



Universidade do Porto
Faculdade de Engenharia

FEUP



Hugo Miguel Pereira Simões Carneiro

SISTEMAS DE CONTROLO DE ACESSO

Faculdade de Engenharia da Universidade do Porto

Mestrado em Engenharia Electrotécnica e de Computadores

Sistemas de Controlo de Acesso

Hugo Miguel Pereira Simões Carneiro

Licenciado em Engenharia Electrotécnica e de Computadores pela Faculdade
de Engenharia da Universidade de Porto

Dissertação submetida para a obtenção do grau de
Mestre em Engenharia Electrotécnica e de Computadores pela Faculdade de
Engenharia da Universidade do Porto



Dissertação realizada sob a orientação do
Professor Doutor Adriano da Silva Carvalho
do Departamento de Engenharia Electrotécnica e de Computadores
da Faculdade de Engenharia da Universidade do Porto

Porto, 2004

621.3(043)/CARh/SIS

UNIVERSIDADE DO PORTO
Faculdade de Engenharia
BIBLIOTECA M
N.º <u>78 333</u>
<u>COU 621.3(043)</u>
<u>4 . 1 . 120 . 05</u>

À minha filha Mafalda

Resumo

O principal objectivo da dissertação “Sistemas de Controlo de Acessos” é familiarizar todos aqueles que consultarem esta dissertação, com os diversos sistemas físicos de controlo de acessos possíveis de serem implementados.

O Sistema de Controlo de Acessos é apenas um dos vários sistemas de Controlo e de Gestão que constituem uma organização. A necessidade de integrar e gerir os diversos sistemas e subsistemas que constituem a organização torna necessária a existência de Sistemas de Informação modernos e abrangentes capazes de efectuar a integração necessária.

O estudo e análise de quatro “módulos” ou subsistemas que representam a integração necessária a implementar, torna-se assim alvo de análise.

Em consequência é efectuada uma análise ao funcionamento de alguns sistemas de controlo de acessos bem como aos principais métodos de validação, biométricos e convencionais, passíveis de serem implementados nesses sistemas.

Sendo um tema de aplicação generalizada, com as características particulares dependendo do domínio de aplicação, escolheu-se um domínio particular, bem representativo de uma parte importante dos Sistemas de Controlo de Acessos: Sistemas de Controlo de Acessos em Estádios de futebol. Assim, para além de uma abordagem geral sobre sistemas de controlo de acessos, estende-se a análise a este caso particular.

A necessidade de analisar o funcionamento do Sistema de Controlo de Acessos num Estádio de futebol, perante diversos cenários, implicou o recurso à simulação. Esta também é utilizada como método de validação do modelo correspondente ao sistema real em questão.

Abstract

The main goal of the “Access Control Systems” dissertation is to make all that consult it familiar with the several access control physical systems possible to be implemented.

The Access Control System is only one of the several Management and Control systems that make an organization. The need to integrate and managing the several systems and subsystems that constitutes the organization makes necessary the existence of a modern and comprise Information Systems capable of doing the necessary integration.

The study and analysis of four “modules” or subsystems that represent the necessary integration to implement, then becomes the target of this analysis.

In consequence it is done an analysis to the functioning of some accesses control systems as well as the main methods of validation, biometrics and conventional, susceptible of being implemented in these systems.

Being a them of generalized application, with the particular characteristics depending on the application domain, it has been chosen a particular domain, well representative of an important Accesses Control Systems part: Accesses Control Systems in football stadiums. Thus, besides a general approach over accesses control systems, the analysis is extended to this particular case.

The need to analyze the functioning of Accesses Control System in a football Stadium, in the presence of several scenarios, has implicated the resource to simulation. This is also used as a model validation method correspondent to the real system in issue.

Índice

Resumo	v
Abstract.....	vi
Índice	viii
Índice de Figuras	x
Capítulo 1 – Introdução.....	13
1.1 Introdução.....	13
1.2 Motivação	14
1.3 Contexto da dissertação	15
1.4 Organização da dissertação	32
Capítulo 2 – Sistemas de informação	35
2.1 Introdução.....	35
2.2 Sistemas Informação.....	36
Introdução	36
2.3 O conceito de Informação, Sistemas de Informação e Tecnologias de Informação	38
2.4 Sistemas de Informação num Estádio de futebol.....	44
A integração.....	46
2.5 Conclusão	50
Capítulo 3 – Controlo e gestão de acessos	51
3.1 Introdução.....	51
3.2 Controlo e Gestão de bilhetes.....	53
Tipos de bilhetes	55
3.3 Controlo do fluxo de espectadores	57
3.4 Controlo do registo de cadastro de identificação de associados.....	58
3.5 Controlo de acessos	59
3.6 Interface/software	62
3.7 Conclusão	70
Capítulo 4 – Métodos de validação.....	71
4.1 Introdução.....	71
4.2 Métodos de validação e identificação biométricos.....	71
Biometria – definição	72
Íris.....	74
Reconhecimento facial	78
Geometria da mão.....	83
Voz	86
Impressão digital	88
4.3 Métodos de validação e identificação não biométricos “convencionais”.....	90
Cartão magnético.....	91
Código de barras.....	93
Etiqueta RFID.....	95
4.4 Conclusão	98
Capítulo 5 – Ambiente de simulação	99
5.1 Introdução.....	99
5.2 O software utilizado.....	100
Introdução ao Arena	102

Características do Arena.....	102
Módulos a utilizar na simulação.....	103
5.3 Conclusão	109
Capítulo 6 – Funcionamento do Sistema de simulação	110
6.1 Introdução.....	110
6.2 Filas de espera	111
Medidas de desempenho.....	112
Nomenclatura.....	113
Caracterização das distribuições das chegadas e do atendimento	113
Classificação das filas de espera – X / Y / Z / A	115
Características do modelo M/M/1	116
Calculo teórico das características do sistema.....	118
6.3 Simulação	119
Sistemas e Modelos	119
Conceito de simulação.....	119
Fases de realização de um projecto de simulação	120
Vantagens da simulação	121
Desvantagens da simulação	122
Conclusão	122
6.4 Calculo das características do sistema recorrendo à simulação	123
6.5 Análise dos resultados obtidos	130
6.6 Análise de um modelo mais próximo da realidade.....	131
Análise dos resultados obtidos	134
Conclusão	144
6.7 Conclusão	145
Capítulo 7 – Conclusão.....	147
Bibliografia	151

Índice de Figuras

Figura 1 – Sistemas de Informação num Estádio de futebol.....	36
Figura 2 – Enquadramento da função SI nas organizações.....	37
Figura 3 – Possível estrutura para a função Sistemas de Informação	38
Figura 4 – Actividades tradicionais no desenvolvimento de Sistemas de Informação	42
Figura 5 – No de Acesso Multiserviço – NAM.....	48
Figura 6 – Exemplo de alguns sistemas de controlo e gestão.....	51
Figura 7 – Arquitectura de um sistema genérico de Controlo e de Gestão.	52
Figura 8 – Exemplo de um posto automático de venda de bilhetes.....	54
Figura 9 – Visualização do estado das vendas das diversas zonas/sectores do estádio	55
Figura 10 – Exemplo de um bilhete com código de barras.....	56
Figura 11 – Exemplo de um bilhete “sem contacto” KeyCard.....	56
Figura 12 – Visualização do fluxo nas diversas zonas/sectores do estádio	58
Figura 13 – Arquitectura de um sistema de controlo de acessos.....	60
Figura 14 – Exemplo de um torniquete electromecânico.....	61
Figura 15 – Criação da tabela de dados.....	62
Figura 16 – Dados colocados na tabela de dados.....	63
Figura 17 – Tabela de dados preenchida	64
Figura 18 – Formulário inicial.....	65
Figura 19 – Visualização dos dados do utilizador/adepto.....	66
Figura 20 – Mensagem de erro (utilizador já se encontra no sistema).....	66
Figura 21 – Mensagem da saída do utilizador	67
Figura 22 – Formulário de introdução de password.....	67
Figura 23 – Formulário preenchido com uma password correcta	67
Figura 24 – Tabela contendo as passwords válidas.....	68
Figura 25 – Formulário de alteração dos dados do utilizador	68
Figura 26 – Mensagem correspondente à introdução de uma password inválida	69
Figura 27 – Processo de análise automático da íris	74
Figura 28 – Exemplo de uma imagem/fotografia do olho	75
Figura 29 – Resultado da localização da íris	76
Figura 30 – Esquema de blocos básico de um sistema de reconhecimento de faces.....	79
Figura 31 – Principais abordagens existentes para o reconhecimento de faces	81
Figura 32 – Exemplo de alguns pontos de controlo e respectivas distâncias ...	82
Figura 33 – Exemplo de certas medidas da mão.....	83
Figura 34 – Imagem de uma impressão digital com o centro e quatro pormenores/detalhes específicos	88
Figura 35 – Exemplos de pormenores/detalhes possíveis de encontrar em impressões digitais	89
Figura 36 – Constituição de um sistema RFID	95
Figura 37 – Funcionamento de um sistema RFID.....	96
Figura 38 – Software utilizado na simulação.....	102

Figura 39 – Aspecto gráfico do Arena.....	103
Figura 40 – Caixa de dialogo do módulo "Arrive".....	104
Figura 41 – Módulo "Server".....	105
Figura 42 – Caixa de dialogo do módulo "Server".....	106
Figura 43 – Módulo "Inspect".....	107
Figura 44 – Módulo "Depart".....	108
Figura 45 – Caixa de diálogo do módulo "Depart".....	108
Figura 46 – Estrutura de um sistema de fila de espera.....	111
Figura 47 – Função densidade de probabilidade de uma variável com distribuição de Poisson.....	114
Figura 48 – Função densidade de probabilidade de uma variável com distribuição exponencial negativa.....	115
Figura 49 – modelo básico com um servidor – M/M/1.....	116
Figura 50 – Modelo do sistema.....	123
Figura 51 – Módulo "Arrive".....	124
Figura 52 – Preenchimento do módulo "Arrive".....	125
Figura 53 – Módulo "Server".....	125
Figura 54 – Preenchimento do módulo "Server".....	126
Figura 55 – Módulo "Depart".....	127
Figura 56 – Preenchimento do módulo "Depart".....	127
Figura 57 – Resultado da simulação para o tempo médio de espera na Fila.....	128
Figura 58 – Evolução do tempo médio de espera na fila.....	128
Figura 59 – Resultado da simulação para o número médio de adeptos na fila	129
Figura 60 – Evolução do número médio de adeptos na fila.....	129
Figura 61 – Modelo mais próximo da realidade.....	131
Figura 62 – Módulo "Inspect".....	132
Figura 63 – Preenchimento do módulo "Inspect" (Revistar).....	133
Figura 64 – Preenchimento do módulo "Inspect" (Torniquete).....	134
Figura 65 – Resultados L_q e W_q	135
Figura 66 – Evolução do tempo médio de espera na fila "Inspect" 1.....	135
Figura 67 – Evolução do tempo médio de espera na fila Revistar.....	136
Figura 68 – Evolução do número médio de adeptos na fila "Inspect" 1.....	136
Figura 69 – Evolução do número médio de adeptos na fila Revistar.....	137
Figura 70 – Resultados taxa de ocupação.....	137
Figura 71 – Modelo com três módulos "Inspect" (Revistar).....	139
Figura 72 – Resultados L_q e W_q	140
Figura 73 – Evolução do tempo médio de espera na fila "Inspect" 1.....	140
Figura 74 – Evolução do tempo médio de espera nas filas Revistar.....	141
Figura 75 – Evolução do número médio de adeptos na fila "Inspect" 1.....	141
Figura 76 – Evolução do número médio de adeptos nas filas Revistar.....	142
Figura 77 – Resultados taxa de ocupação.....	143

Capítulo 1 – Introdução

1.1 Introdução

A implementação de Sistemas de Controlo de Acessos tecnologicamente actuais, capazes de acompanhar a evolução permanente da sociedade onde se inserem é uma realidade mais do que uma necessidade, especialmente se se tratar de uma organização como um Estádio de futebol.

