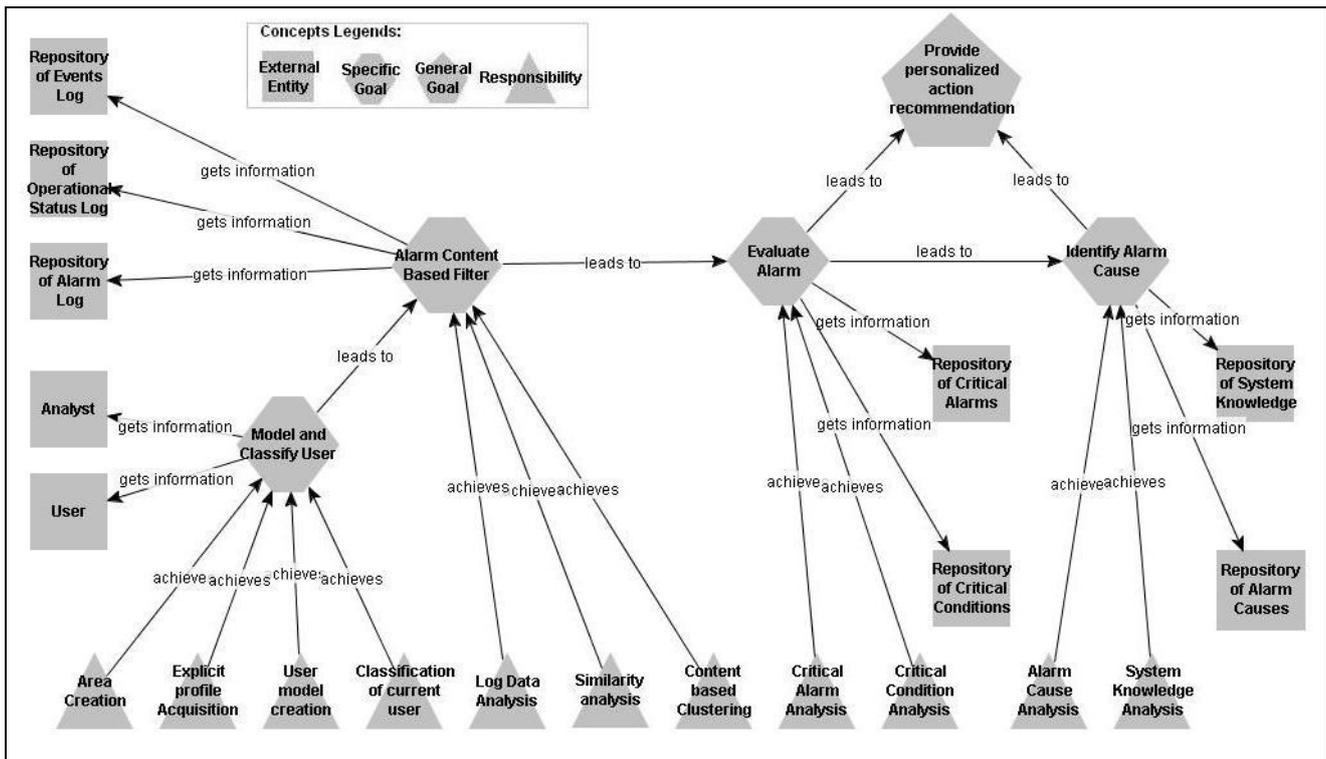


Figura 30 – Modelo de Objetivos do SIGARA

Os Objetivos Específicos descritos nessa seção definirão os Requisitos Funcionais do Sistema Multiagente, e os Requisitos Não-Funcionais serão descritos agora.

Os Requisitos Não-funcionais podem definir o desempenho e a tolerância do sistema, devendo estar associado a um objetivo. Esses requisitos não-funcionais são essenciais para alguns tipos de sistemas como, por exemplo, os sistemas de tempo-real onde o tempo de resposta e o desempenho são fatores críticos.

O SIGARA que está sendo desenvolvido deverá trabalhar em conjunto com Sistemas de Automação e Controle Industrial, que são sistemas de tempo-real, devendo a apresentação das anomalias filtradas ocorrer em no máximo dois segundos – isso significa que os objetivos “*Model and Classify User*”, “*Alarm Content Based Filter*” e “*Evaluate Alarm*” devem ser realizados em no máximo dois segundos apresentando o alarme ou condição crítica relevante. O objetivo específico “*Identify Alarm Cause*” responsável pela identificação da causa mais provável e também o objetivo principal “*Provide personalized action recommendation*” responsável pela recomendação da ação necessária para retornar o sistema à condição normal, devem ser processados em no máximo três segundos.

5.3 Modelagem de Papéis

Nesta seção é apresentada a Modelagem de Papéis, tarefa que determina quem desempenhará as responsabilidades para alcançar os objetivos específicos, e a partir da realização desses, atingir o objetivo geral conforme descrito na seção anterior. Nesta tarefa, pode-se ter que um ou mais papéis serão responsáveis pela execução de um ou mais objetivos específicos. O desempenho destes papéis envolve o uso e a produção de determinados conhecimentos, o atendimento de pré-condições e de pós-condições, e de habilidades específicas para esse fim.

Basicamente, para modelar os papéis deve-se começar pelos objetivos específicos e também objetivo geral, sendo necessário verificar as responsabilidades necessárias para alcançá-los – todos esses conceitos foram desenvolvidos nas Seções 5.1 e 5.2. Dessa forma, cada papel (*“Role”*), que é uma entidade, se encarrega da realização de uma ou mais responsabilidades. Para que os papéis possam ser realizados, devem-se definir os conhecimentos (*“Knowledge”*) que serão necessários para o exercício de uma responsabilidade, bem como aqueles que serão produzidos. Também, devem ser definidas as destrezas ou habilidades (*“Skill”*) que ele vai necessitar possuir para realizar sua responsabilidade. Tem-se também a(s) pré-condição (ões) para que essa responsabilidade seja realizada e/ou as pós-condições alcançadas após a realização da responsabilidade (*“Condition”*). Tem-se ainda o conceito de atividades (*“Activities”*) que devem ser executadas pelos papéis para o cumprimento de suas responsabilidades. Todos esses conceitos foram também apresentados na Tabela 10 [86].

A partir dos modelos das seções anteriores é realizada a modelagem dos papéis, que devido ao grande número de objetivos específicos e suas respectivas responsabilidades, serão apresentados em vários modelos, divididos por objetivos específicos.

5.3.1 Modelo de Papéis - Modelagem e Classificação dos Usuários

A Figura 31 apresenta o modelo de papéis associado ao objetivo específico *“Model and Classify User”*, aonde são representados os papéis necessários para realizar as responsabilidades de criação da área de responsabilidades (*“Area Creation”*), aquisição explícita do perfil do usuário (*“Explicit Profile Acquisition”*), criação do modelo do usuário - *“User Model Creation”* e classificação do usuário atual - *“Classification of Current User”*,

que irão levar ao cumprimento do objetivo específico de modelagem e classificação do usuário - *“Model and Classify User”* apresentados no Modelo de Objetivos da Figura 30, com o desenvolvimento do conhecimento de grupo de itens relevantes para um perfil de usuário - *“Group of items relevant to a user profile”*.

A seguir serão descritos os conceitos que compõem esse modelo de papéis que são os papéis, as responsabilidades, habilidades/destrezas, atividades, condições e entidades externas para que cada responsabilidade possa ser realizada, produzindo o conhecimento necessário para que os objetivos sejam cumpridos.

O conceito Papel possui o relacionamento *“in charge of”* com o conceito Responsabilidade, porque um papel é responsável pela execução de uma ou mais responsabilidades. O papel *“Area Creator”* é responsável pela execução da responsabilidade *“Area Creation”*; o papel *“User Data Acquirer”* é responsável pela execução da responsabilidade *“Explicit Profile Acquisition”*; o papel *“User Modeler”* é responsável pela execução da responsabilidade *“User Model Creation”* e o papel *“Classifier”* é responsável pela execução da responsabilidade *“Classification of Current User”*.

O conceito Responsabilidade possui o relacionamento semântico *“produces”* com o conceito Conhecimento e *“exercised through”* com o conceito Atividade, porque para a execução de uma responsabilidade são realizadas atividades que podem produzir conhecimento. O conceito Conhecimento possui ainda o relacionamento *“used by”* para com as Responsabilidades. Tem-se então a modelagem dos papéis para as seguintes responsabilidades:

- A responsabilidade *“Area Creation”* cria a área de responsabilidade e produz o conhecimento que representa as áreas de responsabilidade - *“Area Responsibilities”*, necessitando para isso usar informações do conhecimento de responsabilidades do sistema - *“System Responsibility”*, que foi criado explicitamente pela entidade externa analista - *“Analyst”*. Para produzir o conhecimento *“Area Responsibilities”*, necessita ainda ter as condições de diferentes posições/ocupações - *“Different work positions”* e diferentes objetivos - *“Different Goals”* satisfeitas, e possuir também a habilidade/destreza para definir as áreas de interesse - *“Techniques to Define Area Interests”*. O papel responsável pela execução dessa responsabilidade é *“Area Creator”* que possui os

conhecimentos das áreas de responsabilidades do sistema - *“System Responsibility”*. O conhecimento *“Area Responsibilities”* deverá também ser compartilhado com *“User”*, que são os usuários que irão utilizar o sistema;

- A responsabilidade que adquire explicitamente o perfil do usuário - *“Explicit Profile Acquisition”* produz como conhecimento o perfil do usuário - *“User profile”*. Para produzir esse conhecimento, possui a habilidade/destreza para poder criar o perfil do usuário - *“Techniques to create user form”* e usar o conhecimento sobre as áreas de responsabilidades criado pelo papel anterior - *“Area Responsibilities”* - necessita também ter a condição que define o perfil do usuário satisfeita - *“User profile is valid”*. O papel responsável pela execução dessa responsabilidade é o papel que captura os dados do usuário - *“User Data Acquirer”* que possui os conhecimentos dos perfis dos usuários - *“User Profile”*;
- A responsabilidade que cria o modelo do usuário - *“User Model Creation”*, produz o conhecimento que representa o modelo do usuário - *“User Model”*, necessitando para isso usar informações sobre o conhecimento do perfil do usuário - *“User profile”*, que foi criado pelas responsabilidades anteriores. Para produzir esse conhecimento, necessita possuir a habilidade/destreza que cria o modelo do usuário - *“Techniques to Create User Model”*. O papel responsável pela execução dessa responsabilidade é o modelador de usuário - *“User Modeler”* que possui os conhecimentos dos modelos dos usuários - *“User Model”*;
- A responsabilidade que classifica o usuário atual - *“Classification of Current User”* produz o conhecimento que representa o grupo de itens relevantes para um determinado perfil de usuários - *“Group of items relevant to a user profile”*, necessitando para isso usar informações do conhecimento do modelo do usuário - *“User Model”*, que foi criado pela responsabilidade anterior. Para produzir esse conhecimento, necessita possuir a habilidade/destreza que faz a classificação - *“Classification”*. O papel responsável pela execução dessa responsabilidade é o classificador - *“Classifier”* que possui o conhecimento que representa o grupo de itens relevantes para um determinado perfil de usuários - *“Group of items relevant to a user profile”*.

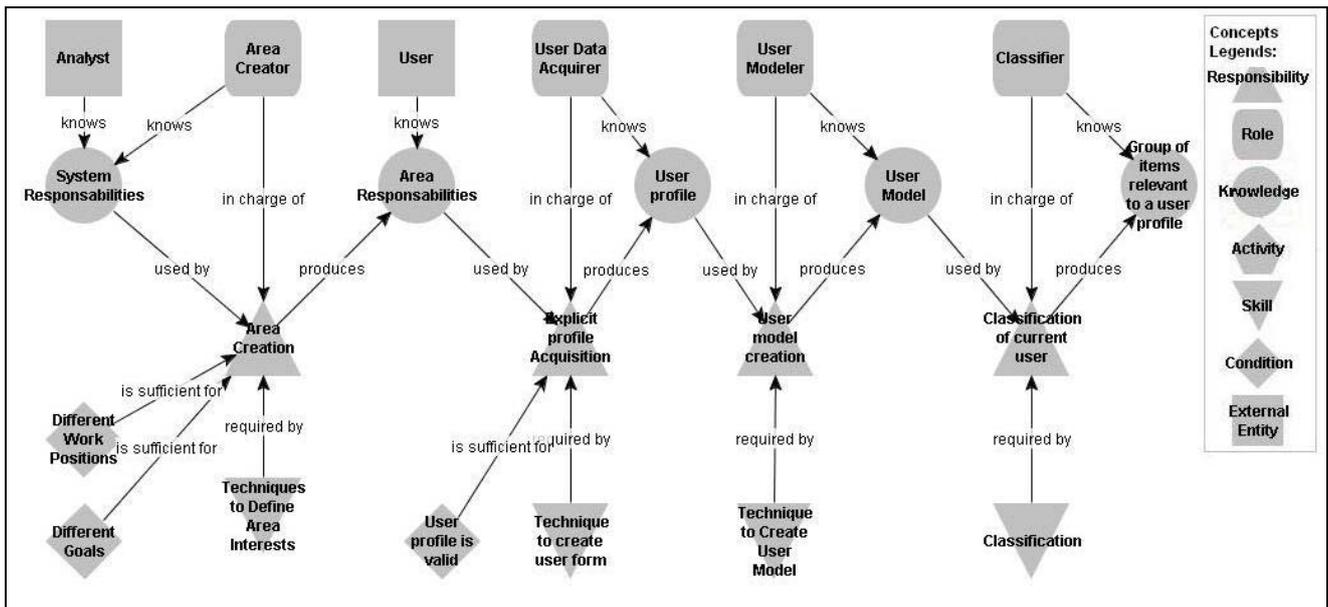


Figura 31 – Modelo de Papéis do SIGARA - Modelagem e Classificação dos Usuários

5.3.2 Modelo de Papéis – Filtragem Baseada em Conteúdo

A Figura 32 apresenta o modelo de papéis associado ao objetivo específico “*Filtragem Baseada em Conteúdo*”, aonde são representados os papéis necessários para execução das responsabilidades “*Log Data Analysis*”, “*Similarity Analysis*” e “*Content Based Clustering*” apresentadas no Modelo de Objetivos da Figura 30. A seguir serão descritos os conceitos que compõem o modelo de papéis de filtragem baseada em conteúdo.