Quer pela complexidade e dimensão deste tipo de organização, a implementação de Sistemas de Informação capazes de integrar todos os sistemas e subsistemas que constituem a organização é a base para o desempenho positivo de cada sistema individual. A integração deve ser implementada de forma a que a troca de informação entre os diversos sistemas e subsistemas flua de uma forma rápida e organizada. Como exemplo da integração, acima mencionada, são analisados alguns subsistemas de Controlo e de Gestão, incluindo obviamente o Controlo de Acessos.

Tecnologicamente, os Sistemas de Controlo de Acessos podem recorrer a tecnologias biométricas, convencionais ou mistas como métodos de validação.

A escolha do tipo de tecnologia a implementar depende do local, do tipo e número de utilizadores e do nível de confiança que se pretende que o Sistema de Controlo de Acessos possua.

Neste quadro, este capítulo faz uma abordagem sucinta às duas grandes classes de controlo de acesso, o controlo de acessos informático e o controlo de acessos físico, para ilustrar por um lado as características fundamentais e por outro caracterizar o trabalho desta dissertação na classe dos acessos físicos.

1.2 Motivação

A motivação para este trabalho surgiu com a realização do Euro 2004 em Portugal e com a necessidade de implementação de sistemas de controlo de acessos, capazes de fazer frente aos novos desafios associados a um evento com esta envergadura.

A construção de infra-estruturas desportivas de dimensão e características como as que vão ser construídas pressupõe a adequação para um conjunto de actividades, desportos e outras, que assegurem a rentabilidade dos investimentos efectuados e em particular no imediato, a realização dos eventos programados para o Euro 2004.

Esta adequação passa imprescindivelmente pela sua adequação a determinados requisitos técnicos e operacionais, os quais são conseguidos através da escolha e implementação de soluções técnicas adequadas, que resultem da identificação das actividades e nível de serviço que se pretende prestar.

O sistema de controlo de acessos desempenha um papel de extrema relevância na concretização dos requisitos acima referidos por afectarem áreas sensíveis da infra-estrutura e pela visibilidade e exposição de que é alvo, contribuindo de forma significativa para a imagem retirada e impressão geral do público.

A concepção, projecto e implementação de uma solução de controlo de acessos é influenciada pelos serviços, funcionalidades e modos de exploração definidos para o estádio, durante e fora dos eventos desportivos.

A necessidade de remodelar, ou implementar novos sistemas de controlo de acessos completamente é uma realidade em todos os recintos que receberão este evento.

Do site do Euro 2004 (www.euro2004.pt) pode observar-se a preocupação/importância que a organização tem com a segurança.

«Dez estádios, em nove das principais cidades de Portugal, receberão 16 selecções europeias em 2004. A segurança será uma das principais preocupações, não só no interior dos estádios e na sua periferia, como também dentro das cidades e nos trajectos que as unem.

Os novos estádios, concebidos com complexas infra-estruturas de acomodação e de segurança e ***munidos dos mais avançados sistemas tecnológicos de controlo de entradas***, de vídeo vigilância, de segurança, de som, de comunicações e de informação, irão proporcionar a todos os espectadores/adeptos uma atmosfera agradável de bem-estar e um sentimento de segurança...»

A aposta no estudo do funcionamento dos sistemas de controlo de acessos existentes, bem como a possibilidade de implementar um sistema de controlo de acessos que, de certa forma, simulasse o funcionamento real, foi a verdadeira motivação para o aparecimento e desenvolvimento desta dissertação.

1.3 Contexto da dissertação

O controlo de acessos é um “sistema” generalizado, abrangendo diversos sectores, como a industria, espectáculo, desporto, cultura, informação, etc.

Na classificação de um sistema de controlo de acessos pode-se distinguir duas classes ou grupos: o controlo de acesso físico e o informático.

Controlo de acessos informático:

No caso de se tratar de controlo de acesso a nível informático, este pode ser subdividido em três subgrupos:

- Controlo de Acessos à Rede – cujo objectivo é proteger os serviços conectados à rede;
- Controlo de Acessos ao Sistema Informático – cujo objectivo é impedir acessos não autorizados ao sistema informático;
- Controlo de Acessos às Aplicações – cujo objectivo é impedir acessos não autorizados à informação residente nos sistemas informáticos.

Basicamente a implementação de um sistema de controlo de acessos informático é constituído pelas seguintes fases:

Identificação

Para que se possa controlar o acesso aos recursos de um sistema informático é necessário antes de mais um sistema de identificação para as entidades que realizam o acesso.

Os utilizadores são geralmente identificados através de nomes curtos, obedecendo a certas restrições, geralmente utiliza-se o primeiro ou o último nome do utilizador real, ou por exemplo as respectivas iniciais. Normalmente não são permitidos espaços, e as letras maiúsculas e minúsculas podem ou não ter o mesmo significado.

Internamente, por razões práticas o sistema atribui a cada utilizador um número de identificação, geralmente conhecido por “username”.

As aplicações em execução (processos) usam geralmente identificadores de utilizadores. Normalmente a identificação adoptada é a do utilizador que tomou a iniciativa de "arrancar" a aplicação, mas existe geralmente a possibilidade (controlada) de a aplicação adoptar também a identificação do proprietário do ficheiro executável.

As máquinas são habitualmente identificadas pelo seu nome ou endereço. A identificação de máquinas para controlo de acesso tem muitas vezes uma utilização complementar relativamente à identificação de utilizadores, por exemplo para restringir as máquinas que um dado utilizador pode usar.

A identificação de máquinas também pode ser usada para definir acessos de forma independente da identificação de utilizador, por exemplo definindo quais as máquinas que têm acesso a determinados serviços.

Para que este mecanismo seja fiável é necessário um controlo total sob a rede, ou então a existência de um processo de autenticação das máquinas evitando que um intruso utilize uma máquina não autorizada para simular uma máquina autorizada.

Qualquer identificação só pode ser aceite depois de autenticada, no caso de endereços de máquinas isto pode ser dispensado numa rede local sobre a qual existe um grande controlo.

Controlo de acesso de utilizadores

Excluindo o controlo de acesso de máquinas, tudo se resume geralmente ao controlo do acesso de utilizadores, as aplicações ficam automaticamente englobadas pelas razões anteriormente apontadas.

Os princípios de implementação do controlo de acesso são simples: para cada objecto do sistema é necessário definir quais os direitos (permissões) que cada utilizador possui, o sistema operativo utiliza estas definições para decidir se deve ou não autorizar uma determinada operação requisitada por um utilizador.

Grupos de Utilizadores

Dado o número de utilizadores e objectos envolvidos, a definição de direitos para cada par (utilizador, objecto) é extremamente pesada, quer sob o ponto de vista do sistema, quer sob o ponto de vista administrativo.

A solução é agrupar. Surge assim o conceito de grupo de utilizadores, normalmente é também identificado por um nome e possui também um número de identificação interno.

O princípio de funcionamento é simples, se um dado grupo possui determinados direitos (permissões) sobre um objecto, então todos os membros desse grupo possuem esses mesmos direitos. Eventuais direitos adicionais que um utilizador possui sobre o objecto acumulam com os direitos derivados do facto de pertencer ao grupo.

Geralmente existe um grupo ao qual pertencem todos os utilizadores, este grupo pode ou não ser explícito. Num caso implícito trata-se de definir direitos por omissão (ou direitos mínimos), um utilizador que não possui nenhum direito explícito sobre o objecto (quer particularmente, quer via grupos a que pertence) possui pelo menos aqueles direitos mínimos.

Direitos sobre Objectos

Obviamente que o tipo de direitos e forma de os definir depende do tipo de objecto, pode distinguir-se os seguintes componentes de um sistema informático:

- ⇒ Processador;
- ⇒ Memória (memória central);
- ⇒ Dispositivos periféricos.

Num sistema multi-utilizador, as aplicações em execução pertencem a diferentes utilizadores. Cada aplicação em execução (processo) possui também um “username”, corresponde geralmente ao “username” do utilizador que a está a usar.

O sistema operativo verifica se o “username” em questão possui direitos que permitem a realização das tarefas requisitadas.

Num sistema operativo protegido, as aplicações não acedem directamente aos objectos, todos os acessos são realizados por invocação de funções do sistema operativo. Só assim é possível uma implementação eficiente do controlo de acesso.

O acesso aos processadores deve ser inteiramente controlado pelo sistema operativo. Num sistema mono-processador, cada aplicação em execução tem direito a uma porção de tempo de utilização. Este mecanismo é totalmente controlado pelo sistema operativo. O controlo do processador não pode

simplesmente ser cedido a um processo esperando que este seja bem comportado e o devolva.

A utilização da memória central num sistema multi-utilizador deve ser especialmente cuidada. A solução mais comum é a utilização de uma separação total: cada aplicação em execução tem à sua disposição um determinado número de blocos de memória à qual mais nenhuma aplicação tem acesso. Igualmente uma aplicação em execução apenas tem acesso aos blocos de memória que lhe pertencem.

Como não existe partilha de memória central entre as aplicações, a eventual necessidade de comunicação terá de ser assegurada por mecanismos especiais (IPC - "Inter-process Communication").

Os dispositivos periféricos concentram a maioria do esforço em termos de controlo de acesso, principalmente porque se pretende uma maior flexibilidade do que foi sugerido para a memória central.

De entre os dispositivos periféricos destacam-se os sistemas de ficheiros. Por um lado pretende-se uma grande flexibilidade, por outro o número de objectos pode ser muito grande. As definições de direitos podem ser implementadas em diversos níveis:

- ⇒ Volume ou disco lógico
- ⇒ Directório
- ⇒ Ficheiro
- ⇒ Registo/Campo

A maioria dos sistemas operativos genéricos fica-se pelo nível de ficheiro, deixando a implementação de controlo mais fino para aplicações especializadas, como por exemplo gestores de bases de dados.

Uma vez definido um mecanismo de controlo de acessos para os sistemas de ficheiros é tentador tratar todos os dispositivos como ficheiros. Isto é muito comum para dispositivos de acesso sequencial como impressoras, mas pode ser generalizado a todos os dispositivos de "hardware" e "software".

Como os sistemas de ficheiros são geralmente organizados em forma hierárquica o mais simples é usar essa hierarquia para agrupar os objectos por forma a simplificar a administração de direitos.

Os tipos de direitos básicos que se definem habitualmente sobre sistemas de ficheiros são "leitura" e "escrita", mas dependendo do tipo de sistema podem ser definidos outros direitos: "execução", "listagem", "alteração de atributos", "impressão", "eliminação", "adição de dados", "bloqueio".

Mesmo usando a hierarquia dos sistemas de ficheiros, a definição de direitos sobre os objectos pode ser pesada. Existem duas abordagens base:

- ⇒ Associar a cada objecto uma lista de utilizadores e respectivos direitos (ACL – "Access Control List").
- ⇒ Associar a cada utilizador uma lista de objectos e respectivos direitos.

Toda esta informação pode ficar guardada numa única base de dados do sistema, ou ser distribuída pelo sistema de ficheiros sob a forma de ACL's ou directamente associada aos objectos.

Seja como for, o acesso do sistema operativo a esta informação deve ser o mais rápido possível. Sempre que um determinado tipo de acesso a um objecto é requisitado por um utilizador/aplicação, o sistema operativo tem de verificar os direitos, directamente através do "username" e indirectamente através do número de identificação interno do grupo.

Por exemplo, numa versão centralizada, com a base de dados organizada por utilizador/grupo, a remoção de um objecto pode tornar-se pesada, obrigando a percorrer todos os utilizadores e grupos do sistema.

Geralmente combinam-se os vários métodos de forma a minimizar a quantidade de informação. O espaço ocupado depende em grande parte do tipo de direitos definidos, no caso mais simples ("leitura" e "escrita") bastam dois bits para cada associação (utilizador; objecto).

Autenticação

O controlo de acesso só faz sentido se existe um sistema de autenticação fiável que garanta que cada perfil de utilizador ("username") apenas pode ser usado por quem de direito. O método mais comum é a utilização de uma "password".

Autenticação/Confidencialidade de Sessão

A autenticação é uma questão fundamental quando duas entidades trocam dados entre si (sessão). Em grande parte trata-se de um problema de distribuição de chaves. Como foi referido, uma implementação segura de distribuição de chaves obriga a:

- ⇒ Criptografia convencional: a existência de um centro de distribuição de chaves (KDC – "Key Distribution Center");
- ⇒ Criptografia de chave pública: a existência de um emissor de certificados de chave pública.

Neste tipo de situação específico pretende-se que seja gerada uma chave K_s (tipicamente de criptografia convencional) que será usada apenas para a sessão a ser estabelecida, esta chave tem de ser distribuída pelas duas entidades participantes de sessão.

Numa abordagem de criptografia convencional o esquema seguinte mostra-se seguro numa sessão A para B, baseia-se no facto de apenas o KDC conhecer as chaves secretas de A e B, a entidade KDC vai ter a responsabilidade de gerar a chave secreta para a sessão:

- ⇒ A envia a B o seu identificador (ID_A) e um identificador de sessão (N_A).
- ⇒ B envia a KDC o seu identificador (ID_B), um identificador de sessão (N_B) e o conjunto ($ID_A + N_A + T_b$) codificado com a chave secreta de B (K_b), ou seja $K_b(ID_A + N_A + T_b)$.
- ⇒ O KDC envia a A $K_a(ID_B + N_A + K_s + T_b) + K_b(ID_A + K_s + T_b) + N_b$

⇒ A envia a B $K_b(ID_a + K_s + T_b) + K_s(N_b)$

Numa abordagem de criptografia de chave pública é usado o esquema seguinte:

- ⇒ A envia ao KDC $(ID_a + ID_b)$.
- ⇒ O KDC devolve a A o certificado de chave pública de B, ou seja $(ID_b + KP_b)$ codificado com a chave privada do KDC.
- ⇒ A envia a B $(N_a + ID_a)$ codificado com a chave pública da B.
- ⇒ B envia ao KDC $(ID_b + ID_a)$ e N_a codificado com a chave pública do KDC.
- ⇒ O KDC envia a B o certificado de chave pública de A, bem como o seguinte: $(N_a + K_s + ID_a + ID_b)$, codificado primeiro com a chave privada do KDC (assinatura) e codificado depois com a chave pública de B (confidencialidade).
- ⇒ B envia a A a assinatura recebida do KDC e N_b , tudo codificado com a chave pública da A.
- ⇒ A envia a B $K_s(N_b)$

"Passwords"

O estabelecimento de uma sessão entre um utilizador (aplicação cliente) e um sistema central (aplicação servidora) deve ser visto como qualquer outro tipo de sessão e recaindo por isso na abordagem anterior.

Na prática corrente as medidas de validação e autenticação são contudo muito mais reduzidas.

Geralmente a autenticação resume-se ao envio ao servidor de um conjunto ("login" + "password"), onde "login" é o nome do utilizador em versão reduzida e de conhecimento mais ou menos público e a "password" é secreta, apenas do conhecimento do utilizador e do sistema, proporciona por isso autenticação do utilizador perante o sistema.

Geralmente apenas se pratica a referida autenticação de clientes perante servidores, contudo num ambiente de rede pouco controlado não é complicado a um intruso simular um dado sistema central, podendo assim obter "password's" de utilizadores que nele tentam entrar.

O facto de o sistema fornecer algum tipo de informação como por exemplo a data/hora do último "login" pode facilitar a detecção deste tipo de situações. Uma solução que também se pode praticar é enviar uma "password" falsa e só depois a verdadeira.

Frequentemente as "password's" são enviadas pela rede sem codificar, situação apenas admissível se existir um total controlo sobre a rede, que deverá sempre ser do tipo comutado.

Como são digitadas pelos utilizadores em local público, podem ser obtidas por terceiros por simples observação.

Ficheiros de "password's"

Um outro problema deste mecanismo é a necessidade do sistema armazenar as "password's" directa ou indirectamente sobre a forma de ficheiros, que além do risco próprio são depois replicados em "backup's".

Neste aspecto a solução mais segura é usar um mecanismo de codificação não reversível, isto é apenas é possível codificar, descodificar é impossível ("one-way encryption").

Quando o utilizador envia a "password" o sistema codifica-a e verifica se o resultado coincide com o que se encontra no ficheiro.

Mesmo este mecanismo apresenta alguns problemas, pode por exemplo acontecer de dois utilizadores usarem a mesma "password", então o resultado codificado seria o mesmo, o que não é admissível.

Nos sistemas Unix este problema é resolvido com o "salt", número de 12 bits composto pela hora e PID na altura em que a "password" é definida, o "salt" de cada utilizador é também armazenado pelo sistema e é sempre adicionado à "password" antes da codificação.

Gestão de "password's"

Mesmo sendo elementar e porque envolve utilizadores existem vários cuidados básicos a ter com a autenticação por "password":

- O sistema deve bloquear a conta após algumas tentativas de "login" falhadas;
- O sistema deve esperar que o utilizador digite a "password" antes de enviar mensagens de erro, que não devem dar pistas sobre o facto de utilizador existir ou não;
- O sistema deve bloquear durante alguns segundos sempre que o acesso é negado;
- Se possível devem ser restringidos os pontos de acesso para cada utilizador, por exemplo endereços de origem. Os horários de acesso também podem ser definidos;
- Devem ser impostos limites quanto ao tamanho mínimo para as "password's";
- O mecanismo dos utilizadores para alteração de "password" deve sempre exigir a "password" anterior;
- Deve ser impossível qualquer tipo de visualização da "password".

Os Utilizadores

O principal problema dos sistemas de autenticação de utilizadores por "password" são os próprios utilizadores.

Um utilizador raramente está alertado para os aspectos de segurança, os seguintes comportamentos são vulgares:

- Emprestar a "password";
- Escrever a "password" num papel;
- Usar uma "password" igual ao login-name, ou palavras/nomes relacionados com o utilizador.

Os utilizadores podem ser obrigados a alterar a sua "password" periodicamente, mas uma escolha sob pressão pode não ser boa ideia, por outro lado os utilizadores tentarão alternar entre duas "passwords".

Para precaver esta última possibilidade alguns sistemas armazenam as "n" últimas "password's" de cada utilizador, assim para voltar à "password" inicial terão de alterar a "password" "n" vezes.

Para evitar este truque alguns sistemas apenas permitem a alteração da "password" uma vez em cada período, o que também tem inconvenientes.

Gerar "password's" aleatórias que os utilizadores são obrigados a usar seria uma boa solução, mas devido à dificuldade em serem memorizadas existe uma forte tendência para as escrever algures.

Existem "softwares" para captar "password's" que os administradores podem usar periodicamente, verificando assim a existência de contas com "password" menos sólida. Contudo a melhor solução é realizar verificações na altura em que os utilizadores definem a "password".

Autenticação com "password" protegida

Quando se procede à autenticação remota por "username/password" a "password" circula pela rede sob forma legível. Uma forma de resolver este problema é usar uma sessão em que todos os dados são codificados, como foi visto anteriormente existem mecanismos que permitem definir uma chave simétrica de sessão que é transmitida usando criptografia de chave pública.

A confidencialidade de toda a sessão nem sempre é necessária. Muitas vezes o único dado que necessita de ser mantido confidencial é a "password" do utilizador.

Para atender a estas situações foram desenvolvidos mecanismos que garantem que a "password" não é transmitida pela rede, são conhecidos por autenticação com "password" protegida.

A utilização de "username/password" coloca-se normalmente num contexto cliente-servidor em que o cliente (utilizador) tem de se autenticar perante o serviço.

O procedimento é o seguinte:

- Depois de estabelecida a ligação o servidor envia ao cliente um código;
- O cliente envia o nome de utilizador e em lugar da "password" envia HASH – um valor numérico de comprimento fixo ("password+código").
- O servidor realiza a mesma operação e verifica se os HASH CODES são iguais, nesse caso a autenticação está concluída.

Este mecanismo simples garante uma elevada segurança, sendo impraticável qualquer tentativa de obter a "password" na rede. Uma outra designação habitual para esta técnica é "passwords encriptadas", mas não se trata de uma verdadeira codificação.

O grande inconveniente desta técnica é a necessidade de o servidor dispor da "password" do utilizador já que tem de calcular HASH ("código+password") para comparar com o valor enviado pelo cliente. Por exemplo os sistemas Unix, por razões de segurança, não permitem dispor da "password" dos utilizadores. Pode-se dizer que este sistema aumenta a segurança das "passwords" na rede, mas diminui a segurança no servidor.

A autenticação com "password" protegida pode ainda funcionar como mecanismo de distribuição de chaves simétricas de sessão, prescindindo assim da criptografia de chave pública para esse efeito. Após autenticação tanto o servidor como o cliente conhecem algo que mais ninguém conhece, a "password" do utilizador. Sendo assim pode ser usado um algoritmo tipo HASH para gerar uma chave secreta a partir da "password", tanto o cliente como o servidor executam este algoritmo e vão obter exactamente a mesma chave que não é do conhecimento de mais ninguém.

Não se trata exactamente de uma distribuição de chaves, mas sim de uma geração em paralelo. Seja como for fica resolvido o problema da distribuição da chave de sessão sem recorrer a criptografia de chave pública.

Como para qualquer mecanismo de geração de chaves é importante garantir que elas variam de sessão para sessão, ou seja é necessário introduzir um parâmetro que garanta chaves diferentes de sessão para sessão, mesmo que a "password" se mantenha, por exemplo gerar o chave a partir de "código+password" em lugar da "password" apenas.

Sessões sem encriptação

A autenticação de utilizadores por "password" não proporciona qualquer tipo de segurança após o estabelecimento da sessão, quando os dados não são codificados, esta pode sofrer ataques passivos (monitorização) e pode também sofrer ataques activos. Por ataque activo entenda-se aqui uma "aquisição" da sessão.