- A responsabilidade que analisa os registros de informação do sistema de automação - “*Log Data Analysis*” produz o conhecimento que possui os bancos de dados das informações do sistema - “*Data Repository*”, necessitando para isso usar informações geradas pelo sistema representadas pelo conhecimento “*System Logs Information*”, que representa as entidades externas que são os bancos de dados dos registros dos eventos - “*Repository of Events Log*”, banco de dados dos registros do estado operacional da planta - “*Repository of Operational Status Log*”, e o banco de dados dos registros de alarmes - “*Repository of Alarm Log*” e do papel que analisa todos esses dados - “*Data Analyser*”. Para produzir esse conhecimento, necessita ainda ter a condição que indica que uma alarme ocorreu - “*Alarm occurred*” ou que um evento operacional ocorreu - “*Event occurred*” satisfeita. Necessita possuir também a habilidade/destreza que permite analisar esses

alarmes e eventos - *“Techniques to Alarm and Event Analysis”*. O papel responsável pela execução dessa responsabilidade é o papel que analisa todos esses dados - *“Data Analyser”*, que possui os conhecimentos sobre os registros de informação do sistema - *“System Logs Information”*.

- A responsabilidade que analisa a similaridade entre os dados do registro de informação com o perfil do usuário - *“Similarity Analysis”* produz o conhecimento que representa a informação da distância da similaridade entre esses dados - *“Similarity Distance Information”*, necessitando para isso usar informações do conhecimento que representa os registros de dados do sistema - *“Data Repository”* e do conhecimento que representa o grupo de itens que é relevante para um determinado perfil de usuários - *“Group of Items relevant to a user profile”* criado no modelo anterior. Para produzir esse conhecimento, necessita ainda ter a habilidade/destreza que permite analisar a distância de similaridade - *“Techniques of Similarity Analysis”*. O papel responsável pela execução dessa responsabilidade é o que realiza a filtragem baseada em conteúdo - *“Content Based Filter”* que possui os conhecimentos sobre as técnicas de clusterização de informações - *“Information of Clustering Techniques”* e grupo de itens que são relevantes para um determinado perfil de usuários - *“Group of Items relevant to a user profile”*.
- Completando esse modelo, tem-se a responsabilidade que realiza a clusterização baseada em conteúdo - *“Content based Clustering”*, produzindo o conhecimento que representa na forma de um vetor os alarmes relevantes que foram filtrados conforme o perfil do usuário - *“Vector of Alarms”* e o vetor com os eventos e as condições críticas que também foram filtradas conforme o perfil do usuário - *“Vector of Critical Conditions”*. Necessita para isso usar informações sobre as técnicas de clusterização - *“Information of Clustering Techniques”* e do grupo de itens que são relevantes para um determinado perfil de usuários - *“Group of Items relevant to a user profile”*. Para produzir esses vetores de conhecimento, necessitam ainda ter a habilidade/destreza para clusterizar esses dados de informação - *“Clustering Techniques”*. O papel responsável pela execução dessa responsabilidade é também o papel que realiza a filtragem baseada em conteúdo - *“Content Based Filter”*, já descrito.

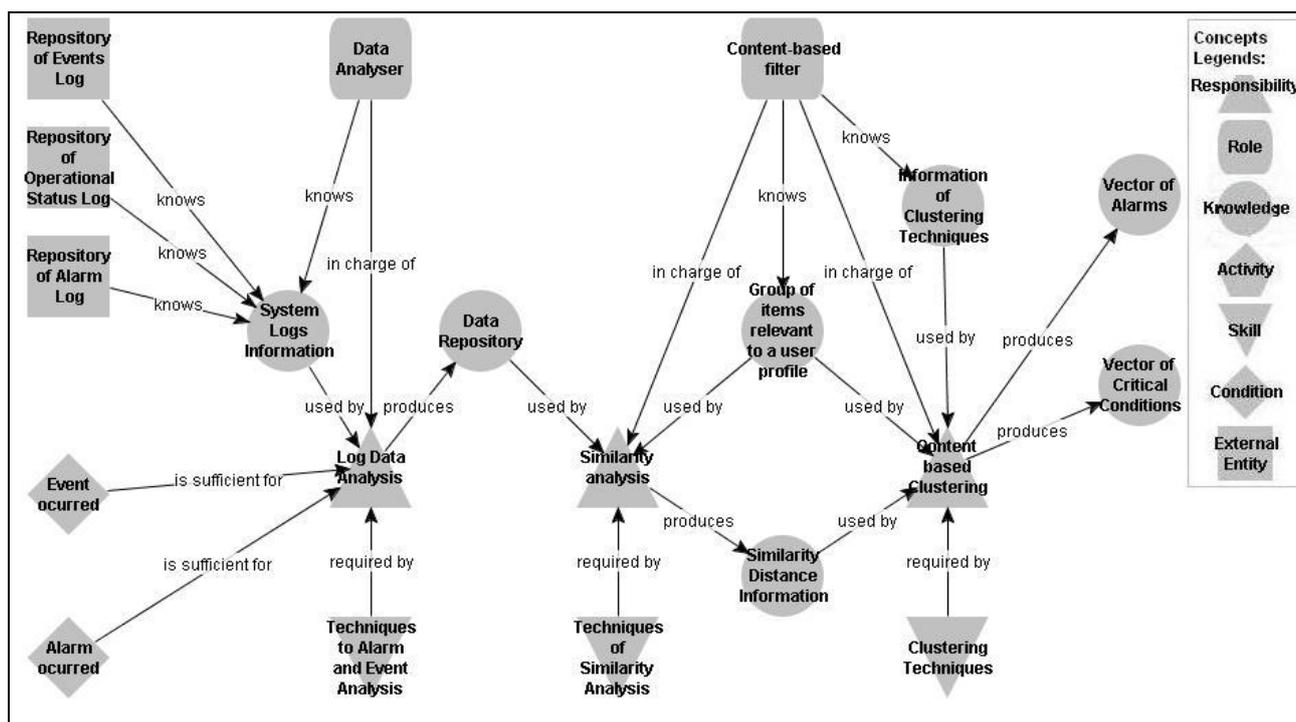


Figura 32 – Modelo de Papéis do SIGARA - Filtragem Baseada em Conteúdo

5.3.3 Modelo de Papéis – Avaliação dos Alarmes

A Figura 33 apresenta o modelo associado ao objetivo específico “Avaliação dos Alarmes”, aonde é representada os papéis necessários para se realizar as responsabilidades “*Critical Condition Analysis*” e “*Critical Alarm Analysis*” apresentados no Modelo de Objetivos da Figura 30. A seguir serão descritos os conceitos que compõem o modelo de papéis de avaliação dos alarmes:

- A responsabilidade que analisa as condições críticas - “*Critical Condition Analysis*” contribui para produzir o conhecimento em forma de vetor que possui as condições críticas e os alarmes que são relevantes - “*Vector of Critical and Relevant Alarms*”; necessitando para isso usar informações do vetor de conhecimento de condições críticas - “*Vector of Critical Conditions*” produzido pelo modelo de papéis anteriores. Para produzir esse conhecimento, necessita possuir a habilidade/destreza que permite analisar as condições críticas - “*Techniques to Analyse Critical Condition*” quando a condição que define que um evento ocorreu - “*Event occurred*” seja satisfeita. O papel responsável pela execução dessa responsabilidade é o papel que avalia o vetor de alarmes - “*Alarm Evaluator*”, que possui os conhecimentos do

vetor de condições críticas - “*Vector of Critical Conditions*” e também obtém informação da base de dados de condições críticas da entidades externa - “*Repository of Critical Conditions*”;

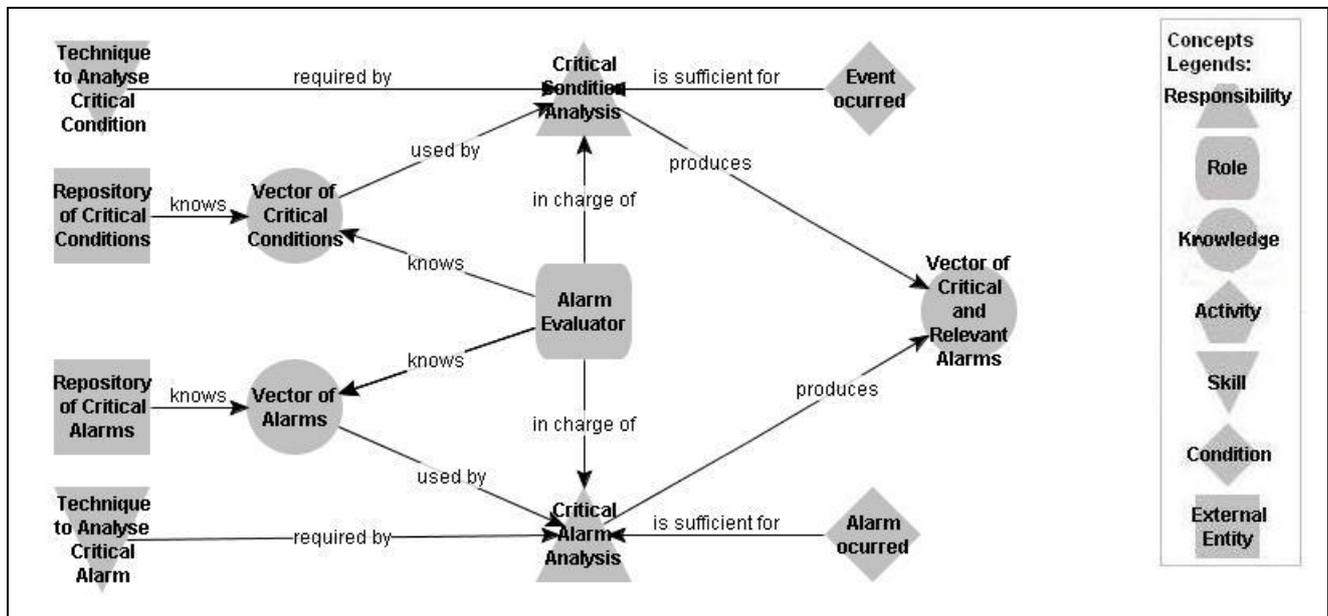


Figura 33 – Modelo de Papéis do SIGARA – Avaliação dos Alarmes

- A responsabilidade que analisa os alarmes críticos - “*Critical Alarm Analysis*” contribui para produzir o conhecimento em forma de vetor que possui as condições críticas e os alarmes que são relevantes - “*Vector of Critical and Relevant Alarms*”, necessitando para isso usar informações do vetor de conhecimento de alarmes - “*Vector of Alarms*” produzido pelo modelo de papéis anteriores. Para produzir esse conhecimento, necessita também possuir a habilidade/destreza que analisa os alarmes críticos - “*Techniques to Analyse Critical Alarms*” e ter a condição que define que um alarme ocorreu - “*Alarm occurred*”, satisfeita. O papel responsável pela execução dessa responsabilidade é o papel que avalia os alarmes - “*Alarm Evaluator*”, que possui o conhecimento dos vetores de conhecimento dos alarmes - “*Vector of Alarms*” e também obtém informação da base de dados de alarmes críticos da entidades externa - “*Repository of Critical Alarms*”.

5.3.4 Modelo de Papéis – Identificação da Causa do Alarme

A Figura 34 apresenta o modelo de papéis associado ao objetivo específico “Identificação da Causa do Alarme”, aonde são representados os papéis necessários para se realizar as responsabilidades “*System Knowledge Analysis*” e “*Alarm Cause Analysis*” apresentados no Modelo de Objetivos da Figura 30. A seguir será descrito os conceitos que compõem o modelo de identificação da causa do alarme:

- A responsabilidade que analisa a causa do alarme - “*Alarm Cause Analysis*” também contribui para produzir o conhecimento com as possíveis causas para o alarme - “*Alarm Causes*”, necessitando para isso usar informações do conhecimento “*Vector of Critical and Relevant Alarms*”. Para produzir esse conhecimento, necessita possuir a habilidade/destreza para analisar as possíveis causas para o alarme - “*Techniques for Cause Analysis*”. O papel responsável pela execução dessa responsabilidade é o identificador das causas do alarme - “*Alarm Cause Identifier*” que possui os conhecimentos do “*Vector of Critical and Relevant Alarms*” e também obtém informação da base de dados da entidade externa que possui as possíveis causas para os alarmes cadastrados - “*Repository of Alarm Causes*”;
- A responsabilidade que analisa as condições do sistema - “*System Knowledge Analysis*”, contribui para produzir o conhecimento que possui as possíveis causas para o alarme ou condição crítica - “*Alarm Causes*”, necessitando para isso usar informações do conhecimento “*Vector of Critical and Relevant Alarms*” produzido pelo modelo anterior, que é um vetor com os alarmes relevantes e condições críticas do sistema já filtradas em função do perfil do usuário. Para produzir o conhecimento “*Alarm Causes*”, necessita possuir a habilidade/destreza para poder analisar as condições do sistema - “*Techniques for System Analysis*”. O papel responsável pela execução dessa responsabilidade é o identificador das causas do alarme - “*Alarm Cause Identifier*”, que possui os conhecimentos do “*Vector of Critical and Relevant Alarms*” e também obtém informação da base de dados da entidade externa que possui os conhecimentos das condições do sistema - “*Repository of System Knowledge*”.

Nesse modelo, também devem ser definidas as mensagens trocadas entre os papéis, entre papéis e entidades externas e os conhecimentos passados como parâmetros.

5.4.1 Modelo de interação entre os papéis da modelagem e classificação dos usuários

Na Figura 35 a seguir tem-se o modelo de interação entre os papéis que trata da modelagem e classificação do usuário. Esse modelo contém os papéis apresentados na Figura 31 necessários para criar as áreas de responsabilidades - “*Area Creator*”, adquirir explicitamente dados do perfil do usuário - “*User data Acquirer*”, criar o modelo do usuário - “*User Modeler*” e classificar o usuário - “*Classifier*”, os quais irão levar ao cumprimento do objetivo específico de modelagem e classificação do usuário - “*Model and Classify User*” apresentados no Modelo de Objetivos da Figura 30.