A facilidade destes ataques a sessões não cifradas depende em grande parte dos meios de transmissão e protocolos usados:

- Numa simples ligação série, tipo terminal, ambos os ataques são fáceis desde que exista acesso físico à linha série;
- Numa rede local de "broadcast" a escuta pode ser realizada em qualquer ponto, os ataques activos deparam com algumas dificuldades;
- Num ambiente de rede o ataque activo a uma sessão não codificada depara com algumas dificuldades: Nestes ambientes as sessões geralmente assentam sobre protocolos de transporte como o TCP que procedem à numeração dos dados para efeito de controlo de erros e de fluxo. Mesmo supondo que o cliente lícito simplesmente desaparece, tomar o lugar desse cliente exige a simulação de uma conexão TCP, exactamente no mesmo estado. Terá ainda de se entrar em consideração com o protocolo de sessão/aplicação que também exige que o estado seja o mesmo do cliente lícito. Por outro lado os protocolos de transporte, ou directamente os protocolos de sessão, assentam sobre níveis de rede que definem endereços de nó, isto significa que será necessário usar o mesmo endereço do nó lícito. Isto é praticamente impossível de conseguir a nível de Internet

(devido ao "routing"). Numa rede local obrigaria a provocar algum tipo de bloqueio na máquina lícita para de seguida tentar tomar o seu lugar. Note-se que numa rede local teria de ser simulado não só o endereço de rede (nível 3) como também o endereço físico (nível 2).

Uma análise desta descrição de características de Controlo de Acessos Informático ilustra claramente que este é um domínio com características, métodos e tecnologias muito próprias e completamente diferentes dos que se verificam nos Controlos de Acessos Informáticos.

De seguida são caracterizados estes, de um modo que permite caracterizar a organização deste dissertação.

Controlo de acessos físico:

Existem diversos tipos de controlo de acessos e mesmo dentro de um determinado sistema pode deparar-se com vários graus ou níveis de acesso distintos. Ou seja, é possível deparar com vários tipos de controlo de acessos, dependendo dos requisitos que se pretende que o sistema cumpra.

Normalmente, o local de implementação, a actividade e a finalidade do controlo são factores a ter em conta no estudo do sistema.

Na verdade não se pode comparar um sistema de controlo de acessos de um laboratório de uma empresa com o de um aeroporto, pavilhão desportivo ou com o de uma biblioteca. Os requisitos impostos por cada local são diferentes.

Essas diferenças podem dever-se ao número de utilizadores, a restrições físicas e/ou económicas, à tecnologia disponível para implementar o sistema ou ao tipo e nível de controlo que se pretende implementar.

Existe contudo algo comum em todos os sistemas de controlo de acessos: o facto de todos eles pretenderem restringir e controlar o acesso a um determinado local, considerado de acesso restrito para determinados indivíduos.

Mesmo estando perante um determinado tipo de problema de controlo de acessos, com requisitos bem definidos, é sempre possível desenvolver diferentes soluções que respeitem as especificações impostas, uma vez que a nível tecnológico existem inúmeras soluções possíveis de ser empregues neste tipo de problemas.

Pode optar-se por tecnologias biométricas, que cobrem a totalidade dos requisitos impostos pelos mais sofisticados sistemas de controlo de acessos ou utilizar sistemas que recorrem a tecnologias não biométricas, ou mais “convencionais”, como a utilização de cartões magnéticos ou códigos de barras.

Os sistemas biométricos podem ser encontrados em quase todas as empresas especializadas da área e podem ser considerados acessíveis face ao desempenho e fiabilidade que apresentam.

Nos casos de tecnologia não biométrica, por se tratar de tecnologia dominada há mais tempo, torna-se melhor aceite por uma parte da sociedade, que apresenta ainda alguma relutância em interagir com sistemas biométricos.

No caso do cartão magnético são bons exemplos a utilização dos cartões de ponto ou cartões Multibanco, sendo o código de barras utilizado quase em todos os produtos com necessidade de controlo, como nos supermercados, lojas comerciais, etc.

Finalmente pode optar-se por sistemas mistos que incluam tecnologias não biométricas complementadas com tecnologias biométricas.

Um exemplo de um sistema misto será o de um determinado edifício em que o controlo de acesso geral seja efectuado recorrendo ao cartão magnético e em que haja certas áreas específicas apenas acessíveis a pessoal

especializado, que recorra por exemplo a um sistema controlado pela verificação da íris por parte de um leitor específico.

Ou seja um só sistema de controlo de acessos, constituído por dois níveis de acesso distintos, com utilização de tecnologias distintas.

Um outro exemplo de um sistema de controlo de acessos que recorre a ambas as tecnologias será a integração de um leitor de impressão digital a um código (PIN). O acesso só será validado no caso da impressão digital corresponder ao código (PIN) correspondente.

Como o controlo de acessos em geral pode ter uma abordagem demasiado vasta, vai apresentar-se um caso particular que inclua uma grande parte dos requisitos possíveis de encontrar noutros sistemas de controlo de acessos: O controlo de acessos a um estádio de futebol.

Ao iniciar qualquer estudo de controlo de acessos, tem que se previamente responder a três questões fundamentais:

- Qual é o problema que se pretende solucionar?
- Qual a tecnologia disponível para solucionar o problema?
- Qual a solução a implementar?

A primeira questão diz respeito à implementação de um sistema robusto, fiável e de baixo investimento, que permita o controlo da entrada dos espectadores/adeptos com segurança, com um tempo mínimo de espera nas filas de entrada ao estádio e cumprindo especificações regulamentares.

Em relação à segunda questão, encontram-se disponível no mercado tecnologias biométricas, convencionais ou mistas, as quais podem ser empregues neste tipo de problema.

A tecnologia a utilizar em cada Sistema de Controlo de Acessos depende de diversos factores, entre eles o local onde o sistema será implementado, o

número e natureza dos utilizadores e o nível de segurança/confiança que se pretende que o sistema apresente.

No caso particular de um Sistema de Controlo de Acessos de um Estádio de futebol, a tecnologia ou método de validação que normalmente é implementado é o cartão magnético ou código de barras.

Tal escolha deveu-se quer ao facto de se estar perante um sistema de controlo de acessos com um elevado número de utilizadores (na ordem dos milhares), quer à própria natureza dos utilizadores em causa, os quais, na sua maioria, não apresentam o cuidado necessário para manusear equipamentos delicados, como é o caso dos biométricos.

O elevado número de utilizadores impõe uma solução que seja robusta e fiável, impossibilitando a implementação de qualquer tipo de método de validação biométrico existente no mercado, uma vez que os respectivos leitores biométricos estarem apenas preparados para um número reduzido (face aos números em causa) de utilizadores – para além da razão acima mencionada.

Por exemplo, um dos métodos mais comercializados no mercado, o leitor de impressão digital é completamente incompatível com qualquer solução que envolva o número de utilizadores que um estádio típico comporta. Tal deve-se ao facto do leitor apresentar “gordura” ou sujidade, que impossibilita o seu correcto funcionamento, após ser utilizado algumas vezes consecutivas.

No caso do cartão magnético ou do código de barras, trata-se de um solução válida, fiável, robusta e já empregue com sucesso em diversos estádios.

Finalmente, a solução a implementar depende da tecnologia escolhida, ou seja depende dos métodos de validação pretendidos. Estes limitam a escolha do hardware utilizado na implementação do sistema de controlo de acessos.

escolha recaiu sobre estes “módulos”, uma vez serem um bom exemplo de integração com uma relação específica entre cada um deles.

Também é apresentada uma interface/software possível de ser implementado nos “módulos” acima mencionados, de forma a tornar possível visualizar/simular o funcionamento desses mesmos “módulos”. É possível visualizar desde a criação da base de dados, onde são definidos e inseridos os dados de cada utilizador, ao funcionamento pormenorizado do software/aplicação de controlo de acessos criada.

A ferramenta utilizada para desenvolver este software foi o Access.

No quarto capítulo encontra-se uma análise sobre os diversos métodos de validação possíveis de implementar em sistemas de controlo de acesso. Esses métodos estão divididos em tecnologias biométricas e não biométricas ou “convencionais”.

A título de introdução é efectuada uma breve apresentação sobre o que se entende por biometria bem como a necessidade de distinguir os termos identificação e verificação em sistemas biométricos.

A análise das principais características biométricas utilizadas em sistemas de controlo de acessos é efectuada logo de seguida.

Assim são analisadas as seguintes características biométricas: íris, face, geometria da mão, voz e impressão digital.

De seguida passa-se para as tecnologias não biométricas ou convencionais com a análise do cartão magnético, código de barras e etiquetas RFID.

No quinto capítulo encontra-se uma apresentação do software utilizado para simular o sistema de controlo de acessos, o Arena.

Por se tratar de um software com diversas aplicações e opções, a apresentação do software restringiu-se a posicionar o software no universo das linguagens de programação e dos simuladores, referir algumas características do Arena e conclui-se efectuando uma análise aos módulos que serão utilizados no modelo de simulação do capítulo 5.

No sexto capítulo encontra-se uma análise ao funcionamento do sistema de simulação. Esta análise consiste na definição do conceito de filas de espera, na nomenclatura utilizada, nas medidas de desempenho normalmente utilizadas, na caracterização das distribuições das chegadas e do tempo de atendimento, na classificação das filas de espera e na caracterização do modelo M/M/1.

Também são calculadas (cálculo teórico) as características do modelo que representa o sistema de controlo de acessos.

Posteriormente é analisada a aplicação da simulação ao modelo que representa o sistema de controlo de acessos ao estádio afim de se poder comparar os resultados obtidos na simulação com os valores teóricos previamente calculados.

Na simulação são utilizados três modelos distintos, o primeiro corresponde ao modelo ideal – modelo utilizado no cálculo teórico, um segundo modelo que já corresponde a um modelo mais aproximado da realidade – já inclui o módulo “Revistar” e finalmente o último modelo, o qual é praticamente idêntico ao anterior – apenas o número de módulos “Revistar” aumentou de um para três.

Em todos os três modelos são apresentados quer de uma forma gráfica, quer de uma forma numérica os resultados da simulação (medidas de desempenho).

No sétimo capítulo encontra-se a conclusão desta dissertação.

Capítulo 2 – Sistemas de informação

2.1 Introdução

Em qualquer tipo de organização, os Sistemas de Informação implementados são determinantes para o nível de funcionamento e desempenho de todos os recursos existentes. Os Sistemas de Informação são como os alicerces da organização, uma vez serem os responsáveis pela integração de todos os sistemas existentes na organização, bem como da interface entre os recursos informático e humanos (interface homem/máquina).

Só através da existência de um Planeamento de Sistemas de Informação moderno e que satisfaça as necessidades da organização em questão é que esta pode sobreviver no mercado em que se encontra.

Assim, antes de se iniciar a análise dos sistemas de Controlo e de Gestão, mais precisamente dos Sistemas de Controlo de Acessos – tema desta dissertação – vai efectuar-se uma análise aos Sistemas de Informação devido à importância que estes representam no funcionamento de qualquer organização.

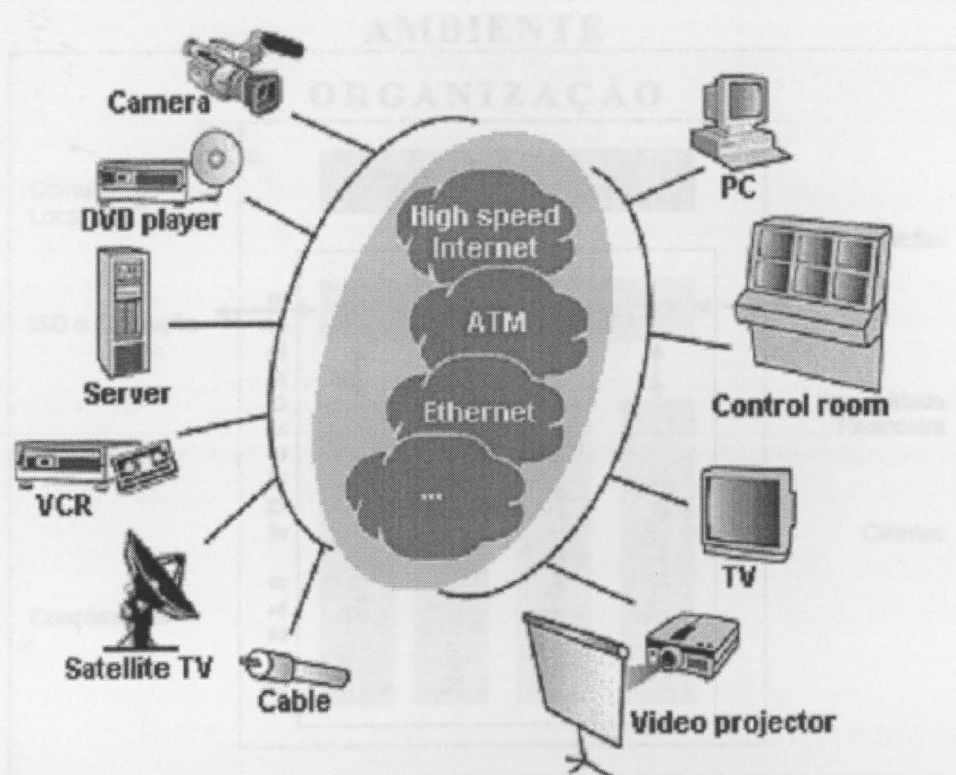


Figura 1 – Sistemas de Informação num Estádio de futebol

Figura 2 – Enquadramento da função SI nas organizações

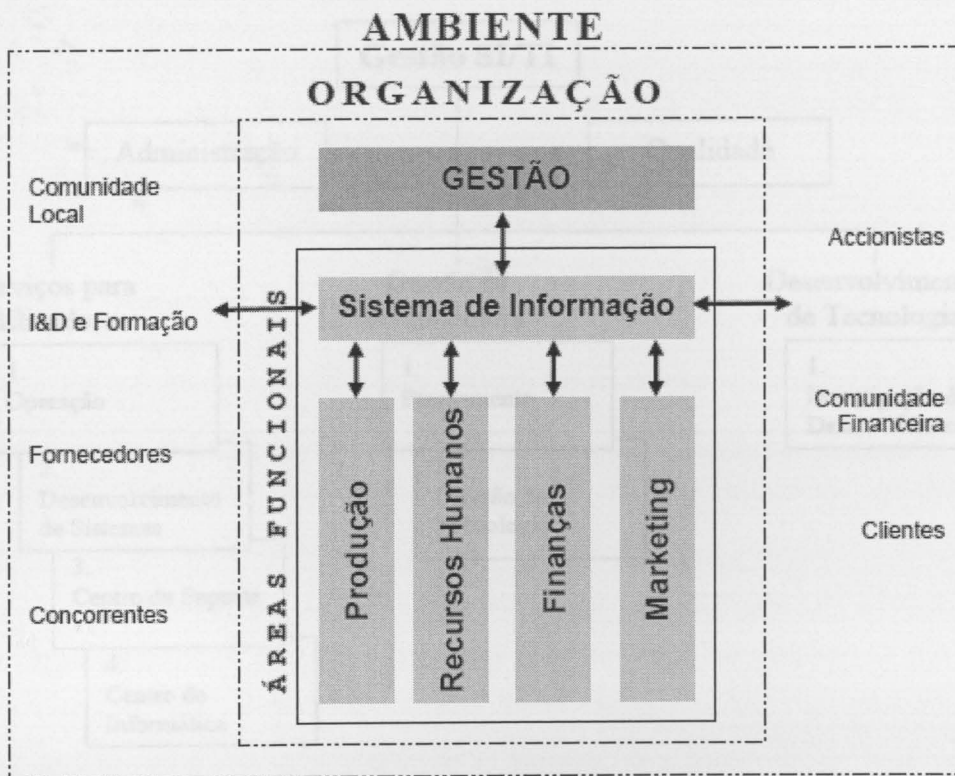
2.2 Sistemas Informação

Inicialmente neste capítulo é efectuada uma apresentação aos Sistemas de Informação numa organização. Posteriormente será analisado o caso concreto em que a organização é um Estádio de futebol

Introdução

A função Sistemas de Informação (SI) tem como preocupação gerir o recurso Informático e o modo como esta informação é recolhida, armazenada, processada e distribuída na organização, pelo que é responsável pela gestão do recurso informação e do sistema de informação da organização.

O conhecimento dos factores que influenciam a evolução da função Sistemas de Informação numa organização e do padrão que caracteriza tal crescimento, permitirá às organizações conhecerem o seu estado de desenvolvimento no que diz respeito às técnicas de gestão da função Sistemas de Informação, permitindo-lhes identificar um conjunto de indicadores daquilo que será necessário fazer no sentido de caminhar em direcção ao próximo estado.



Legenda: Fluxo de Informação

Figura 2 – Enquadramento da função SI nas organizações

Inicialmente neste capítulo é efectuada uma apresentação aos Sistemas de Informação numa organização. Posteriormente será analisado o caso concreto em que a organização é um Estádio de futebol.

Reconhecendo a importância do Sistemas de Informação numa organização como crucial ao bom desempenho da mesma a partir da própria informação reconhecida como um recurso que deve ser gerido com a mesma determinação que o são os restantes recursos da organização, a Gestão do Sistemas de Informação pode ser definida como o conjunto de actividades que, numa organização, são necessárias para gerir a informação, o sistema de informação e a adopção de tecnologias de informação para a suportar.

Informação é aquele conjunto de dados que quando fornecido adequada e oportunamente, melhora o conhecimento da pessoa que o recebe ficando a

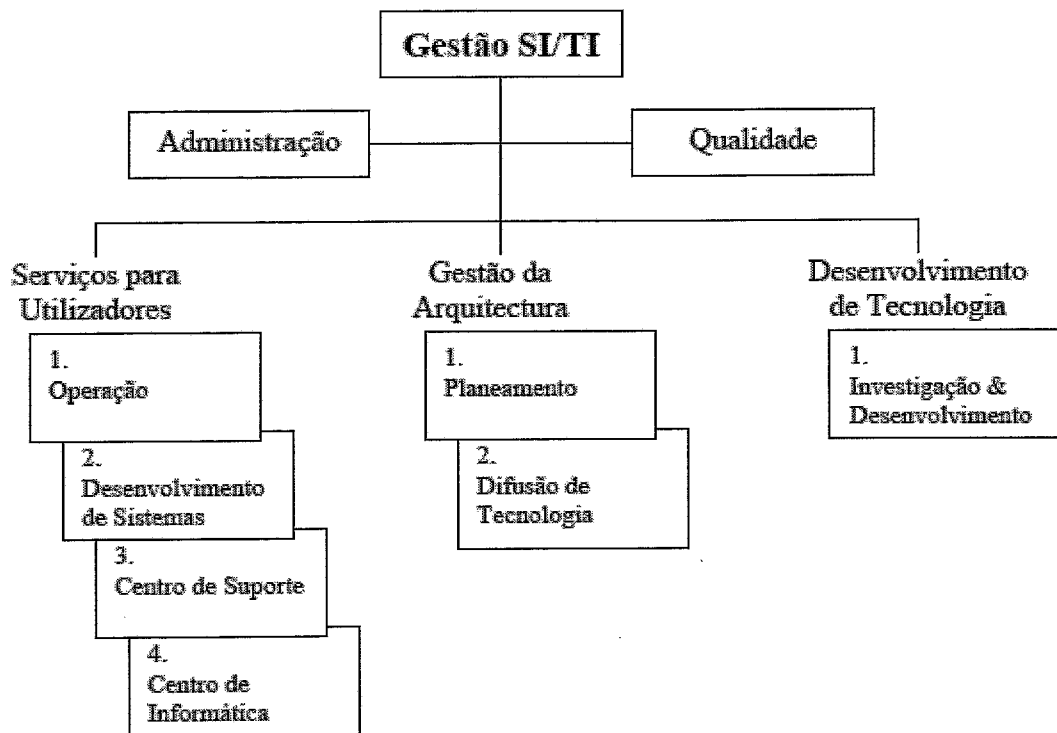


Figura 3 – Possível estrutura para a função Sistemas de Informação

2.3 O conceito de Informação, Sistemas de Informação e Tecnologias de Informação

Reconhecendo a importância do Sistemas de Informação numa organização como crucial ao bom desempenho da mesma e sendo a própria informação reconhecida como um recurso que deve ser gerido com a mesma determinação que o são os restantes recursos da organização, a Gestão do Sistemas de Informação pode ser definida como o conjunto de actividades que, numa organização, são necessárias para gerir a informação, o sistema de informação e a adopção de tecnologias de informação para a suportar.

Informação é aquele conjunto de dados que quando fornecido adequada e atempadamente, melhora o conhecimento da pessoa que o recebe ficando a

mesma mais habilitada a desenvolver determinada actividade ou tomar determinada decisão.

A Informação é um dos recursos cuja gestão e aproveitamento mais influencia o sucesso das organizações, destacando-se que todas possuam um Sistema de Informação com o propósito de as auxiliar no cumprimento da sua missão.

Sistema de Informação (SI) é um sistema que reúne, guarda, processa e faculta informação relevante para a organização, de modo a que a informação seja acessível para aqueles que a querem utilizar, incluindo gestores, funcionários, clientes e cidadãos.

A principal missão da função Sistema de Informação é ajudar as organizações a encontrar os seus objectivos, a criar valor de negócio, a ganhar vantagens competitivas, a facilitar a melhoria do desempenho das pessoas, a fornecer suporte cognitivo e a diminuir o tempo, o espaço e as limitações quanto a distâncias físicas, através de uma integração sistémica dos aspectos estratégicos, de gestão, tecnológicos e de operação no desenvolvimento, gestão e uso de informação, sistemas de informação e tecnologias de informação, como um todo.

A evolução dos Sistemas de Informação nas organizações reflecte novas preocupações por parte da gestão. Esta evolução parte de uma fase em que as Tecnologias de Informação (TI) eram utilizadas numa óptica exclusivamente do aumento da eficácia nas operações internas, com ganhos importantes no volume e velocidade de processamento, até chegar às fases mais avançadas com a utilização dos Sistemas de Informação para ganhar ou manter vantagem competitiva.

Tecnologias de Informação (TI) é o conjunto de equipamentos (Hardware) e suportes lógicos (Software) que permitem executar tarefas como aquisição, transmissão, armazenamento, recuperação e exposição de dados.

A existência de um Sistema de Informação e de Tecnologias de Informação nas organizações, conduz à necessidade de se planear o rumo desejado para

o Sistemas de Informação e planejar a forma como as Tecnologias de Informação deverão ser utilizadas na satisfação dos objectivos da organização.

Assim, **Planeamento de Sistemas de Informação (PSI)** pode ser definido como a actividade de identificação de políticas, definição de objectivos e construção de planos e orçamentos em que sejam contemplados os objectivos de gestão da organização e o Sistema de Informação. O Planeamento de Sistemas de Informação deverá conduzir a uma representação da visão global do Sistema de Informação da organização e, simultaneamente, incluir elementos necessários para o seu desenvolvimento.

O Planeamento de Sistemas de Informação tem evoluído de um planeamento escrito para uma parte integrante do planeamento de negócio. Um dos motivos para isso acontecer deriva das organizações terem necessidade de uma função sistema de informação mais eficaz, ou seja, mais madura, de forma a se manterem competitivas.