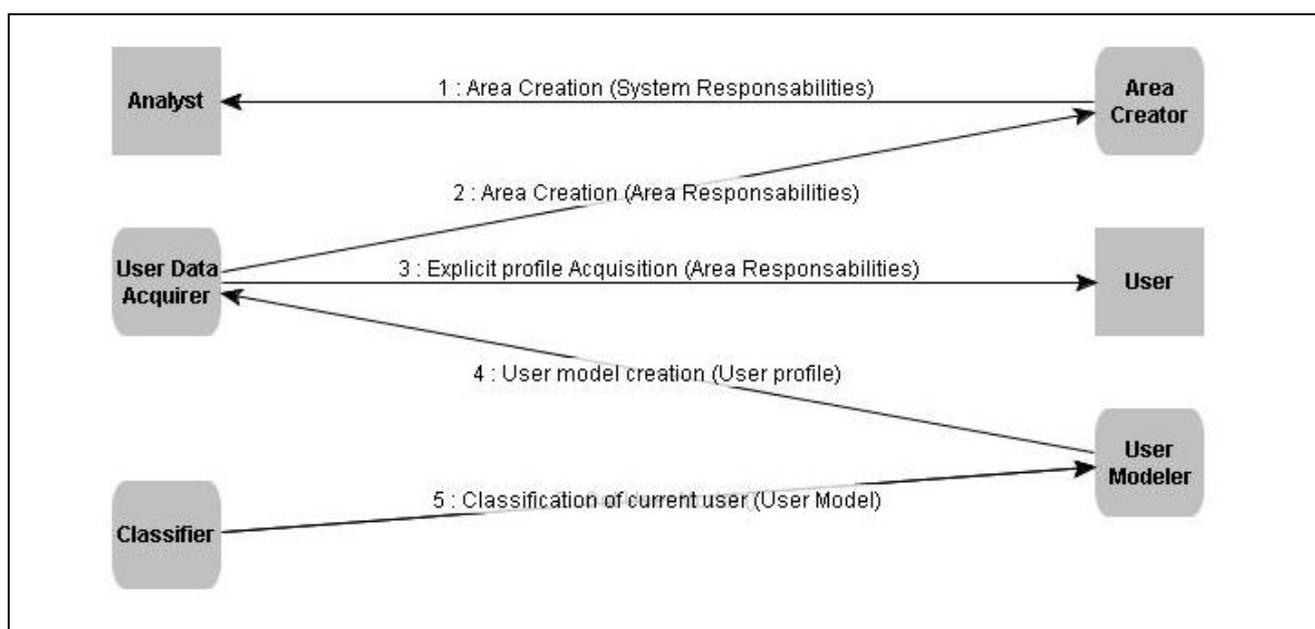


Figura 35 – Modelo de Interação entre Papéis – Modelagem e Classificação dos Usuários

O papel “*Area Creator*” cria as áreas de responsabilidades recebendo os conhecimentos necessários sobre as responsabilidades do sistema diretamente do analista, que é uma entidade externa ao sistema. A criação dessas áreas ocorre inicialmente, quando da configuração do sistema, e depende do nível de conhecimento que o Analista tem do

sistema, sendo que o mesmo pode realizar consultas a usuários mais experientes do sistema para identificar melhor essas áreas.

O papel *“User Data Acquirer”* adquire explicitamente os dados do usuário, através de uma interface gráfica onde o usuário é cadastrado conforme as responsabilidades que irá possuir, construindo assim o perfil desse usuário. Para isso, necessita também receber os conhecimentos sobre as áreas de responsabilidades produzidas pelo papel *“Area Creator”*.

O perfil desse usuário será agora utilizado pelo papel *“User Modeler”* que irá criar o modelo desse usuário, armazenando todos esses dados no banco de dados do sistema.

Dessa forma, toda vez que um usuário novo logar no sistema ele será cadastrado, gerando assim o seu perfil. E toda vez que um usuário já cadastrado logar no sistema, ele será classificado através do papel *“Classifier”*, usando para isso o conhecimento do modelo dos usuários existentes criados a partir dos dados do seu perfil.

5.4.2 Modelo de interação entre papéis da filtragem baseada em conteúdo

O modelo de interação entre os papéis apresentado na Figura 36 modela a interação entre os papéis apresentados na Figura 32, necessários para se realizar o objetivo específico de filtragem baseada em conteúdo dos alarmes – *“Alarm Content Based Filter”*.

Os papéis que serão modelados são o papel que analisa os dados gerados pelo sistema – *“Data Analyser”*, e o papel que realiza a filtragem baseada em conteúdo - *“Content Based Filter”*.

O papel *“Data Analyser”* irá analisar os dados do *“System Logs Information”* através da responsabilidade *“Log Data Analysis”*, dados esses que foram gerados pelo sistema de automação industrial – entidade externa à nossa aplicação, que são as bases de dados de registro de alarmes – *“Repository of Alarm Log”*, de registro de eventos do sistema – *“Repository of Events Log”*, e de registro do estado operacional do sistema – *“Repository of Operational Status Log”*.

O papel *“Content Based Filter”* irá realizar a filtragem baseada em conteúdo conforme os itens de informação criados pelo papel anterior, usando o conhecimento do grupo de itens relevantes para um perfil de usuário – *“Group of items relevant to a user profile”*, criado pelo papel *“Classifier”*, através da responsabilidade *“Classification of current user”*.

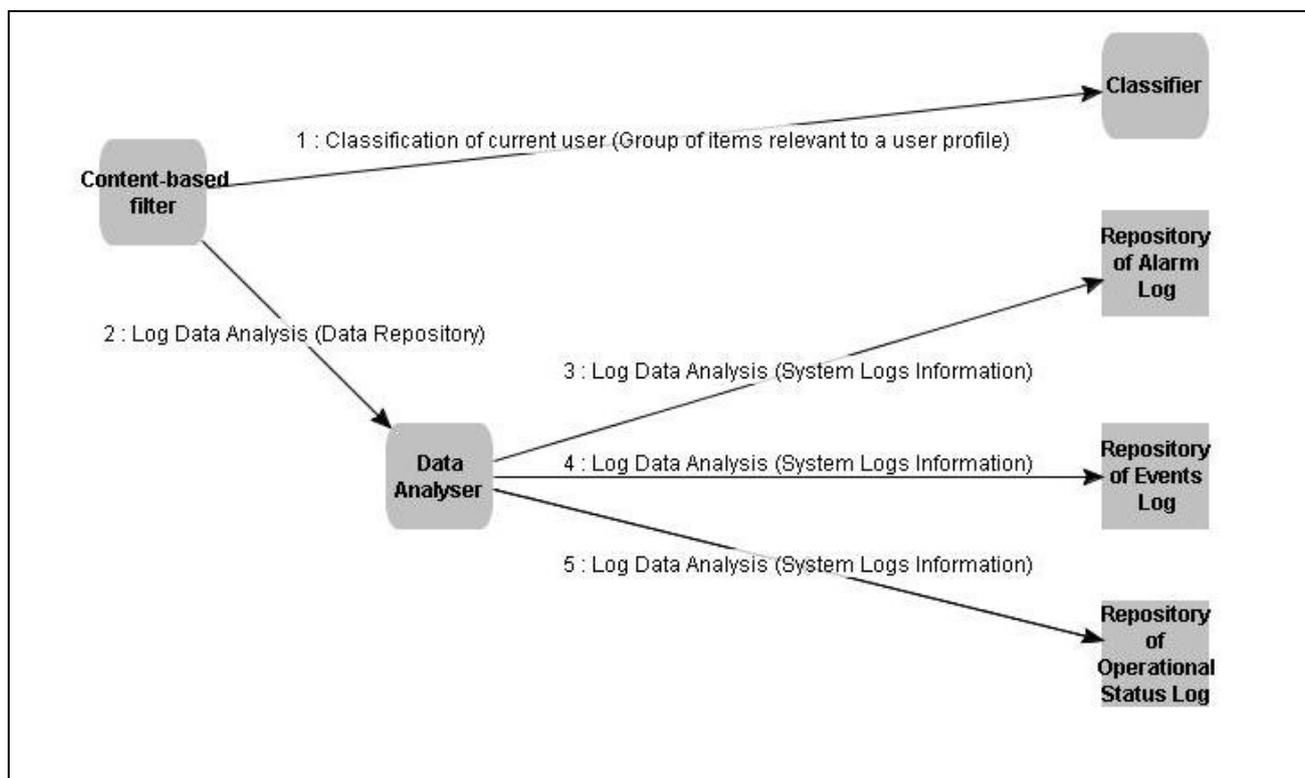


Figura 36 – Modelo de Interação entre Papéis – Filtragem baseada em Conteúdo

5.4.3 Modelo de interação entre os papéis da avaliação dos alarmes

Esse modelo de interação entre papéis, apresentado na Figura 37, refere-se à interação entre os papéis necessários para se realizar a avaliação de criticidade e relevância dos alarmes e eventos, realizando assim o objetivo específico “*Evaluate Alarm*” apresentado no modelo de objetivos da Figura 30.

Esse terceiro modelo de interações apresenta o papel “*Content based Filter*”, que irá gerar conhecimentos necessários para o papel “*Alarm Evaluator*” desempenhar suas funções, que são o vetor de condições críticas - “*Vector of Critical Conditions*” e o vetor de alarmes relevantes - “*Vector of Alarms*”. Para fazer essa avaliação, o papel “*Alarm Evaluate*” necessita também analisar os conhecimentos presentes nos bancos de dados de condições críticas – “*Repository of Critical Conditions*”, e de alarmes críticos – “*Repository of Critical Alarms*”, que são entidades externas ao sistema. Essa análise é realizada através da execução das responsabilidades “*Critical Condition Analysis*” e “*Critical Alarm Analysis*” do modelo de papéis da Seção 5.3.3.

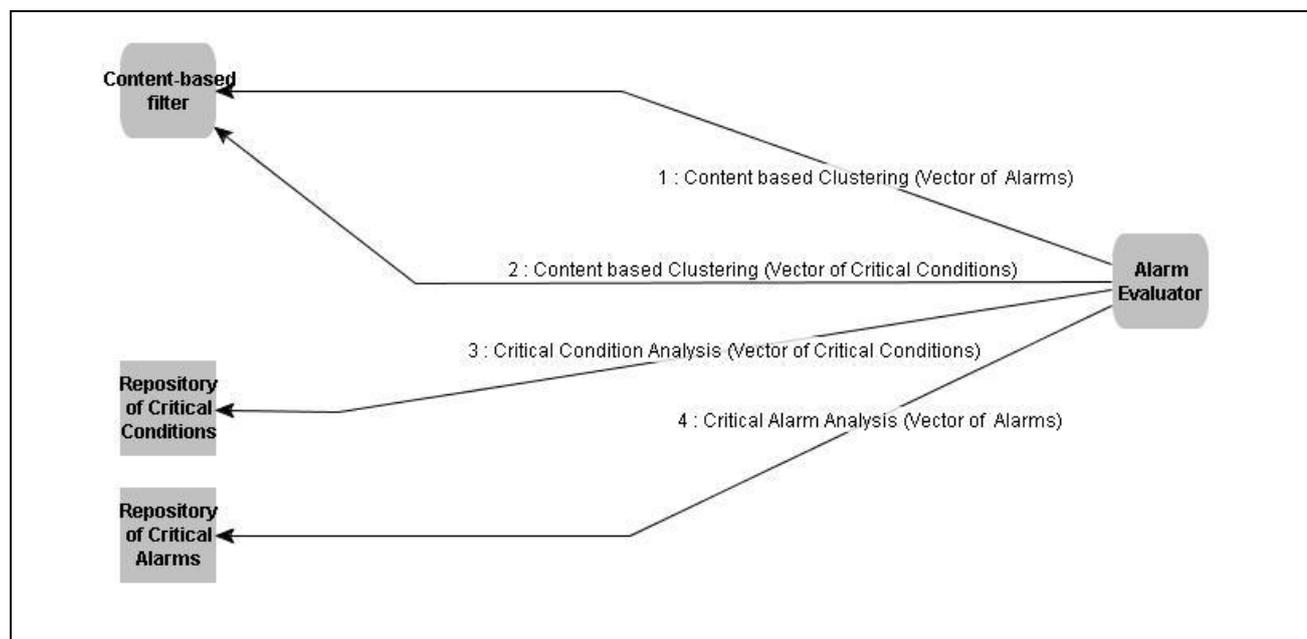


Figura 37 – Modelo de Interação entre Papéis – Avaliação dos Alarmes

5.4.4 Modelo de interação entre papéis da identificação da causa do alarme

O quarto e último modelo de interação entre papéis, apresentado na Figura 38, refere-se à interação entre os papéis necessários para se realizar a identificação das causas dos alarmes relevantes e críticos, bem como das condições críticas, realizando assim o objetivo específico *“Identify Alarm Cause”* apresentado no modelo de objetivos da Figura 30 e no modelo de papéis da Figura 34.

Esse modelo de interações apresenta o papel *“Alarm Evaluator”*, que irá gerar conhecimentos necessários para o papel *“Alarm Cause Identifier”* desempenhar suas funções, que são o vetor de condições críticas - *“Vector of Critical Conditions”* e o vetor de alarmes críticos e relevantes - *“Vector of Critical and Relevant Alarms”*. Para fazer essa avaliação, o papel *“Alarm Cause Identifier”* necessita também analisar os conhecimentos presentes nos bancos de dados de conhecimentos do sistema - *“Repository of System Knowledge”*, e de causas de alarmes - *“Repository of Alarm Causes”*, que são entidades externas ao sistema. Essa análise é realizada através da execução das responsabilidades *“System Knowledge Analysis”* e *“Alarm Cause Analysis”*.

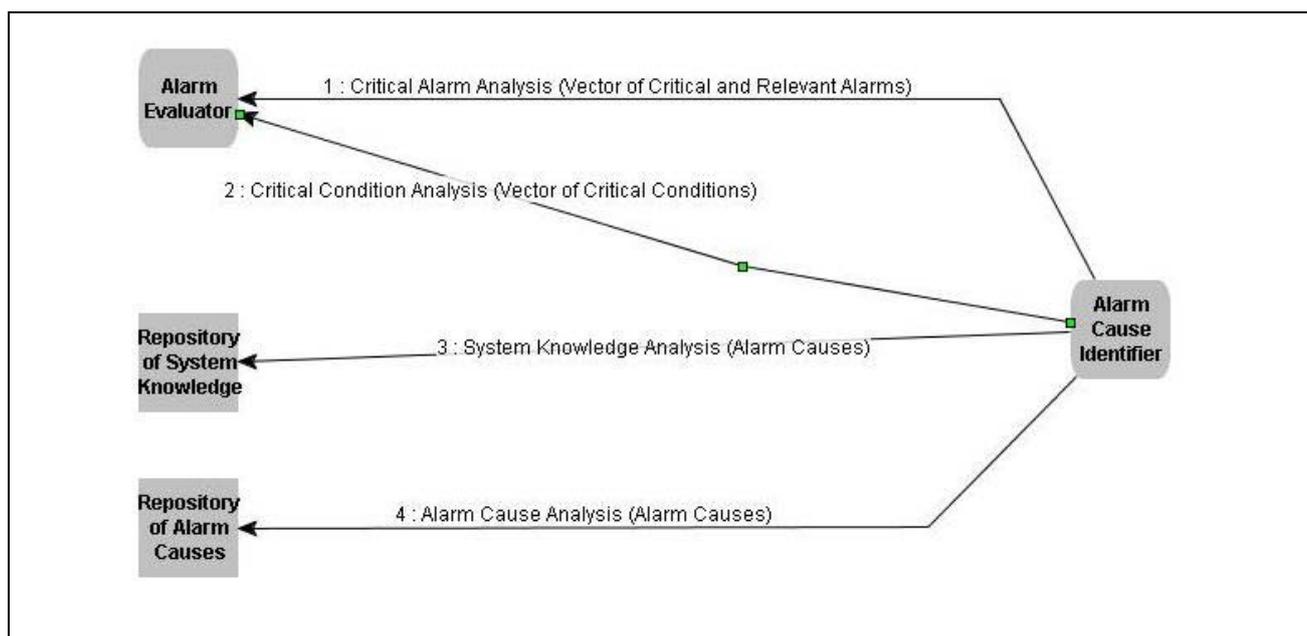


Figura 38 – Modelo de Interação entre Papéis – Identificação das causas do Alarme

5.5 Prototipação da Interface do Usuário

Finalizando a fase de Análise da Aplicação, tem-se a tarefa de Prototipação da Interface com o Usuário, onde se apresentam as possíveis interações de entidades externas, neste caso os usuários, com o sistema. A partir dos modelos criados nas tarefas anteriores, que são os modelos de conceitos, de objetivo, de papéis e de interações entre papéis, define-se um protótipo da interface com o usuário, inicialmente um rascunho, que pode ser refinado com auxílio de alguma ferramenta gráfica de desenvolvimento de interfaces.