Sendo o Planeamento de Sistemas de Informação uma actividade de gestão por excelência é susceptível de ser hierarquizado em três níveis: estratégico, tático e operacional. De acordo com este pressuposto, o Planeamento de Sistemas de Informação pode ser realizado:

Ao nível estratégico, onde é um processo de alinhamento do plano de Sistemas de Informação com os objectivos e planos da organização, e/ou de identificação dos Sistemas de Informação que trazem vantagens competitivas à organização. Tipicamente são tomadas medidas de longa duração por períodos de tempo que dependem da volatilidade da organização e do seu meio ambiente.

A este nível, o objectivo é estabelecer a direcção do desenvolvimento em vez de identificar projectos de desenvolvimento específicos. Aqui, é necessário o envolvimento dos gestores de sistemas de informação e dos restantes gestores da organização. O pessoal de sistemas de informação contribuem com os conhecimentos analíticos, informativos e técnicos para o processo de planeamento, enquanto os restantes gestores contribuem com o conhecimento do negócio. Esta mistura é óptima por razões políticas, pois há a necessidade

de promover o diálogo, a cordialidade e o respeito mútuo entre o pessoal de Sistemas de Informação e o resto da organização.

Ao nível tático, onde é um processo centrado na identificação de prioridades e na realização de planos de acção para o desenvolvimento e medida de desempenho, a serem utilizados no planeamento operacional. Geralmente, neste nível, o planeamento de sistemas de informação cobre um maior espectro de projectos do que no nível estratégico.

Os projectos considerados neste nível devem ter sido originados por esforços de planeamento estratégico, pedidos de utilizadores, rotinas de manutenção ou mandato de origem exterior à organização. Geralmente, a carteira de aplicações é primeiro categorizada de acordo com a sua origem e depois ordenada por prioridades. Tópicos tais como migração de software e hardware, recuperação de desastres, formação de pessoal de sistemas de informação, capacidade de planeamento e segurança geral também deverão ser considerados a este nível.

Durante o planeamento tático, uma mistura de participantes de planeamento estará outra vez presente. Esta mistura depende do objectivo do exercício do planeamento tático.

Ao nível operacional, onde é um processo de realização de planos de implementação detalhados para cada projecto identificado. Implica a selecção e aprovação de projectos a serem começados no planeamento actual e no próximo planeamento anual, monitorando e controlando os esforços de desenvolvimento de sistemas. Os grupos de planeamento, a este nível, compreendem tipicamente mais recursos humanos de sistemas de informação. Representantes dos utilizadores e dos gestores serão, contudo, requeridos a participar no desenvolvimento de sistemas, revisão de resultados, protótipos, etc.

A actividade de **Desenvolvimento de Sistemas de Informação (DSI)** caracteriza-se fundamentalmente como sendo um processo de mudança que visa melhorar o desempenho dos subsistemas de informação.

O objectivo é analisar a forma como as Tecnologias de Informação podem ser utilizadas para potenciar mudanças significativas no modo como o negócio é conduzido e, eventualmente, levar a organização à obtenção de vantagens competitivas.

A construção de sistemas informáticos corresponde a uma postura técnica próxima da engenharia de software, podendo então considerar-se como uma visão restrita do Desenvolvimento de Sistemas de Informação.

No Desenvolvimento de Sistemas de Informação, a construção de sistemas informáticos é um subproblema que poderá mesmo não se por, quer por ser considerado desnecessário o suporte informático, quer pelo facto de as aplicações informáticas julgadas necessárias e adequadas poderem ser obtidas a partir de terceiros. No entanto, mesmo que a construção de sistemas informáticos não ocorra na organização, a definição dos seus requisitos é uma actividade importante do Desenvolvimento de Sistemas de Informação. O Desenvolvimento de Sistemas de Informação é assim visto como uma actividade próxima da engenharia de sistemas.

Actividades tradicionais de Desenvolvimento de Sistemas de Informação

Na prática, como ilustra a Figura 4, o Desenvolvimento de Sistemas de Informação engloba a análise, concepção, construção e implementação de Sistemas de Informação.

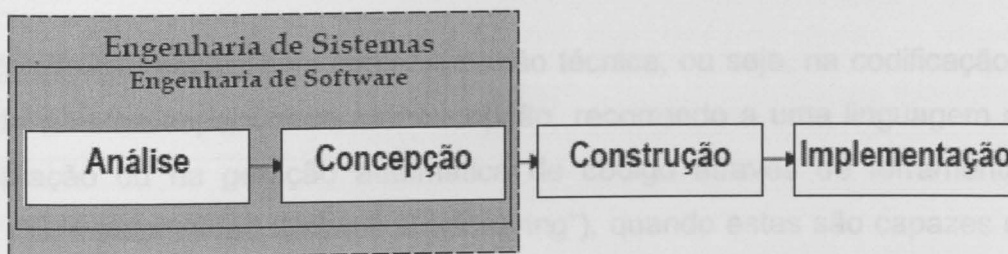


Figura 4 – Actividades tradicionais no desenvolvimento de Sistemas de Informação

A análise é essencialmente uma actividade de percepção. Exige-se ao analista, a capacidade de identificar conjuntamente com os utilizadores os processos e respectivos requisitos de informação de uma área ou actividade da

organização, recorrendo para isso a mecanismos adequados. Do resultado devem constar modelos ou especificações de sistemas novos independentes da tecnologia que os suportará. Nesta fase exige-se ao analista capacidade de abstracção de modo a reconhecer, analisar e resolver problemas do Sistema de Informação. Actualmente esta actividade também é conhecida por Engenharia de Requisitos.

No caso da Engenharia de Sistemas, e porque o software é sempre parte de um sistema maior, a análise começa por estabelecer os requisitos para todos os elementos do sistema e depois aloca algum subconjunto desses requisitos ao software. Esta visão é essencial quando o software tem de estar ligado com outros elementos tais como hardware, pessoas e base de dados.

No caso da Engenharia de software, o Processo de obtenção de requisitos é intensificado e focado especialmente no software. Para entender a natureza do software a construir, o engenheiro de software tem de entender os requisitos de informação do domínio do discurso, bem como funções, comportamentos, desempenhos e ligações requeridas.

Com a concepção pretende-se criar a especificação técnica detalhada para construção do sistema, nomeadamente, estrutura de dados, estrutura do software, interfaces e algoritmos de procedimentos detalhados, traduzindo os requisitos em representações de software.

A construção consiste na implementação técnica, ou seja, na codificação e teste do sistema especificado na concepção, recorrendo a uma linguagem de programação ou na geração automática de código através de ferramentas CASE (“Computer Aided Software Engineering”), quando estas são capazes de suportar de forma integrada a concepção e construção de sistemas.

Por último, a implementação consiste em pôr a funcionar correctamente na organização o subsistema de Informação, tendo em conta aspectos como a sua integração do Sistema de Informação global, formação dos utilizadores e controlo de qualidade com o fim de manter o sistema.

Após ter sido efectuada uma apresentação genérica aos Sistemas de Informação existentes numa organização, vai-se de seguida passar para o caso concreto em que a organização é um Estádio de futebol.

2.4 Sistemas de Informação num Estádio de futebol

Mais do que nunca, a necessidade de implementar Sistemas de Informação funcionais e capazes, em recintos desportivos e em particular em estádios de futebol é uma realidade/necessidade de forma a fazer face aos desafios que este tipo de organização se encontra sujeita, quando é palco de eventos quer desportivos, como o Campeonato Europeu de Futebol 2004 (Euro 2004), quer recreativos, como a realização de concertos.

Assim, no caso particular de um Estádio de futebol é possível identificar no mínimo três classes de serviços que se consideram imprescindíveis para o nível de serviço pretendido. Estas classes são:

- ⇒ Serviços de Supervisão, Segurança, Controlo e Gestão de Acessos:
 - CCTV (“Close Circuit Television”);
 - SCADA (“Supervisory Control and Data Acquisition”) – Gestão Técnica Centralizada;
 - Telefones de Emergência;
 - Sistema de Controlo de Acessos;
 - Sistema de Detecção de Intrusão, Incêndios, Inundação e Gases;
 - Sistema de Bilhética.

- ⇒ Serviços de Informação ao Público:
 - Sistema de Informação visual e multimédia;

- Sistema de Sonorização;
- CATV (“Community Antenna Television”).

⇒ Serviços e Sistemas de Apoio à Operação e Gestão:

- Posto de Comando;
- Rede de Transmissão de Dados;
- Rede de Cabos;
- Rede de Cablagem estruturada.

A diversidade de serviços acima identificados é obtida através de uma igual diversidade de subsistemas.

A necessidade de coordenação e condução das operações durante os eventos desportivos, bem como a necessidade de potenciar a eficiência das equipas de operações e manutenção fora dos eventos desportivos conduz à existência de uma Sala de Controlo de Operações destinada à organização (staff) do Estádio e à criação de uma Sala de Segurança destinada às forças de segurança.

Nestas salas encontram-se disponíveis todas as informações e controlo dos diferentes subsistemas, de modo a permitir uma gestão integrada e coordenada de todas as acções e operações, resultante da disponibilização no mesmo local de toda a informação necessária à tomada de decisões.

Ambas as Salas são constituídas por dispositivos de visualização de informação tais como monitores, vídeo wall, representações sinópticas do estádio e estações de trabalho, que de modo fácil e rápido permitem a identificação e a avaliação da situação bem como o desencadeamento das acções necessárias.

A Sala de Controlo de Operações destinada às forças de segurança possui as mesmas informações presentes na Sala de Controlo de Operações destinada à organização, operando de um modo “slave” sempre que se trate de comandos a efectuar sobre os equipamentos do Estádio.

Atendendo à diversidade de subsistemas e consequentemente à proliferação de diferentes unidades de comando, é essencial a existência de

um sistema integrador de comunicações e comandos que permita a uniformização das posições de trabalho bem como o agrupamento de forma flexível das funções relativas aos diferentes sistemas e ainda flexibilidade na atribuição de missões a cada posição de trabalho, função do cenário operacional em presença.

Assim, o sistema é designado como Plataforma de Integração de Comunicações e serve de interface único entre as posições de operador e os diferentes subsistemas, uniformizando as posições de operação ao nível das interfaces com o operador e pela flexibilidade na atribuição do controlo a diferentes subsistemas.

A integração

O conceito de Integração esta visível em três níveis distintos:

- ⇒ Nível Funcional;
- ⇒ Nível Físico;
- ⇒ Nível da Implementação.

Nível Funcional

Ao Nível Funcional, a integração esta disponível pela existência de uma Plataforma de Integração de Comunicações e Controlo com as características já referidas:

- ⇒ Integração do Controlo dos operadores dos diferentes subsistemas na mesma plataforma;
- ⇒ Uniformização do Interface Homem-Máquina;
- ⇒ Multi Operador;
- ⇒ Flexibilidade e selectividade na atribuição das funções/missões a cada operador;

Bem como na existência de interligação entre os diferentes subsistemas ao nível funcional, ex. SCADA e Vídeo para a visualização automática de imagens associadas a determinados alarmes.

Nível Físico

Ao Nível Físico, a Integração esta presente pela uniformização e integração do transporte de sinal e cobertura física da área do estádio, recorrendo a uma Rede de Transmissão de Dados de Alto Débito, que serve de meio de transmissão único e suporta todos os requisitos de transmissão de todos os subsistemas. Para tal, são utilizados cabos de fibra óptica e de cobre em par entrançado.

Pretende-se assim anular a existência de cabos e meios de comunicação dedicados, excepto nas situações de carácter legal e regulamentar, que não sejam de todo possíveis de alterar ou ultrapassar no quadro de um evento com a dimensão e abrangência do Euro 2004.