5.5.1 Considerações Gerais sobre o Protótipo

Para desenvolvimento dos protótipos das interfaces, serão utilizados conhecimentos de “Arquitetura da Informação”, definidos por Peter Morville e Louis Rosenfeld [91]. O objetivo de se estar aplicando conhecimentos de arquitetura da informação deve-se ao fato de que para o sistema ser corretamente utilizado, o mesmo deve ser de fácil navegação e entendimento por todos. Peter Morville e Louis Rosenfeld [91] defendem que um usuário nunca deve se sentir perdido dentro de um site da web ou aplicação de sistema, a ponto de não saber voltar ao ponto inicial, ou de não conseguir localizar o que

realmente deseja dentro do sistema. No caso da aplicação em estudo, SIGARA, a navegação deve ser intuitiva e de fácil entendimento, principalmente para o usuário final que irá receber a recomendação; pois deve auxiliar os usuários em momentos críticos, onde o que menos se deseja é perder tempo com navegação.

A linguagem escolhida para o desenvolvimento do Protótipo foi Java, utilizando o pacote “Visual Web Pack” do NetBeans, versão 5.1.1 [92] [93]. O Java e o NetBeans são softwares e ferramentas de código aberto e livre, multiplataforma, de fácil acesso e alta performance. A tela do NetBeans com o protótipo da aplicação WebSIGARA é apresentada na Figura 39.

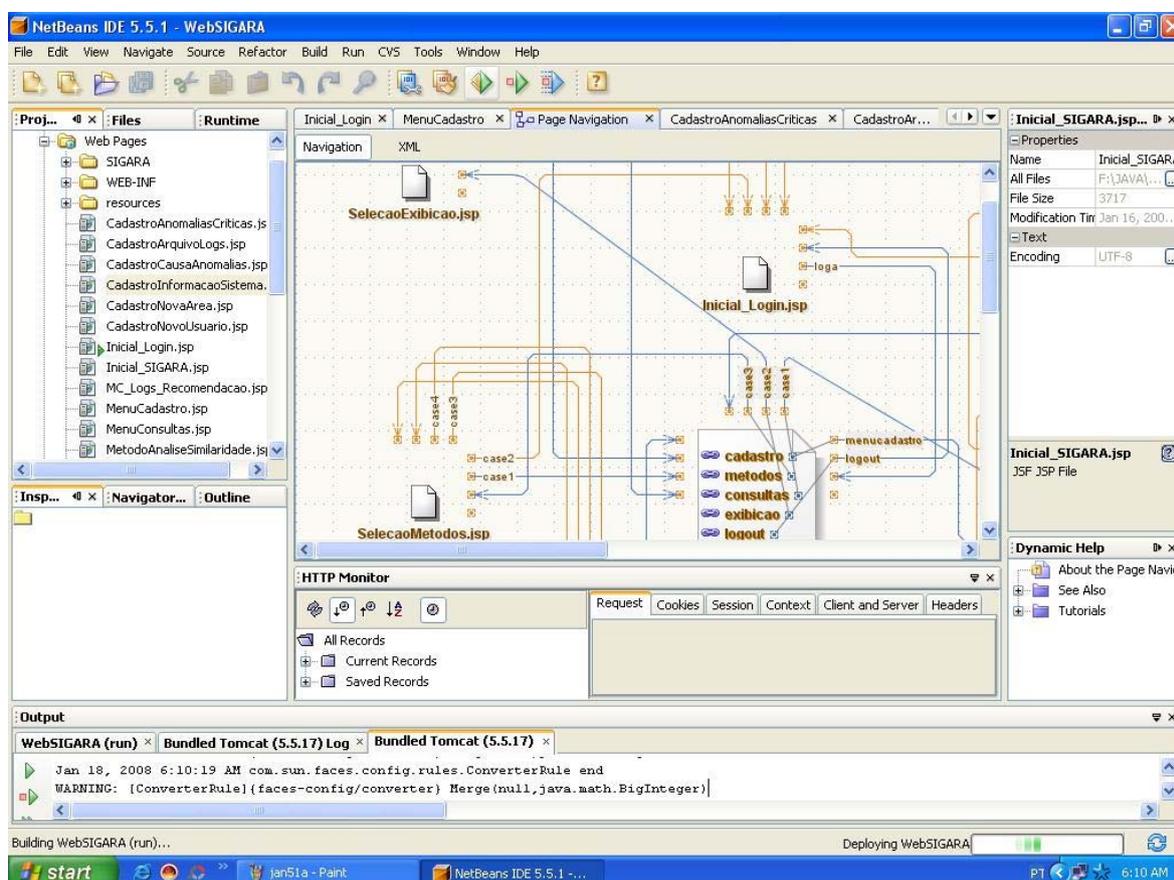


Figura 39 – Tela do aplicativo NetBeans IDE 5.5.1 utilizado para desenvolvimento do protótipo da WebSIGARA

A versão utilizada do NetBeans e do sistema operacional para desenvolver esse modelo são em Inglês, não apresentando corretamente alguns caracteres da língua portuguesa, como acentos.

Vale ressaltar ainda que devido ao fato da prototipação proporcionar uma visualização mais clara dos objetivos da aplicação, será realizada uma analogia entre suas principais funcionalidades exibida e seu relacionamento com os elementos dos modelos apresentados nas seções anteriores. Com essa analogia espera-se explicar de maneira gráfica esses conceitos, de uma forma mais didática. Porém, convém notar que nem todas os conceitos, objetivos, relacionamentos, etc. apresentados anteriormente nesses modelos podem ser explicitamente visualizados no protótipo, visto que alguns destes são contemplados internamente na aplicação, não sendo possível sua exibição em forma de interface gráfica.

5.5.2 Telas de cadastro da aplicação

A página inicial do protótipo é a tela de Autenticação do Usuário, apresentada na Figura 40, onde os usuários informam o seu login e sua senha para terem acesso ao sistema. O sistema irá checar a autenticação do usuário através desses dados, caso seja um novo usuário será exibido uma mensagem, para que ele acesse o sistema através do botão de Novo Usuário. Acionando esse botão, os novos usuários também poderão acessar o sistema, sendo necessário criar inicialmente um cadastro básico de “novo usuário”, recebendo assim liberação de acesso restrito, somente com opção de leitura e consulta - essa atividade cabe ao papel “*User Data Acquirer*” apresentado nas seções anteriores.

Ao informar o nome do usuário para o sistema e clicar no botão de Logar no SIGARA, esse usuário será checado pelo sistema, que irá buscar seu perfil e habilitar somente funções previstas no seu cadastro. Após checar o usuário através do papel “*Classifier*”, será apresentada uma lista das funções principais do SIGARA, no formato de navegação hierárquica [91]. Na navegação hierárquica quando se clica em um item, o sistema apresenta sub-opções de navegação permitindo que seja possível acessar as várias funcionalidades do sistema.

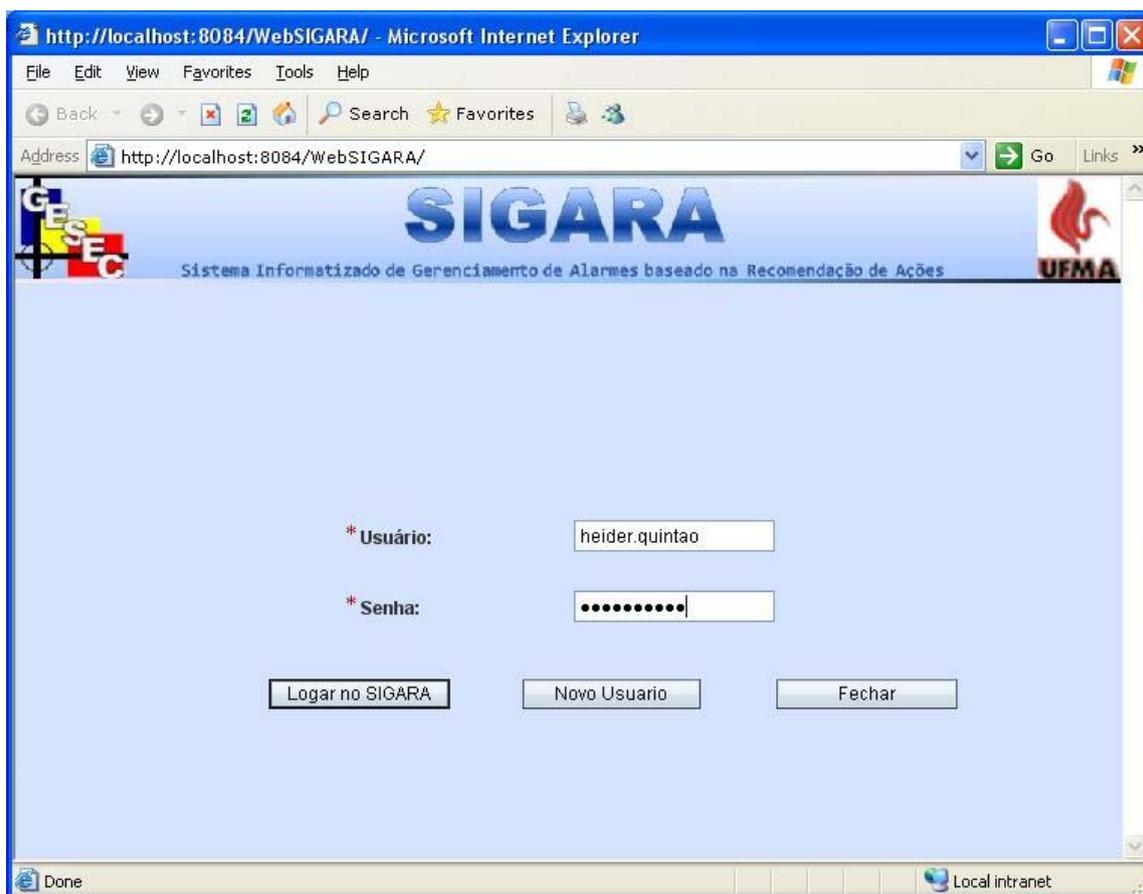


Figura 40 – Tela inicial de autenticação do usuário

Sendo o usuário um Operador do SIGARA, será aberta a tela apresentada na Figura 41 a seguir, onde estará liberado para navegação pelo operador somente as funções de Consulta e Seleção de Modos de Exibição. As outras opções estarão bloqueadas.



Figura 41 – Tela com a lista das funções principais para usuário Operador

Sendo o usuário um Administrador dos recursos do SIGARA, ou de maneira simplificada um Analista, será aberta a mesma tela mas com todas as opções de navegação liberadas: função de cadastro, seleção de métodos e algoritmos, função de consulta e seleção do modo de exibição, conforme Figura 42. Esse controle de exibição de funções é realizado pelo papel “*Classifier*” através da execução da responsabilidade “*Classification of Current User*”. Esse papel é responsável por classificar os usuários conforme seu modelo, para que as recomendações de ações sejam conforme sua necessidade, e além disso, realiza também o controle de acesso a funções do SIGARA.



Figura 42 – Tela com lista das funções principais para o usuário Analista

A partir de agora será explicada a navegação completa do sistema a partir do login de um usuário Analista, pois esse usuário possui acesso a todas as funcionalidades presentes no sistema, sendo que a navegação para os demais usuários será baseada nesse perfil, com as devidas limitações definidas na fase de cadastro.

As telas que serão apresentadas a seguir referem-se todas à função de Cadastro. Essas telas são de acesso restrito ao Analista ou de quem mais tiver essa funcionalidade no perfil. Essas telas irão permitir a configuração das principais funções do sistema, permitindo que o SIGARA possa utilizar corretamente todas essas funções, a partir dos dados cadastrados.

A tela de Menu de Cadastros permite que a partir dela o Analista possa navegar em todas as opções de cadastro existente no sistema, informando os dados necessários para o sistema de recomendação desempenhar corretamente suas funções.



Figura 43 – Tela com as Funções de Cadastro do usuário Analista

A partir do Menu de Cadastros, o Analista pode acessar a tela para cadastrar as Áreas de Responsabilidade, apresentada na Figura 44, podendo o Analista atribuir mais de uma responsabilidade para cada Área. A partir dessas áreas de responsabilidades cadastradas serão definidos os perfis dos usuários, perfis esses que serão utilizados nas tarefas de filtragem de alarmes e condições críticas, e também na recomendação das ações corretivas. Conforme apresentado no Modelo de Papéis que trata a Modelagem e Classificação dos Usuários na Figura 35, as áreas de responsabilidades são criadas de forma explícita pelo analista, a partir dos conhecimentos sobre o sistema que o analista possui.

The screenshot shows the SIGARA web application interface. At the top, there is a header with the logo 'GESEC' on the left, the title 'SIGARA' in large blue letters in the center, and the logo 'UFMA' on the right. Below the header, a navigation bar contains 'Menu de Cadastros', 'Inicial SIGARA', and 'Logout'. The main content area is titled 'Cadastro de Nova Area de Responsabilidade'. It features a dropdown menu for 'Areas de Responsabilidades Cadastradas' with 'Item 1' selected, and a text input field for 'Nome da Nova Area' containing 'Manutenção de Turno'. Below these are four columns of radio button options: 'Seleção de Responsabilidades' (Operacao, Manutencao Eletrica, etc.), 'Acesso a telas de Cadastro' (Nova Aea Responsabilidade, Novo Usuário, etc.), 'Acesso a telas de Consulta' (Aeas Responsabilidades, Usuários, etc.), and 'Acesso aos Métodos' (Classificação Usuário, Análise Similaridade, etc.). There are also 'Seleção Modo Exibição SIGARA' options (Ícone, Banner, SIGARA) and 'Seleção Modo Exibição Causas' options (Diagrama Espinha Peixe, FTA - Fault Tree Anal., Tabela). At the bottom right, there are 'Confirma' and 'Limpa' buttons.

Figura 44 – Tela de Cadastro das Áreas de Responsabilidades

Da mesma tela do Menu de Cadastros, o Analista pode selecionar a tela de Cadastro de Usuários apresentada na Figura 45, onde o Analista irá cadastrar o Usuário em função das Áreas de Responsabilidades que foram cadastradas na tela anterior, podendo atribuir apenas uma área de responsabilidade para cada usuário.

Na tela de cadastro de usuário o papel “*User Data Acquirer*” realiza a responsabilidade “*Explicit profile acquisition*”, capturando de maneira explícita os dados do usuário.

Quando o usuário que está tentando acessar o sistema não for ainda cadastrado – for um novo usuário, o seu acesso será liberado “parcialmente” para a tela de Cadastro de Usuário, que irá possuir visível apenas os campos que o usuário necessita preencher, que são o nome, login e senha. Os demais campos serão bloqueados, devendo o analista depois normalizar o cadastro desse novo usuário. Quando o novo usuário confirmar seus dados cadastrais a partir da tela de cadastro, será direcionado diretamente para a tela de Menu de Consultas (que será apresentado na Figura 52).

The screenshot shows the 'Cadastro de Novo Usuário' (New User Registration) page of the SIGARA system. The page header includes the GESEC logo, the title 'SIGARA', the subtitle 'Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendação de Ações', and the UFMA logo. A navigation bar contains 'Menu de Cadastros', 'Inicial SIGARA', and 'Logout'. The main content area is titled 'Cadastro de Novo Usuário' and contains the following fields and buttons:

Usuarios Cadastrados no Sistema:	<input type="text" value="Item 1"/>
Nome do Novo Usuario:	<input type="text" value="Heider Quintão"/>
Login:	<input type="text" value="hquintao"/>
Senha:	<input type="password" value="....."/>
Senha (repetir):	<input type="password" value="....."/>
Area de Responsabilidade:	<input type="text" value="Item 1"/>
<input type="button" value="Confirma"/>	<input type="button" value="Limpa"/>

Figura 45 – Tela de Cadastro do Usuário em função da área de responsabilidade

Na próxima tela apresentada na Figura 46, o Analista irá cadastrar as Anomalias Críticas, que abrangem os alarmes e as condições críticas. Para cada Anomalia Crítica será selecionado o sistema (conjunto de equipamentos) ao qual a anomalia fará referência, o estado operacional desse sistema no momento da ocorrência, e no caso do sistema possuir mais de um equipamento, selecionar o equipamento responsável pela geração da anomalia. A partir dessas seleções iniciais, na parte inferior da página serão apresentados as variáveis cadastradas no sistema, e o Analista poderá selecionar quais grandezas irão compor essa anomalia, indicando o valor dessa grandeza que irá disparar o alarme. Essa função de cadastro irá gerar os repositórios de condições críticas e de alarmes críticos, apresentados no Modelo de Papéis de Avaliação dos Alarmes, da Figura 33.

The screenshot shows the 'Cadastro das Anomalias Críticas' (Critical Anomalies Registration) screen. At the top, there is a header with the 'SIGARA' logo and the text 'Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendação de Ações'. Below the header, there are navigation links: 'Menu de Cadastros', 'Inicial SIGARA', and 'Logout'. The main content area is titled 'Cadastro das Anomalias Críticas' and contains the following form elements:

- Selecao da Anomalia Critica:** A dropdown menu with 'Item 1' selected.
- Sistema:** A dropdown menu with 'Item 1' selected.
- Equipamento:** A dropdown menu with 'Item 1' selected.
- Estado:** A dropdown menu with 'Item 1' selected.
- Modo de Operacao:** A dropdown menu with 'Item 1' selected.
- Selecionar Grandeza:** Three dropdown menus, each with 'Item 1' selected.
- Valor critico:** Three empty text input fields corresponding to the 'Selecionar Grandeza' dropdowns.
- Limites:** Three radio button options: 'Superior', 'Inferior', and 'Estado ...'.
- Estado ...:** Three radio button options: 'On' and 'Off'.

At the bottom of the form, there are two buttons: 'Salvar' (Save) and 'Limpar' (Clear).

Figura 46 – Tela de Cadastro de Anomalia Crítica

Semelhante à tela de Cadastro de Anomalias Críticas da Figura 46, a tela de Cadastro das Causas das Anomalias Críticas da Figura 47 permite que o Analista realize o cadastro das causas de maneira detalhada – caso não seja informado nenhuma causa para a anomalia crítica que foi criada, uma tela de aviso irá aparecer diariamente, solicitando a adição dessa informação. Esse cadastro irá gerar o repositório de dados que contém as causas dos alarmes – “*Repository of Alarm Causes*”, da Figura 34.

A tela de cadastro das Causas das Anomalias Críticas possui três opções para interface gráfica, sendo uma baseada no Diagrama de Ishikawa [94] (ou Diagrama Espinha de Peixe), outra no FTA (“*Fault Tree Analysis*”) e outra discursiva no formato de tabela (sem relacionamento entre as causas). O exemplo a seguir utiliza o diagrama de Ishikawa onde o Analista pode cadastrar as possíveis causas para o alarme que foi cadastrado através dessa metodologia. Assim, a partir dessas informações, o sistema irá filtrar as possíveis causas em função do estado do sistema e fazer a recomendação da ação mais adequada. Uma grande vantagem do uso do Diagrama de Ishikawa é que sua técnica é de conhecimento das equipes de manutenção e operação mais experientes, o que facilita a captura das informações relevantes sobre o sistema com essas equipes.

The screenshot displays the 'Cadastro das Causas das Anomalias' (Registration of Anomaly Causes) screen in the SIGARA system. At the top, the system name 'SIGARA' is prominently displayed, along with the logo of UFMA (Universidade Federal do Maranhão) and the text 'Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendação de Ações'. Navigation links include 'Menu de Cadastros', 'Inicial SIGARA', and 'Logout'.

The main content area features a 'Selecao da Anomalia:' dropdown menu currently set to 'Item 1'. Below this is a hierarchical tree diagram for selecting causes. The tree is organized into three main categories: 'MÉTODO', 'MÁQUINA', and 'MEIO AMBIENTE'. Under 'MÉTODO', there are 'Sobrecarga Motor' and 'Excedido num comandos'. Under 'MÁQUINA', there are 'Falha controle' and 'Falha sensor temp.'. Under 'MEIO AMBIENTE', there are 'Temp. elevada oleo' and 'Temp. elevada motor'. A central horizontal line connects these categories to a second level of options: 'Não especializada' (under Método), 'Oleo inadequado' (under Máquina), and 'Baixa pressao' and 'Nivel oleo baixo' (under Meio Ambiente). These options lead to three final categories: 'MÃO-DE-OBRA', 'MATERIAL', and 'MEDIDA'. A dropdown menu on the right side of the tree shows the 'Anomalia Seleccionada: FALHA GERAL DA UNIDADE HIDRAULICA'. At the bottom of the tree, there are 'Salvar' and 'Limpar' buttons.

Figura 47 – Tela de Cadastro das Causas das Anomalias Críticas

Na tela da Figura 48 apresenta-se o Cadastro das Informações do Sistema, onde será detalhado as ações recomendadas para cada possível causa cadastrada na tela de Cadastro das Causas das Anomalias Críticas da Figura 47. Esse cadastro irá gerar o repositório de dados de informações e conhecimentos do sistema – “*Repository of System Knowledge*”, que será utilizado pelo papel “*Alarm Cause Identifier*” que ao definir as prováveis causas para a anomalia crítica – “*Alarm Causes*”, irá também gerar as recomendações de ações aqui cadastradas.

SIGARA
Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendação de Ações

Menu de Cadastros Inicial SIGARA Logout

Cadastro das Informacoes e Conhecimentos do Sistema

Selecao da Anomalia Critica:

Causa da Anomalia	Acao Recomendada para solucionar a anomalia
Temperatura Elevada Oleo	Checar nivel do oleo, checar temperatura da sala, checar sistema trocador de calor
Temperatura Elevada Motor	Checar acoplamento, checar nivel do oleo, checar temperatura da sala, checar
Vazamento de Oleo	Checar nivel do oleo, checar tubulacoes, checar retentores
Falha Sistema de Controle	Checar disjuntor de controle, checar estado rede, checar rede
Baixa pressao do Oleo	Checar nivel oleo, checar vazamento, checar sensor de pressao

Salvar Limpar

Figura 48 – Tela de Cadastro das Informações e Conhecimento do Sistema

A próxima tela apresentada na Figura 49 tem o objetivo de definir para o SIGARA o local onde os arquivos de registros gerados pelo sistema estão armazenados para consulta e análise. Esses arquivos de registro, normalmente chamados de “logs”, podem estar armazenados em pastas diferentes, sendo necessário informar para o SIGARA corretamente a pasta em que ele se encontra e o seu tipo, para que possa ser corretamente acessado pelo sistema. Essa interface permite ao Analista selecionar vários arquivos simultaneamente, de modo que o sistema poderá analisar logs de várias funções e sistemas simultaneamente.

Esses arquivos compõem os repositórios de registros do sistema de automação industrial, que são as entidades externas “*Repository of Events Log*”, “*Repository of Operational Status Log*” e “*Repository of Alarm Log*” apresentadas no Modelo de Objetivos da Figura 30.

SIGARA
Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendação de Ações

Menu de Cadastros Inicial SIGARA Logout

Cadastro dos Arquivos de Logs do Sistema

Tipo do Arquivo de origem dos registros/logs:

Alarme
 Evento
 Estado Operacional

Selecao do Arquivo:

Cadastro dos Arquivos		
Nome do Arquivo	Tipo do Arquivo	Local
row1_column3	row1_column2	row1_column3
row1_column3	row2_column2	row2_column3
row1_column3	row3_column2	row3_column3
row1_column3	row4_column2	row4_column3
row1_column3	row5_column2	row5_column3

Figura 49 – Tela de Cadastro dos Arquivos de Registro

5.5.3 Telas de seleção dos métodos da aplicação

A tela com a função de seleção dos métodos apresentada na Figura 50 permite que o Analista possa selecionar o método desejado, o qual deve estar devidamente cadastrado e testado no sistema. Como essa seleção pode também ocorrer em tempo de operação, o sistema permite que o analista possa simular rapidamente a operação do sistema com os vários métodos cadastrados, realizando comparação entre as respostas geradas.

Esses métodos estão também presentes nos modelos de papéis apresentados anteriormente, pois para cada papel (“*Role*”) que se encarrega de realizar uma ou mais responsabilidades, deve-se definir os conhecimentos ou habilidades (“*Skill*”) necessários para esse papel. São esses os conhecimentos, destrezas ou habilidades que o papel vai necessitar possuir para realizar sua responsabilidade que se chama de métodos.



Figura 50 – Tela com as Funções de seleção dos métodos e algoritmos do SIGARA

A seleção dos métodos apresentada na Figura 50 permite que o usuário possa selecionar o método desejado, com a opção de simulação. Dentre os vários métodos possíveis para cada função, são citados os métodos apresentados no Capítulo 3, por exemplo para Classificação do Usuário como a seleção da técnica de filtragem baseada em conteúdo através da seleção do método de clusterização mais adequado, conforme os métodos apresentados na Seção 3.1; e também a Análise de Similaridade, tendo como opção a seleção entre os métodos de similaridade estudados na Seção 3.1.1 e testados na Seção 3.3.1, como Similaridade do Cosseno e do Produto Interno, que foram utilizados em um estudo de caso usando filtragem baseada em conteúdo.

Na Figura 51 a seguir, apresenta-se a tela de seleção do método de análise de similaridade, que possibilita o usuário realizar simulações e testes com os métodos já configurados no sistema.

SIGARA
Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendacao de Acoes

Selecao de Metodos Inicial SIGARA Logout

Selecao do Metodo de Analise de Similaridade

Distancia Euclideana
 Produto Interno
 Cosseno
 Espaco Vetorial

Confirma
Limpa

Figura 51 – Tela de seleção dos Métodos para Análise de Similaridade

5.5.4 Telas de consulta dos registros do SIGARA

A tela com a função de consulta aos registros do SIGARA é apresentado na Figura 52, permitindo ao usuário final – o Operador, bem como ao Analista, a consulta de todos os dados cadastrados no SIGARA; como o cadastro de usuários e de áreas de responsabilidades. Permite também a visualização de todos os dados usados e gerados pelo sistema, como os arquivos de logs de alarmes e eventos provenientes dos sistemas de automação industrial, o resultado da filtragem e priorização desses logs, com a visualização dos alarmes críticos e condições críticas, e também das ações recomendadas aos usuários.



Figura 52 – Tela com as Função de consulta de todos os dados do SIGARA

A Figura 53 apresenta a tela de consulta dos registros de anomalias críticas. A tela apresenta inicialmente uma tabela, ordenada pela hora, de todos os alarmes e condições críticas registrados pelo sistema. Selecionando um alarme histórico desejado, ou o atual, abre-se o Diagrama de Ishikawa, com todas as possíveis causas que foram cadastradas, porém, o sistema recomenda a possível causa de forma destacada, nesse caso com moldura vermelha. Com essa interface, o usuário terá à sua disposição todos os dados necessários para sua avaliação, sendo essa tela de grande ajuda.

A partir do momento que o sistema for recomendando as causas para anomalias críticas, e essas causas forem corretas, o sistema irá se ajustando para recomendar sempre as causas mais corretas. Para uma maior flexibilidade para essa funcionalidade, várias técnicas podem ser implementadas, ficando a disposição dos analistas para testes e simulações, como por exemplo inteligência artificial ou recomendação colaborativa, explicadas nos capítulos anteriores – funcionalidades essas que não são objeto deste trabalho.

The screenshot displays the SIGARA (Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendação de Ações) interface. At the top, there are logos for GESEFC and UFMA, and the title 'SIGARA'. Below the title, it says 'Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendação de Ações'. The navigation bar includes 'Menu de Consultas', 'Inicial SIGARA', and 'Logout'.

The main content area is titled 'Consulta Registro das Anomalias Criticas'. It features a search bar with the text 'Consulta Registro de Anomalia Critica:' and a list of critical anomalies with their timestamps:

- 20:40 Falha Geral da Unidade Hidráulica (highlighted in yellow)
- 21:22 Falha Sistema de Lubrificação Rolos
- 22:12 Falha posição carro de Lingotamento
- 22:55 Falha posição carro de Ligotamento
- 23:11 Falha acionamento carro de Lingotamento

Below the list are two buttons: 'Consulta' and 'Limpar'. A fishbone (Ishikawa) diagram is shown, illustrating the causes of the selected anomaly. The diagram is structured as follows:

- MÉTODO** (Method) - No specific causes listed.
- MÁQUINA** (Machine) - Causes include 'Falha controle' and 'Falha sensor temp.'.
- MEIO AMBIENTE** (Environment) - Causes include 'Temp. elevada oleo' and 'Temp. elevada motor' (highlighted in yellow).
- MÃO-DE-OBRA** (Manpower) - Cause is 'Não especializada'.
- MATERIAL** (Material) - Cause is 'Oleo inadequado'.
- MEDIDA** (Measurement) - Causes are 'Baixa pressão' and 'Nivel oleo baixo'.