A uniformização de protocolos de comunicação é um ponto vital e crítico, assim todos os subsistemas têm as comunicações baseadas em protocolos standard, com preferência para a comunicação sobre TCP/IP.

Nível de Implementação

Ao Nível da Implementação, a Integração esta presente pela existência de uma entidade única definida como Integradora, que está presente de forma activa em todas as fases do ciclo de vida do projecto, assegurando o fornecimento da Solução de Comunicações e Segurança, assumindo-se como interface único face ao Cliente final em relação aos diferentes subsistemas e que assegure a performance da solução face aos requisitos das especificações.

Está-se na presença não de inúmeros subsistemas de comunicações e segurança mas sim perante uma Solução de Comunicações e Segurança, constituída por vários subsistemas, integrados.

A Solução de Comunicações e Segurança é constituída por 4 níveis:

- ⇒ Nível de Transmissão;
- ⇒ Nível de Distribuição;
- ⇒ Nível de Serviços;
- ⇒ Nível de Integração e Sala de Controlo de Operações.

Nível de Transmissão

O Nível de Transmissão é constituído por um backbone de cabos de Fibra Óptica e de Cobre Par Entrançado e por uma rede de transmissão de dados de alta capacidade.

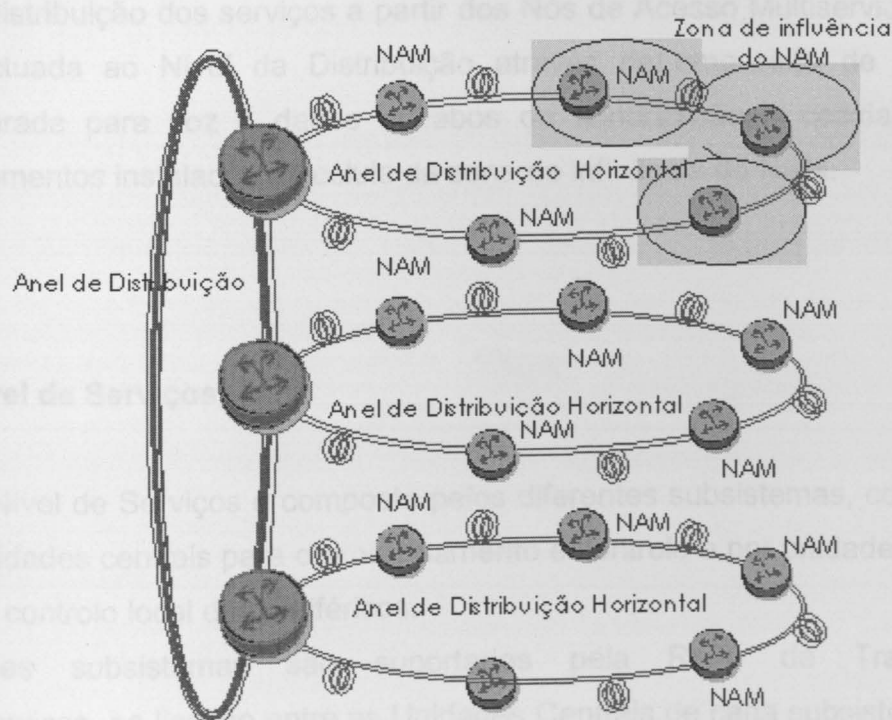


Figura 5 – No de Acesso Multiserviço – NAM

A rede de cabos de Fibras Ópticas desenrola-se em duas dimensões: uma distribuição horizontal para abranger os diferentes níveis do estádio e uma distribuição vertical para interligar os diferentes níveis horizontais.

Em paralelo com esta rede de Fibra Óptica, existem cabos de par entrançado Categoria 5E e cabos TVHV/TE1HE.

A Rede de Transmissão de Dados é constituída por Nós de Acesso Multiserviço, estruturando uma solução em anéis, de modo a assegurar caminhos alternativos e redundância nas comunicações.

Nível de Distribuição

De cada Nó de Acesso Multiserviço, derivam para a sua zona de influência, célula, todos os serviços e canais de todos os subsistemas para atacar os periféricos aí instalados.

A distribuição dos serviços a partir dos Nós de Acesso Multiserviço – NAM, é efectuada ao Nível da Distribuição através de uma rede de cablagem estruturada para voz e dados e cabos de sonorização e coaxial para os equipamentos instalados na célula da zona de influência do NAM.

Nível de Serviços

O Nível de Serviços é composto pelos diferentes subsistemas, constituídos por unidades centrais para o processamento e controlo e por unidades remotas para o controlo local dos periféricos.

Estes subsistemas são suportados pela Rede de Transmissão Multiserviços, na ligação entre as Unidades Centrais de cada subsistemas e as Unidades Remotas e/ou Periféricos principais, localizadas junto dos diferentes NAM.

Todos os sistemas utilizam comunicação por TCP/IP.

Nível de Integração e Sala de Controlo de Operações

O Nível de Integração e Sala de Controlo de Operações é constituído pela Plataforma de Integração de Comunicações e Controlo e pelos dispositivos de visualização da Sala de Controlo de Operações.

2.5 Conclusão

A necessidade de existir um Sistema de Informação capaz de integrar todos os sistemas e subsistemas existentes nos Estádios de futebol é um requisito o qual não deve ser remetida para segundo plano.

Neste capítulo foi discutida a arquitectura de informação e de serviços apropriada.

Por se tratar da integração de três grandes sistemas ou classes de serviços: Serviços de Supervisão, Segurança, Controlo e Gestão de Acessos, Serviços de Informação ao Público e Serviços e Sistemas de Apoio à Operação e Gestão, os quais são constituídos por diversos subsistemas, no próximo capítulo vai efectuar-se uma análise mais pormenorizada aos Serviços de Supervisão, Segurança, Controlo e Gestão de Acessos, mais precisamente o Controlo e Gestão de Acessos por ser o sistema ou conjunto de subsistemas que mais se encontra relacionado com o tema desta dissertação.

Na verdade pela sua especificidade em termos de domínio de aplicação esta classe justifica uma abordagem/análise cuidada e autónoma.

Capítulo 3 – Controlo e gestão de acessos

3.1 Introdução

Um sistema de controlo de acessos é parte integrante de um conjunto de diversos Sistemas de Controlo e Gestão, uma vez que interage directa ou indirectamente com alguns desses sistemas.

O tipo de sistema que mostra esta dissertação representa um conjunto de funcionalidades que o caracterizam e a Figura 6 ilustra.

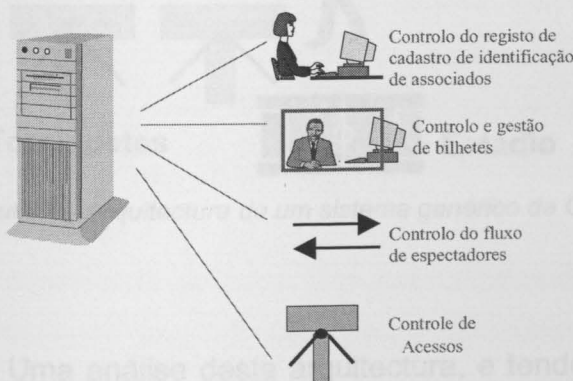


Figura 6 – Exemplo de alguns sistemas de controlo e gestão

Uma análise destas funcionalidades e a sua integração no sistema “original” aponta para a necessidade de implementação de uma arquitectura que permita uma operacionabilidade apropriada.

Tal arquitectura é, de base, uma arquitectura distribuída com interface aos utilizadores nos diversos nós.

A Figura 7, representa a arquitectura típica de um Sistema de Controlo e de Gestão e respectivos componentes possível de implementar num estádio de futebol.

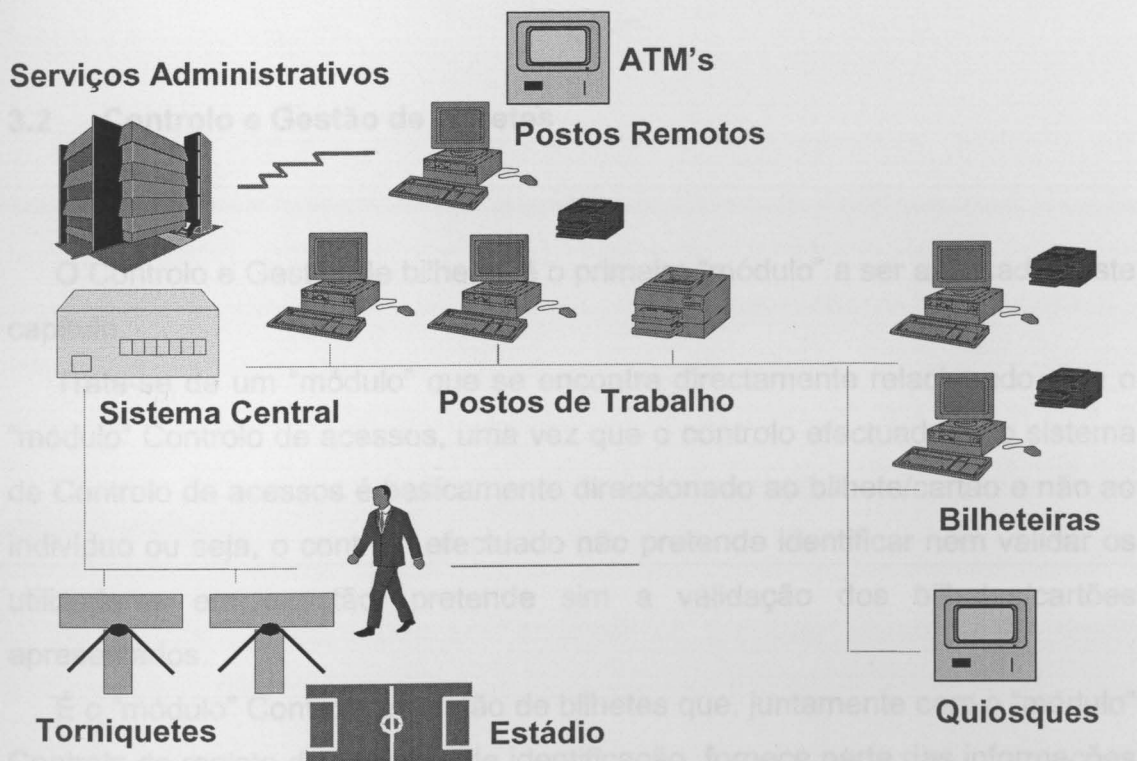


Figura 7 – Arquitectura de um sistema genérico de Controlo e de Gestão.

Uma análise desta arquitectura, e tendo em vista o projecto do sistema de controlo e gestão, conduz ao estudo de cada nó e suas características funcionais. Uma abordagem efectuada a cada nó e respectivas funcionalidades são designadas por “módulos” ou subsistemas.

O *Controlo e Gestão de bilhetes*, o *Controlo do fluxo de espectadores*, o *Controlo do registo de cadastro de identificação de associados* e o *Controlo de acessos* foram os “módulos” de controlo e gestão escolhidos para demonstrar o funcionamento de um sistema global de controlo e gestão. A escolha recaiu sobre estes “módulos”, uma vez serem um bom exemplo de integração com uma relação específica entre cada um deles.

Desta forma consegue-se enquadrar melhor o “problema” do controlo de acessos em estádios de futebol, possibilitando uma visão mais ampla quer de toda a envolvente, quer de sistemas do mesmo género.