On the right side of the diagram, a dropdown menu shows the selected anomaly: 'Anomalia Selecionada: FALHA GERAL DA UNIDADE HIDRAULICA'.

Figura 53 – Tela de consulta do registro de alarmes e condições críticas, com a opção da apresentação gráfica da possível causa

A Figura 54 apresenta a tela de consulta das recomendações de ações para os registros de anomalias críticas. Essa tela apresenta inicialmente uma tabela, ordenada pela hora, de todos as anomalias críticas registrados pelo sistema. Selecionando uma anomalia histórica desejada, ou a atual, abre-se o Diagrama de Ishikawa, com todas as possíveis causas que foram cadastradas com indicação da possível causa de forma destacada – semelhante à tela anterior, porém esse diagrama é menor, pois a tela possui além dessas informações, o texto da ação que foi recomendada. Com essa interface, o usuário terá à sua disposição todos os dados necessários para a avaliação da causa do alarme, e da ação proposta. Automaticamente o sistema apresenta a ação recomendada para a causa proposta. Caso o usuário queira consultar as recomendações das outras possíveis causas, basta clicar sobre elas.

The screenshot displays the SIGARA web application interface. At the top, there are logos for GESEFC, SIGARA, and UFMA. Below the logos, the text reads 'Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendação de Ações'. The navigation bar includes 'Menu de Consultas', 'Inicial SIGARA', and 'Logout'. The main section is titled 'Consulta Recomendações'. On the left, there are buttons for 'Consulta' and 'Limpar'. The central area shows a search result for a critical anomaly: '20:40 Falha Geral da Unidade Hidraulica'. Below this, it lists recommended actions: 'Checar nível d eÓleo, Checar temperatura da Sala, Checar Sistema do Trocador de Calor'. A hierarchical tree diagram is shown, with categories like 'MÉTODO', 'MÁQUINA', 'MEIO AMBIENTE', 'MÃO-DE-OBRA', 'MATERIAL', and 'MEDIDA'. A selected anomaly is highlighted in yellow: 'Falha sensor temp.' under 'MÁQUINA' and 'Temp. elevada motor' under 'MEIO AMBIENTE'. A dropdown menu on the right shows 'Anomalia Seleccionada: FALHA GERAL DA UNIDADE HIDRAULICA'.

Figura 54 – Tela de consulta do registro de ações recomendadas para as anomalias críticas

5.5.5 Interface do SIGARA para seleção do modo de Exibição

O SIGARA poderá ser utilizado de duas formas: em uma estação cliente dedicada funcionando paralelamente à estação de supervisão e controle da planta ou sendo executado na mesma estação. As telas de interface com o usuário final do SIGARA, nesse caso principalmente a equipe de manutenção e operação, apresentam três soluções de exibição do sistema, conforme apresentado na Figura 55 , sendo detalhado a seguir a primeira opção.



Figura 55 – Tela com a Seleção dos modos de exibição do SIGARA

Nessa opção, ao se selecionar “Ícone” e confirmar a alteração, a aplicação SIGARA será minimizada, aparecendo um ícone em um dos cantos da tela, com um símbolo para a Anomalia Crítica Geral, e um ícone para a tela/sistema em exibição no supervisão. O ícone mudará de cor em função do status do sistema, conforme apresentado na tela da Figura 56.

Na tela do sistema de supervisão e controle, no modo de apresentação Ícone se tem três botões na tela, sendo:

- **SIGARA** – ao ser acionado pelo usuário, irá abrir a aplicação SIGARA no modo maximizado sobrepondo a tela do sistema de controle e automação;
- **GERAL** – é um botão que representa o estado do sistema de uma forma geral. Quando ocorrer alguma anomalia crítica relevante para todo o sistema, o botão irá mudar de cor indicando que o sistema apresenta uma falha grave. Acionando esse botão, a aplicação SIGARA será aberta já na tela de consulta de anomalias críticas, exibindo todos os registros da aplicação, destacando o registro que gerou a condição de falha;

- **Local** – esse botão tem indicação e funcionalidade semelhante ao botão **GERAL**, com a diferença que o botão **Local** indica o status operacional do sistema ou equipamento que está sendo apresentado na tela. Ao ser acionado, também abrirá a aplicação SIGARA na página de consulta, porém irá filtrar e exibir os registros somente do sistema ou equipamento que estava sendo exibido. Para plantas industriais complexas, onde para cada sistema tem-se um operador, essa tecla local é de maior utilidade, pois irá filtrar os registros apresentando somente aqueles que sejam de interesse do usuário, referente à tela que estava em uso.

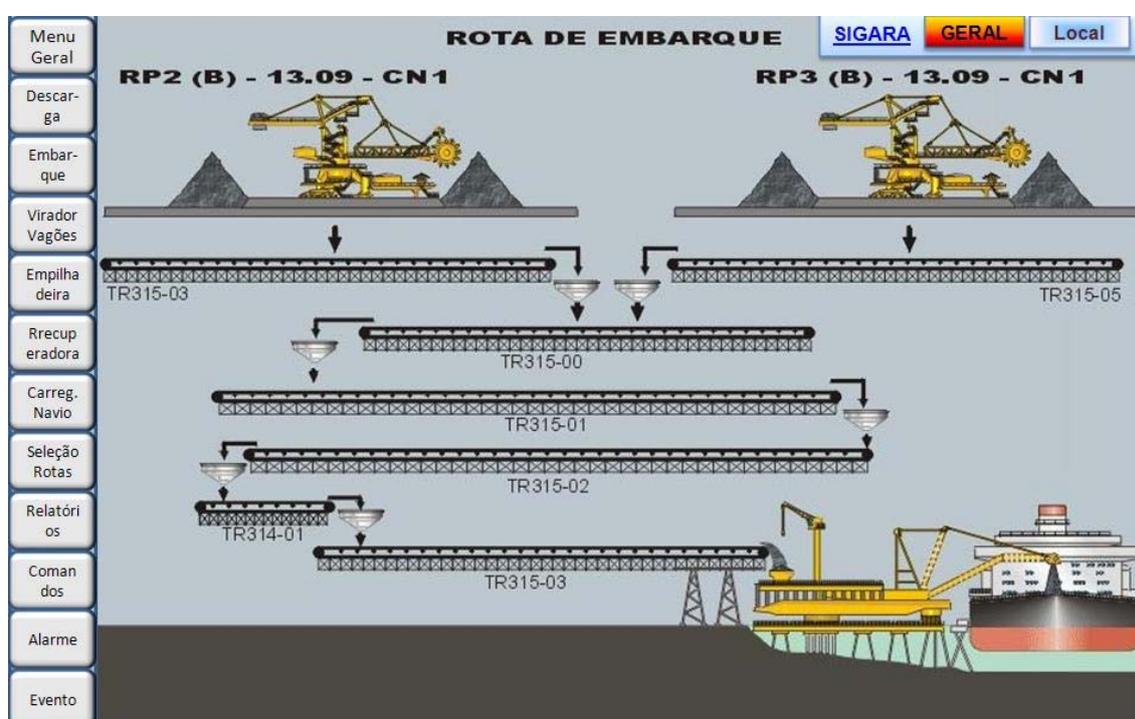


Figura 56 – Tela do sistema de automação e controle industrial, com o modo de exibição ÍCONE do SIGARA

No modo de exibição **Banner**, apresentado na Figura 57, a aplicação do SIGARA também será minimizada, aparecendo sobreposto à aplicação do sistema de automação e controle um banner (uma janela). Quando o usuário desejar, pode maximizar o banner, entrando na aplicação do SIGARA. Esse Banner terá duas áreas distintas: uma área Geral para apresentar anomalias críticas de todo o sistema, e outra para apresentar anomalias críticas do sistema em exibição.

A grande diferença desse modo de exibição para o anterior, é que além de indicar o estado operacional da planta industrial como um todo e do sistema ou equipamento em exibição na tela, são apresentados também o texto descritivo das anomalias - alarmes relevantes e condições críticas. Caso o usuário deseje acessar o SIGARA para consultar registros históricos dos alarmes, condições críticas e também as recomendações de ações realizadas, basta acionar o botão desejado. Clicando-se no botão SIGARA abre-se o aplicativo; no botão Causas abre-se a janela das Causas e Efeitos; e no botão Ações a tela de Recomendação de Ações, filtrando conforme área em que esses botões estão localizados (Geral ou Local).

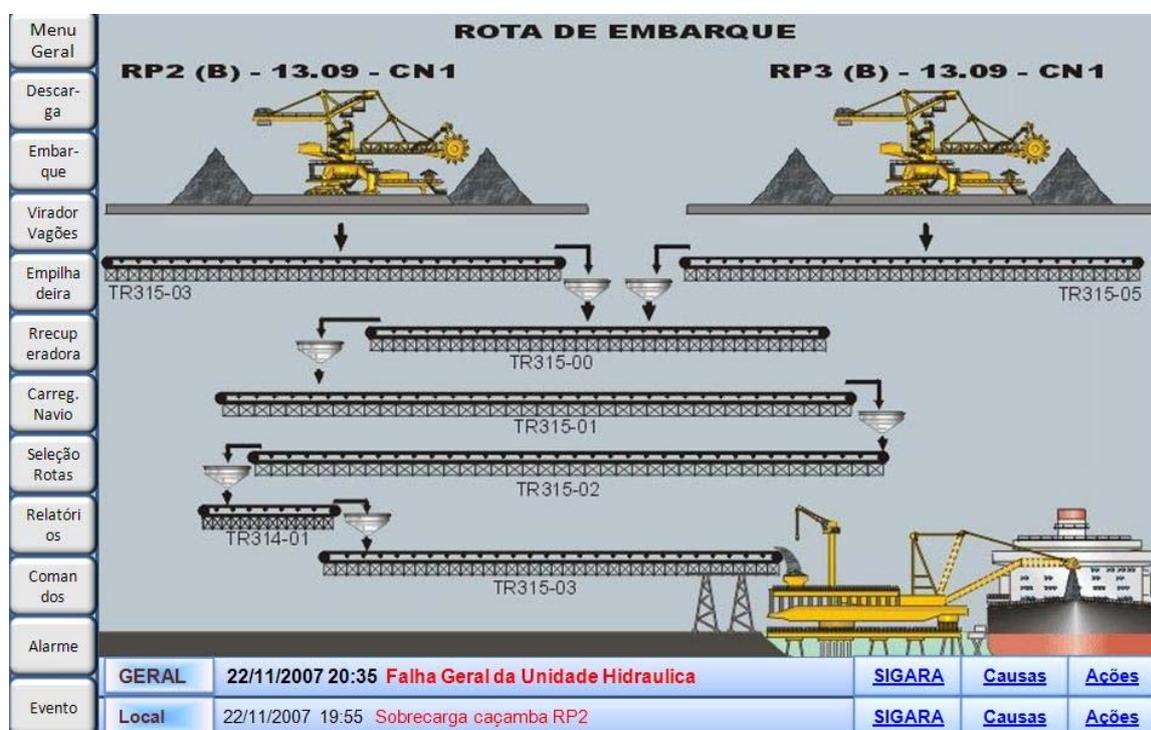


Figura 57 – Tela do sistema de automação e controle industrial, como modo de exibição BANNER do SIGARA

Clicando nas **Causas** da Falha Geral, abre-se uma janela com a apresentação gráfica das possíveis causas: a forma de exibição pode ser “Espinha de Peixe”, “FTA” ou “Tabela”. Nesse caso, será utilizado como exemplo “Espinha de Peixe”, onde a possível causa é ressaltada através da mudança de cor do seu quadro. Esse modo de exibição é bem prático, pois não sobrepõe totalmente a aplicação do sistema de automação e controle industrial, ficando sobreposta parcialmente, conforme apresentado na tela da Figura 58.

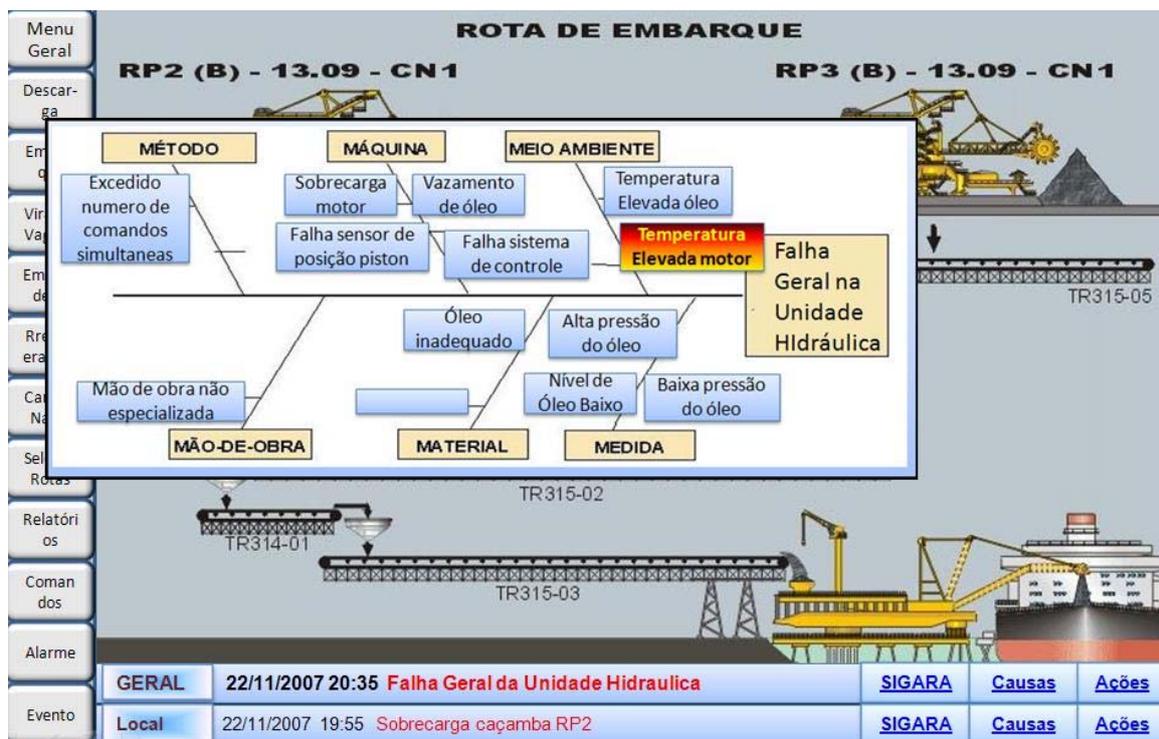


Figura 58 – Tela do sistema de automação e controle industrial, como modo de exibição BANNER do SIGARA, exibindo possíveis causas através do Diagrama de Ishikawa

Para o mesmo modo de exibição Banner, clicando nas **Causas** da Falha Geral, abre-se uma janela com a apresentação gráfica das possíveis causas. Nesse caso agora se tem um “FTA” – árvore de análise de falhas, que é outro modo de exibição das causas, sendo a possível causa ressaltada, conforme apresentado na tela da Figura 59 com preenchimento da moldura com outra cor.

Na terceira opção de modo de exibição, **SIGARA**, o SIGARA irá ser executado em tela cheia, devendo o usuário usar teclas de controle para trocar da aplicação do sistema de supervisão para o SIGARA, conforme apresentado anteriormente na Figura 55, por exemplo. Pode também ser configurado um link para troca das telas entre os sistemas.

Para todos os modos de exibição, no caso de “**Alta Criticidade**” um banner irá para o meio da tela apresentando a causa provável e uma ação recomendada para o operador.

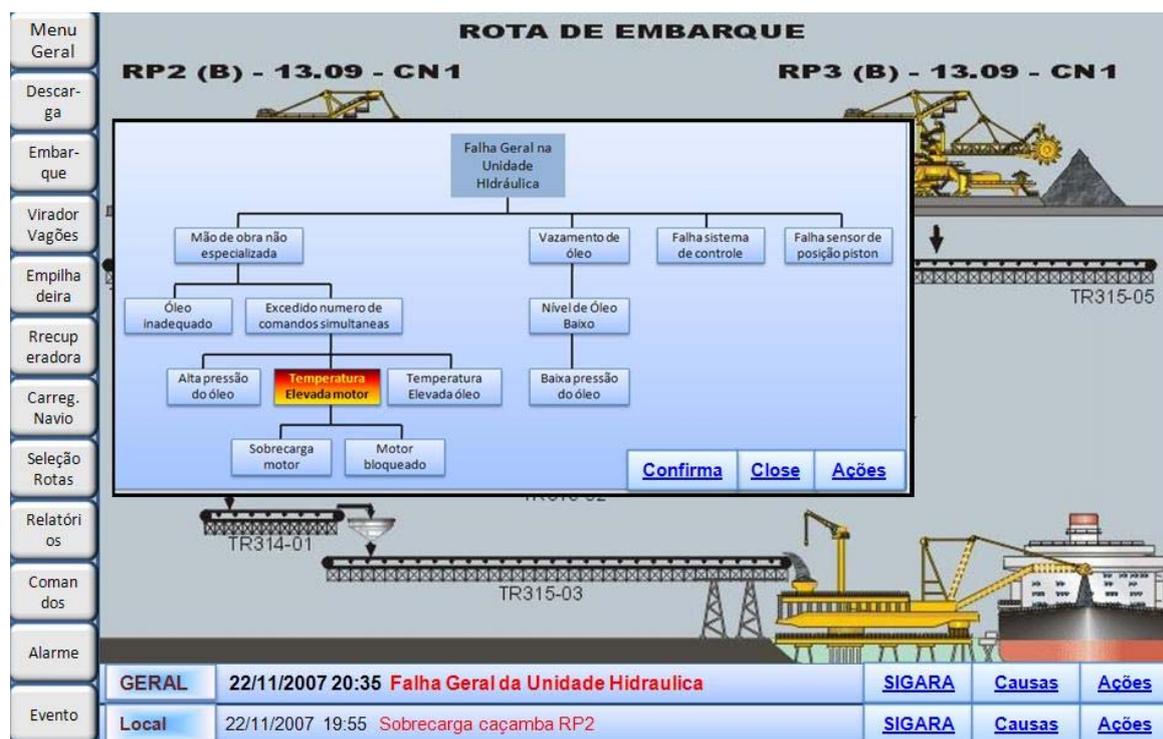


Figura 59 – Tela do sistema de automação e controle industrial, como modo de exibição BANNER do SIGARA, exibindo possíveis causas através do FTA

5.6 Considerações Finais sobre a Análise e Especificação da Aplicação

Conforme nossa expectativa, a realização das tarefas presentes na fase de análise da aplicação na ontologia ONTORMAS, conforme metodologia MAAEM, proporcionaram uma visualização mais detalhada das funcionalidades necessárias para a aplicação do SIGARA. Através dos modelos de conceitos e objetivos se pode definir detalhadamente os objetivos necessários, realizando várias referências a métodos e funções apresentadas nos sistemas pesquisados no Capítulo 2 e 3, porém a representação desses conceitos ficou mais completa, ao adicionarmos os relacionamentos entre esses conceitos. Através do modelo de papéis pôde-se obter de uma maneira clara a representação de todos os conceitos necessários para se atingir esses objetivos. A prototipação proveu um maior entendimento do funcionamento do SIGARA, tendo em vista que permitiu uma visão mais próxima da aplicação em seu estágio final. Tal visualização proporcionou também refinamentos complementares nos modelos desenvolvidos anteriormente, tais como: correções e ajustes, introdução de novos conceitos e relacionamentos, melhor visibilidade

das responsabilidades desempenhadas pelos papéis de modo a suportar os objetivos específicos.

6. CONCLUSÃO DO TRABALHO

Este trabalho apresentou a análise e especificação dos requisitos de um Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendação de Ações (SIGARA), aplicando a metodologia MAAEM e a ontologia ONTORMAS.

A especificação da aplicação SIGARA desenvolvida apresenta assim dois grandes diferenciais frente aos SIGAs existentes hoje no mercado, sendo o primeiro diferencial o uso de técnicas de filtragem de informação, que irão filtrar os alarmes e as ações que o sistema irá recomendar aos usuários de maneira diferenciada, de modo que os operadores receberão alarmes e ações que dizem respeito à sua responsabilidade; os outros usuários também receberão alarmes e ações customizadas, diferenciando usuários da manutenção, engenharia e segurança, por exemplo. Outros sistemas apresentam ações em função do estado operacional da planta industrial, porém, o SIGARA através das técnicas de filtragem, executará essa função de maneira mais diferenciada ainda, pois filtrará os estados e alarmes antes de recomendar as ações, apresentando novamente, somente o que diz respeito a certo grupo de usuários. Com isso, reduz-se drasticamente a sobrecarga dos usuários por não estarem recebendo alarmes e ações que não lhes dizem respeito, agilizando o processo de tomada de decisões e garantindo um retorno mais rápido à condição normal de operação.

O segundo diferencial presente nesse estudo diz respeito ao uso da metodologia MAAEM e ontologia ONTORMAS, que apresentam grande capacidade para expressar um domínio de conhecimento, neste caso o gerenciamento de alarmes de sistemas industriais, através do uso de ferramentas de modelagem, utilizando aquelas que mais se adéquam ao contexto analisado para gerar modelos desse conhecimento. O uso conjunto de ontologias e agentes fazem com que essa modelagem seja muito mais poderosa que modelagens normais, baseadas em orientação a objetos e textos descritivos. Como explicado anteriormente, os agentes são muito mais poderosos que objetos ou classes, podem ser desenvolvidos em paralelo ou separado facilitando a sua engenharia, e quando formam um sistema multiagente o resultado final é sempre melhor do que os resultados dos agentes de maneira individual. As ontologias são também mais poderosas do que diagramas de fluxo de dados ou outros gráficos para explicitar o conhecimento. As ontologias são consideradas estruturas ideais para representação do conhecimento, pois

facilitam a captura do conhecimento armazenado por possuírem alto nível de representatividade semântica, bem como formalidade, reusabilidade e adaptabilidade, dentre outros. Isso permite não apenas o aumento na produtividade e qualidade da produção de software, mas também a criação de produtos cada vez mais inteligentes e capazes de otimizar a execução de tarefas e o suporte na tomada de decisões. Além disso, o uso do *Protégé* para representar graficamente as ontologias através do ambiente desenvolvido pelo GESEC auxilia as tarefas de desenvolvimento dos modelos, suportando, através da metodologia MAAEM, refinamentos da aplicação em questão, bem como o seu reuso e desenvolvimento futuro.

Obteve-se como resultado final, uma representação dos requisitos de um SIGARA, cobrindo a lacuna existente no mercado que não possui modelos de SIGA e SIGARA aceitos por todos, permitindo inclusive que esses modelos possam servir de base para desenvolvimentos futuros sendo reutilizados por outros estudiosos da área, podendo vir a receber novos conceitos ou serem adequados para outros domínios de conhecimento.

6.1 Resultados e Contribuições

Apresenta-se abaixo as principais contribuições decorrentes dos resultados obtidos ao longo deste trabalho:

- Modelo de um Sistema Informatizado de Gerenciamento de Alarmes baseado na Recomendação de Ações (SIGARA), que realiza a filtragem das anomalias críticas, e apresenta aos usuários somente as que são relevantes e necessitam tomar uma ação (essa filtragem leva em consideração o perfil do usuário, o estado operacional do equipamento, e a criticidade dessa anormalidade conforme um banco de dados de criticidade e relevância), e também a recomendação personalizada dessas ações em caso de falhas no sistema (através de técnicas de filtragem da informação e de árvore de análise de falhas, realizadas a partir de um banco de dados de conhecimento do sistema);
- Adicionalmente, o SIGARA apresenta funcionalidades presentes em vários SIGA e CCM de mercado, mas nenhum desses sistemas apresenta uma flexibilidade de seleção, simulação e uso desses métodos. Geralmente os modelos existentes não

são genéricos, sendo focados em uma solução específica, e não possuem essa flexibilidade;

- Demonstração prática de como o desenvolvimento de sistemas a partir da representação do conhecimento através de ontologias, com uso de metodologias e ferramentas orientadas a agentes podem contribuir para a concepção de sistemas com qualidade, além da redução do tempo de desenvolvimento e, conseqüentemente, do custo das aplicações;
- Com esse trabalho conseguiu-se também observar na prática o poder da abstração do agente para a modelagem de problemas complexos. Basta observar, que se estivesse trabalhando com qualquer outro paradigma computacional na construção do SIGARA, se estaria falando em componentes, chamadas a procedimentos remotos e programação concorrente. Porém, na abordagem multiagente, o desenvolvimento se baseou em agentes de software, troca de mensagens e comportamentos, tendo assim a distância cognitiva reduzida, o que facilita o entendimento da aplicação e a sua modelagem;
- Com o estudo e a análise do estado da arte dos SIGA e CCM existentes no mercado, propõe-se o resultado deste trabalho como uma proposta de especificação para um SIGARA.

6.2 Perspectivas Futuras

Como proposta de trabalho futuro, tem-se a continuação da aplicação da metodologia MAAEM com a ontologia ONTORMAS ao SIGARA, com o projeto e implementação da aplicação. Além das tarefas presentes na MAAEM que ainda não foram realizadas, pode-se também melhorar os modelos apresentados, inserindo novos conceitos e novas responsabilidades, como por exemplo, uma avaliação da ação realizada, de modo a checar a sua eficácia, alimentando e refinando a base de conhecimento do SIGARA.

Tendo em vista que SIGARA é um tema por demais extenso e um vasto campo a ser explorado, a ferramenta proposta possui apenas algumas funcionalidades consideradas por nós relevantes a partir das pesquisas e estudos realizados, as quais se acredita dar

suporte a necessidades reais do domínio em questão. Mesmo assim, a implementação prática de todas estas funcionalidades seria por demais extensas para o escopo deste trabalho. Contudo, se reconhece que tal ferramenta ainda pode ser bastante aperfeiçoada, pois essa primeira versão contemplou apenas o necessário para o objetivo ao qual este trabalho se propôs, conforme citado anteriormente.

Sendo assim, é sugerida como trabalhos futuros a conclusão das fases de projeto da aplicação e implementação da aplicação, conforme metodologia MAAEM. Tal sugestão decorre do fato que o tema Gerenciamento de Alarmes e Recomendação de Ações está com o seu uso crescente, podendo trazer ganhos de até 2% na produtividade de uma planta industrial, com investimentos de cifras bem menores do que as de aumento de produção através do investimento em novos equipamentos.

7. REFERÊNCIAS BIBLIOGRÁFICAS

1. **ARC Advisory Group.** Use Critical Condition Management to Improve Your Bottom Line. *ARC Strategies*. April 2002.
2. **Ribeiro, Marco Antonio.** *Automação Industrial*. Salvador : Tek Treinamento Consultoria, 1999.
3. **White, Percival e Arnold, Pauline.** *A Era da Automação*. Rio de Janeiro, RJ : Lidador Ltda, 1993.
4. **O'Brien, Larry and Woll, Dave.** Alarm Management Strategies. *ARC Strategies*. November 2004.
5. **Quintão, Heider.** *Estrutura da Rede Industrial do TPPM*. São Luis, MA CVRD, 2005.
6. **Hill, Dick.** Time To Re-Think Alarm Management Strategies. *ARC INSIGHT 049MH&MP*. 2001.
7. **HSE.** *The explosion and fires at the Texaco Refinery, Milford Haven, 24 July 1994: A report of the investigation by the Health and Safety Executive into the explosion and fires on the Pembroke Cracking Company Plant at the Texaco Refinery*. s.l. : HSE Books, 1994. ISBN 0 7176 1413 1.
8. **EEMUA.** The British Engineering Equipment and Materials Users Association. [Online] EEMUA. <http://www.eemua.co.uk>. Acesso em 5 de Maio de 2007.
9. **EEMUA.** Alarm systems, a guide to design, management and procurement. No. 191 *Engineering Equipment and Materials Users Association*. 1999.
10. **Labor, United States Department of.** Occupational Safety & Health Administration. OSHA. [Online] [Cited:] <http://www.osha.gov/>. Acesso em 11 de Abril de 2007.
11. **Labor, United States Department of.** Process safety management of highly hazardous chemicals. - 1910.119. *Occupational Safety & Health Administration - Regulations (Standards - 29 CFR)* . [Online] http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=9760. Acesso em 19 de Abril de 2007.
12. **HSE.** The British Health Safety Executive. [Online] HSE. <http://www.hse.gov.uk/comah/sragtech/>. Acesso em 4 de Fevereiro de 2007
13. **HSE.** Better Alarm Handling. *HSE Chemical Sheet number 6*. 2001.

14. **ISA.** Instrumentation, Systems, and Automation Society. [Online] ISA. <http://www.isa.org/> . Acesso em 4 de Fevereiro de 2007
15. **ISA.** Technical Report ISA – TR91.00.02–2003 - Criticality Classification Guideline for Instrumentation. *ISA - The Instrumentation, Systems, and Automation Society. International Standard.* January de 2003.
16. **ISA.** Standard ISA—18.1—1979 (R2004] - Annunciator Sequences and Specifications. *ISA - The Instrumentation, Systems, and Automation Society. International Standard presented at ISA EXPO.* 2005.
17. **Dunn, D. G. and others.** ISA SP-18 – Alarm Systems Management and Design Guide. *ISA EXPO 2005. Illinois USA.* October 25-27, 2005.
18. **IEC.** International Electrotechnical Commission. [Online] IEC. <http://www.iec.ch/>. Acesso em 5 de Dezembro de 2006.
19. **IEC.** IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. *International Standard IEC 61.508-1.* First Edition, December 1998.
20. **IEC.** IEC 61511 - Functional Safety: Safety Instrumented Systems for the Process Industry Sector. *International Standard IEC 61.511-1.* First Edition, January 2003.
21. **ASM.** The Abnormal Situation Management. [Online] ASM. <http://www.asmconsortium.com/>. Acesso em 10 de Novembro de 2006.
22. **ARC.** ARC Advisory Group. [Online] ARC. <http://www.arcweb.com/default.aspx>. Acesso em 10 de Novembro de 2006.
23. **Chemtech.** Chemtech - A Siemens Company. [Online] Chemtech. <http://chemtech.com.br/>. Acesso em 19 de Março de 2007.
24. **ProSysinc.** Process Systems Consultants. [Online] ProSysinc. <http://www.prosysinc.com/>. Acesso em 21 de Janeiro de 2007.
25. **Arts, Control.** Control Arts. [Online] Control Arts Inc. <http://controlartsinc.com/>. Acesso em 10 de Novembro de 2006.
26. **PAS.** Process Automation Services. [Online] PAS. <http://www.pas.com/>. Acesso em 10 de Novembro de 2006.
27. **Exida.** Exida. [Online] Exida. <http://www.exida.com/>. Acesso em 19 de Novembro de 2006.

28. **Honeywell.** Honeywell. [Online] Honeywell. <http://www.honeywell.com/>. Acesso em 14 de Novembro de 2006.
29. **Matrikon.** Matrikon. [Online] Matrikon. <http://www.matrikon.com>. Acesso em 21 de Outubro de 2006.
30. **TIPS.** TIPS. [Online] TIPS. <http://www.tips.com/>. Acesso em 18 de Novembro de 2006.
31. **Chemtech e Guimarães, Flávio.** www.chemtech.com.br. [Online] http://www.chemtech.com.br/templates/chemtech/publicacao/publicacao_sol.asp?cod_Canal=2&cod_Publicacao=539&cod_menu=2. Acesso em 20 de Março de 2007.
32. **Ghosh, Asish e Woll, Dave.** Best Practices in Critical Condition Management. *ARC Insights - 13MPH*. 2004.
33. **Liu, J., et al.** Intelligent Alarm Management Through Suppressing Nuisance Alarms and Providing Operator Advice. *Chemical & Process Engineering Center, National University of Singapore*.
34. **UReason.** UReason Software Technology Company . [Online] <http://www.ureason.com/>. Acesso em 15 de Outubro de 2006.
35. **UReason.** OASYS-AM - Alarm and Event Management in Process Industry. *UReason*. [Online] http://www.ureason.com/index.php?option=com_content&task=view&id=42&Itemid=60. Acesso em 14 de Outubro de 2006.
36. **Scharpf, Eric W. and Marszal, Edward.** *Safety Integrity Levels* . s.l. : ISA - Instrument Society of America, 2002.
37. **Bullemer, P. T., et al.** Collaborative Decision Support for Operations Personnel. *INTERKAMMA 99 - ISA Technical Conference*.
38. **ATP.** Advanced Technology Program. [Online] ATP. <http://www.atp.nist.gov/index.html>. Acesso em 2 de Março de 2007.
39. **Sampaio, M. C., et al.** Smart Alarms - Tratamento Inteligente de Alarmes para Centros de Operação dos Sistemas da CHESF. *Eletroevolução (Rio de Janeiro)*. 2006, Vols. v. 44, p. 29-37.
40. **Sampaio, M. C., et al.** *A Robust and Maintenance-Free Alarm Processing Solution for Transmission System Operations Control Centers*. Cuernavaca, Morelos, México : International Colloquium on Telecommunications and Informatics for the Power Industry, 2005.

41. **Berkhin, Pavel.** *Survey of Clustering Data Mining Techniques*. San Jose, CA, USA : Accrue Software Inc.
42. **Jain, A. K., Murty, M. N. and Flynn, P. J.** Data Clustering: a Review. *ACM Computing Surveys*. 1999, Vols. 31, no 3, pp. 264-323.
43. **Jain, A. K. and Dubes, R. C.** *Algorithms for Clustering Data*. Upper Saddle River, NJ - USA : Prentice-Hall Inc, 1988.
44. **Gowda, K. C. and Diday, E.** Symbolic clustering using a new dissimilarity measure. *IEEE Transactions Syst. Man cybern.* 1992, Vols. 22, pp 368-378.
45. **Sheth, Beerud Dilip.** *A Learning Approach to Personalized Information Filtering*. s.l. : Massachusetts Institute of Tecnology, Department of Electrical Engineering and Computer Science, 1994.
46. **Wilson, D. Randall and Martinez, Tony R.** Improved Heterogeneous Distance Functions. *Journal of Artificial Intelligence Research*. 1997, Vols. 6, pp. 1-34.
47. **Castro, Pedriana.** *Calcular a similaridade entre um vetor de pesos do documento e a consulta utilizando as técnicas produto interno e cosseno*. São Luis, Brasil : GESEC UFMA, 2006.
48. **Knuth, Donald E.** *The Art of Computer Programming*. s.l. : Addison-Wesley Professional, 1998.
49. **Tanaka, Eiichi.** Theoretical aspects of syntactic pattern recognition. *Pattern Recognition*. July, pp. 1053-1061, 1995, Vols. 28, issue 7.
50. **Belkin, N. J. and Croft, W. B.** Information Filtering and Information Retrieval: Two Sides of the Same Coin? *Communications of the ACM*, vol. 35 No. 12, pp.29-38. 1992.
51. **Adomavacius, G. e Tuzhilin, A.** Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions. *IEEE Transactions on Knowledge and Data Engineering*, v. 17, n. 6. June de 2005.
52. **Balabanovic, M. and Shoham, Y.** Combining Content-Based and Collaborative Recommendation. *Communications of the ACM*. March 1997.
53. **Buckeley, C. e Salton, G.** Optimization of relevance feedback weights. *In Proceedings of the 18th Annual Internacional ACM SIGIR Conference on Research and Development in Informatin Retrieval*. 1995.

54. **Krulwich, B. and Burkey, C.** Learning user information interests through extraction of semantically significant phrases. *AAAI Spring Symposium on Machine Learning in Informatin Access*. 1996.
55. **Lang, K.** Newsweeder: Learning to filter netnews. *12th International Conference on Machine Learning*. 1995.
56. **Harman, D.** Overview of the Third Text. *REtrieval Conference (TREC-3). In Proceedings of the 3rd Text REtrieval Conference*. 1995.
57. **Papagelis, Manos, et al.** Incremental Collaborative Filtering for Highly-Scalable Recommendation Algorithms. *15th International Symposium on Methodologies of Intelligent Systems (ISMIS'05)*, pp. 553-561. 2005.
58. **Ungar, Lyle H. and Foster, Dean P.** A Formal Statistical Approach to Collaborative Filtering. *Conference on Automated Learning and Discovery (CONALD)*. 1998.
59. **Ungar, Lyle H. and Foster, Dean P.** Clustering Methods for Collaborative Filtering. *AAAI Workshop on Recommendation Systems. Technical Report WS-98-08*. 1998.
60. **Resnik, P., et al.** GroupLens: An Open Architecture for Collaborative Filtering of Netnews. *CSCW '94: Conference on Computer Supported Cooperative Work (Chapel Hill, 1994)*, pp. 175-186. 1994.
61. **Burke, R.** Knowledge-Based Recommender Systems. *Encyclopedia of Library and Information Systems*. 2000, Vol. 69 Supplement 32.
62. **Torres Junior, Roberto Dias.** *Combining Collaborative and Content-based Filtering to recommend research papers*. s.l. : Dissertação de Mestrado, UFGRS, 2004.
63. **Famili, A.** Use of decision tree induction for process optimization and knowledge refinement of an industrial process. *Artificial Intelligence for Eng. Design, Analysis and Manufacturing (AI EDAM)*, 8(1): pp. 63-75. 1994.
64. **Breiman, L., et al.** *Classification and regression trees*. Monterey, California USA : Wadsworth, Inc, 1984.
65. **Girardi, Rosario.** *Engenharia de Software baseada em Agentes*. Itajai, Santa Catarina, Brasil : Anais do IV Congresso Brasileiro de Ciencia da Computação (CBCOMP 2004). Ed. Univali, pp. 913-937, 2004.
66. **Lindoso, Alisson and Girardi, Rosário.** Uma Técnica baseada em Ontologias para o Reuso de Padrões de Software e de Frameworks no Projeto de Aplicações Multiagente. *First Workshop on Software Engineering for Agent-oriented Systems (SEAS 2005)*, 19º

Simpósio Brasileiro de Engenharia de Software (XIX SBES). Uberlândia, Minas Gerais, Brasil. October 3, 2005.

67. **Gruber, Thomas R.** *Toward principles for the design of ontologies used for knowledge sharing.* Padova, Italy : International Workshop on Formal Ontology, 1993.

68. **Protégé.** *Protégé Frames.* [Online] 2007. <http://protege.stanford.edu/>. Acesso em 11 de Fevereiro de 2007.

69. **Ziegler, P., Sturm, C. and Dittrich, K. R.** Unified Querying of Ontology Languages with the SIRUP Ontology Query API. *Datenbanksysteme in Business, Technologie und Web (BTW 2005), Karlsruhe, Germany. 2005, Vols. P-65 of Lecture Notes in Informatics, pp. 325–344.*

70. **Ziegler, P. and Dittirch, K. R.** User-Specific Semantic Integration of Heterogeneous Data: The SIRUP Approach. *First International IFIP Conference on Semantics of a Networked World (ICSNW 2004).* 2004, Vols. 3226 of Lecture Notes in Computer Science, pp. 44–64, Paris, France.

71. **Ziegler, Patrick, et al.** Detecting Similarities in Ontologies with the SOQA-SimPack Toolkit. *10th Int. Conference on Extending Database Technology (EDBT 2006).* 2006.

72. **GESEC.** Grupo de Pesquisa em Engenharia de Software e Engenharia de Conhecimento, Departamento de Informática da UFMA. [Online] 2007. <http://maae.deinf.ufma.br/>.

73. **Wooldridge, Michael and Jennings, Nicholas R.** Intelligent agents: Theory and practice. *Knowledge Engineering Review .* 1995, Vols. 10, number 2, pp. 115-152.

74. **Russel, S. and Norvig, P.** *Artificial Intelligence: A Modern Approach.* s.l. : Prentice-Hall, 1995.

75. **Genesereth, M. R. and Ketchpel, S. P.** Software Agents. *Communication of the ACM, 37[7], pp. 48-53.* 1994.

76. **Shoham, Y.** Agent-oriented programming. *Artificial Intelligence.* 1993, Vols. 60 (2), pp. 51-92.

77. **Bates, J., Bryan Loyall, A. and Scott Reilly, W.** An architecture for action, emotion, and social behaviour. *Technical Report CMU-CS-92-144, School of Computer Science, Carnegie-Mellon University, Pittsburgh, PA.* 1992.

78. **Ferber, J. and Gasser, L.** Intelligence artificielle distribuée. *International Workshop on Expert Systems & Their Applictaions. Cours n.9. France.* 1991.

79. **Alvares, Luis Otavio e Sichman, Jaime Simão.** *Introdução aos Sistemas Multiagentes*. Brasília : XVII Congresso da SBC, Jornadas de Atualização em Informática, 1997.
80. **Gasser, L.** Boundaries, identity and aggregation: Plurality issues in multiagent systems. *Decentralized Artificial Intelligence*. In Eric Werner and Yves Demazeau, editors. pages 199-212, 1992.
81. **Faria, Carla.** *MADDEM - Uma Técnica para a Aquisição e Construção de Modelos de Domínio e Modelos de Usuários Baseados em Ontologias para a Engenharia de Domínio Multiagente*. São Luis, MA, Brasil : Dissertação de Mestrado em Engenharia Elétrica – Área de Ciência da Computação, UFMA, 2004.
82. **Lindoso, Alisson N. e Girardi, Rosário.** The SRAMO Technique for Analysis and Reuse of Requirements in Multi-agent Application Engineering. *IX Workshop on Requirements Engineering, Cadernos do IME, UERJ Press, 20*. Rio de Janeiro 2006, pp. 41-50.
83. **Serra, Ivo.** *Uma Abordagem Gerativa para a Engenharia de Domínio Multiagente*. São Luis, MA, Brasil : Dissertação de Mestrado em Engenharia Elétrica – Área de Ciência da Computação, UFMA, 2004.
84. **Serra, Ivo, Girardi, Rosario e Henrique, José.** *Um Modelo de Domínio baseado em Ontologias para a Recuperação e Filtragem de Informação*. Itajaí, Santa Catarina, Brasil : Anais do IV Congresso Brasileiro de Computação (CBCOMP 2004], Ed. UNIVALI, pp. 124-129, 2004.
85. **Costa, Adriana Leite.** *ProEDM: Um processo para a Engenharia de Domínio Multiagente* . São Luis, MA - Brasil : GESEC, UFMA, 2007.
86. **Costa, Adriana Leite.** *ProEAM: Um processo para a Engenharia de Aplicações Multiagente* . São Luis, MA - Brasil : GESEC, UFMA, 2007.
87. **Lindoso, Alisson Neres.** Uma metodologia baseado em ontologias para a Engenharia de Aplicações Multiagente. *Dissertação de Mestrado em Engenharia Elétrica – Área de Ciência da Computação. UFMA. 2006*.
88. **Costa, Adrina Leite.** *Especificação de Processo para a Engenharia de Domínio Multiagente*. São Luis, MA - Brasil : Monografia do Curso de Análise e Projeto de Sistemas da UFMA, 2006.

89. **Lindoso, Alisson N., Girardi, Rosário and Oliveira, Ismênia.** Uma Experiência no Projeto de um Framework Multiagente para a Recuperação e Filtragem de Informação. *Anais do IV Congresso Brasileiro de Computação (CBCOMP 2004)*, Ed. UNIVALI. Santa Catarina. Brasil. October 8 - 12, 2004.
90. **Dublin, Trinity College, et al.** Software Agents - A Review. *Broadcom Éireann Research Ltda.* May de 1997.
91. **Rosenfeld, Louis and Morville, Peter.** *Information Architecture for the World Wide Web: Designing Large-Scale Web Sites.* s.l. : O'Reilly Media, Inc., 2002.
92. **SUN.** NetBeans IDE 5.5.1. *NetBeans.* [Online] <http://www.netbeans.org>. Acesso em 15 de Outubro de 2007.
93. **Gonçalves, Edson.** *Dominando NetBeans.* Rio de Janeiro : Ciência Moderna Ltda, 2006. 85-7393-519-7.
94. **Falconi, Vicente.** *TQC - Controle da Qualidade Total no Estilo Japonês.* s.l. : Bloch Editores, 1992. 85-85447-03-6.