3.2 Controlo e Gestão de bilhetes

O Controlo e Gestão de bilhetes é o primeiro “módulo” a ser analisado neste capítulo.

Trata-se de um “módulo” que se encontra directamente relacionado com o “módulo” Controlo de acessos, uma vez que o controlo efectuado pelo sistema de Controlo de acessos é basicamente direccionado ao bilhete/cartão e não ao indivíduo ou seja, o controlo efectuado não pretende identificar nem validar os utilizadores em questão, pretende sim a validação dos bilhetes/cartões apresentados.

É o “módulo” Controlo e Gestão de bilhetes que, juntamente com o “módulo” Controlo de registo de cadastro de identificação, fornece parte das informações necessárias a serem introduzidas na base de dados que constituem o sistema de controlo de acessos. Um exemplo destas informações são as quantidades e codificação dos bilhetes vendidos, bem como a informação referente ao pagamento de cotas dos associados.

A gestão de bilheteiras tem de ser vista segundo perspectivas distintas:

- 1 – Emissão de lotes de ingressos anterior aos desafios.
- 2 – Compra/Emissão de ingressos nas bilheteiras do estádio.
- 3 – Compra de ingressos fora do estádio.

1 – A emissão de bilhetes em lote normalmente é da responsabilidade dos postos instalados no sector administrativo. Compete a este sector emitir lotes de ingressos para os diversos sectores do estádio.

Com a emissão destes lotes, os respectivos lugares ficam automaticamente cativos, não sendo possível fazer a sua venda sem antes haver um retorno ou realocação dos mesmos.

2 – Nas bilheteiras locais, automáticas e com operador, poderão ser instaladas consolas de monitorização dos processos de vendas a nível central, sendo portanto possível visualizar, sobre a representação gráfica das zonas/sectores do estádio, as taxas de vendas/reservas 'on-line' (Figura 9). Esta potencialidade revela-se de primordial importância, numa situação em que, por exemplo se torne necessário estar a executar em tempo real a distribuição entre lugares disponíveis para venda local e os lugares cativos em venda remota.

Na Figura 8 encontra-se um exemplo de um tipo de posto de venda automática de bilhetes.



Figura 8 – Exemplo de um posto automático de venda de bilhetes

3 – Da forma idêntica, o sistema pode parametrizar determinado número de lugares, e disponibilizar os mesmos para venda na rede ATM ou pela Internet.

Pelo facto de existirem diferentes necessidades, há a necessidade da existência de diversos suportes de dados para as respectivas autorizações. Assim, irá ser efectuada uma breve análise dos diversos tipos de bilhetes (bilhetes com código de barras, e bilhetes sem contacto) utilizados em estádios de futebol.

O bilhete com Código de Barras



Figura 10 – Exemplo de um bilhete com código de barras

Apesar de se poderem realizar completamente todas as funções relacionadas com as entradas com este tipo de bilhete, ele é antes de tudo mais apropriado para o espectador ocasional.

A sua concepção é tão barata, que mesmo em entradas de baixo valor ele pode ser utilizado, sendo mesmo, através da impressão do código de barras sobre o fundo preto, completamente seguro contra falsificações.

Os bilhetes de código de barras são impressos em aparelhos de codificação nas bilheteiras ou em impressoras especiais nos parceiros com pré-venda e controlados com leitores nas entradas.

Estes bilhetes podem ter impressões a cores de ambos os lados, com excepção da zona do código de barras.

O bilhete “sem contacto”



Figura 11 – Exemplo de um bilhete “sem contacto” KeyCard

Para demonstrar este tipo de bilhete, foi escolhido o “KeyCard” da Skidata (Figura 11), uma vez ter sido tido esta uma das marcas escolhidas por diversos estádios (ver http://www.skidata.com/en/ref/event/ref_stadium.asp).

Os espectadores assíduos podem ser, por exemplo, através da participação numa campanha de adesão ou num sorteio, motivados a adquirir um “KeyCard” que é já quase um cartão de sócio.

Este suporte de dados, comprado pelo espectador poderá ser programado caso a caso com a respectiva permissão de acesso, nas bilheteiras do estádio, em outros pontos de pré-venda ou mesmo na Internet.

O “KeyCard” pode ser fornecido a cores e pode ter a fotografia do portador. Além disso a técnica “ThermoRewrite” permite a reinscrição de novos dados.

O “KeyCard” tem um sistema de armazenamento de dados em vários níveis, de modo a permitir a sua utilização não só para a entrada no estádio, mas também ter o sistema de acumulação de bónus, o acesso a transportes ou parques de estacionamento e o porta-moedas electrónico para pagamento nos bares e nos restaurantes assim como nas lojas do clube.

3.3 Controlo do fluxo de espectadores

O sistema de controlo de fluxo de espectadores encontra-se (fisicamente) dependente do sistema de controlo de acessos, uma vez serem os torniquetes, que constituem o sistema de controlo de acessos, que incluem o módulo responsável pelo controlo de fluxos.

Existe um software próprio, o qual é responsável por disponibilizar permanentemente relatórios actualizados sobre as condições de acessos ao estádio. Desses múltiplos relatórios são destacados os seguintes:

- Estatística por tipo de ingressos (bilhetes, cartões de sócio, etc.).
- Taxas de ocupação por sectores.

- Tempos médios de acesso em cada torniquete/porta.
- Resumo consolidado ou detalhado de ocorrências por torniquete/porta.
- Estatística de anomalias em cada torniquete/porta.

Esta informação também pode ser visualizada de uma forma gráfica (Figura

12).



Figura 12 – Visualização do fluxo nas diversas zonas/sectores do estádio

3.4 Controlo do registo de cadastro de identificação de associados

O controlo do registo de cadastro de identificação de associados, pode ser considerado como que um modulo de gestão de clientes. Neste caso, os clientes são os associados do clube em questão.

A identificação individual de cada associado, bem como a actualização do cadastro do associado em questão é da responsabilidade dos sectores administrativos.

O registo do cadastro completo de cada associado é basicamente constituído pelos seguintes elementos:

- Número de sócio;
- Nome completo;
- Morada completa + morada para cobrança/publicidade;
- Data de nascimento;
- Data de admissão;
- Numero de B.I.;
- N.I.B. – unicamente para os associados que procedam ao pagamento das cotas por transferência bancária;
- Sexo;
- Profissão + habilitações literárias;
- Situação como sócio – categoria (cativo ou normal);
- Parque automóvel – acesso ao parque do recinto;
- Fotografia;
- Observações – lista negra.

Toda esta informação é inserida na base de dados no acto de entrega da proposta de novo sócio ao clube.

Esta informação é confidencial e para uso exclusivo de clube.

3.5 Controlo de acessos

Basicamente, dum sistema de controlo de acessos pretende-se um controlo de acessos a determinados locais do estádio considerados de domínio reservado, ou seja obtenção ou não, de acesso a determinada porta do estádio.

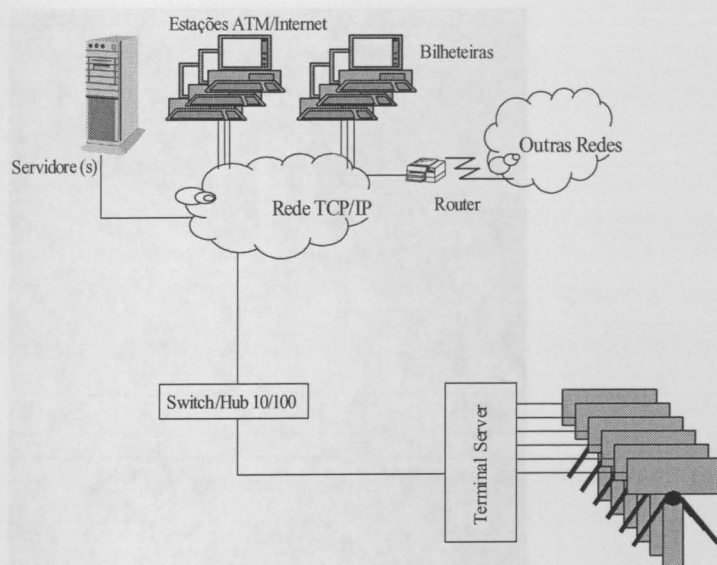


Figura 13 – Arquitectura de um sistema de controlo de acessos

Fisicamente todo o recinto está vedado, assim, para que o adepto tenha acesso tem de se deslocar à porta correspondente ao seu bilhete/ingresso. Ai, mediante a apresentação do ingresso, ser-lhe-á concedido ou não acesso ao recinto.

A Figura 13 é um exemplo de um tipo de arquitectura possível de implementar num estádio de futebol.

Os torniquetes electromecânicos (Figura 14) são os elementos seleccionados para controlar/vedar fisicamente os acessos às diversas portas do estádio. Em cada porta é instalado um ou mais torniquetes, consoante o tamanho, importância da porta e respectiva afluência (esta informação é dada pelo controlo do fluxo de espectadores visto anteriormente).

Em cada torniquete é instalado um sistema de validação de bilhetes e/ou cartões de acesso, o qual concede ou não o acesso ao recinto mediante a apresentação do ingresso.

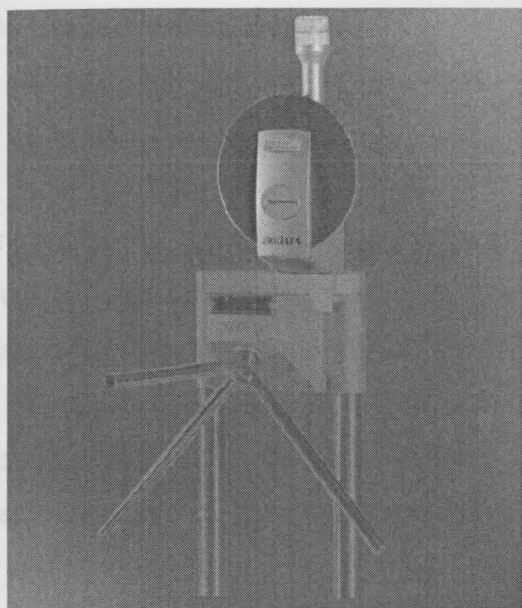


Figura 14 – Exemplo de um torniquete electromecânico

Os torniquetes são ligados entre si, e ao sistema central, através de uma rede de comunicações possibilitando assim a troca constante de dados/informação.

Quando o sistema central verifica algum tipo de incoerência entre o código lido e a informação da base de dados relativa aquele código, de imediato, aparece no monitor de LCD do torniquete uma mensagem inerente ao tipo de ocorrência, que originou a recusa de acesso.

Por ser do conhecimento geral, que este tipo de situações acontecem é que este tipo de solução nunca dispensará a presença de entidades fiscalizadoras durante o processo de entradas e que obrigarão um espectador 'não validado' a desimpedir o corredor de acesso para dar vez aos seguintes.

3.6 Interface/software

Após a análise dos “módulos” de controlo e gestão acima mencionados, vai apresentar-se uma interface/software que possibilita de alguma forma visualizar/simular o funcionamento dos “módulos” anteriormente analisados, ou seja possibilita complementar a informação teórica anteriormente apresentada.

O objectivo desta interface/software é o simular a interface/software existente nas entradas (torniquetes) de um estádio de futebol, de forma a possibilitar a validação dos acessos – por exemplo através de cartão magnético ou código de barras.

A criação/construção da base de dados é o ponto de partida de toda a interface/software que se pretende criar.

Assim o primeiro ponto é criar uma tabela onde se possa colocar os dados que se pretende na base de dados (Figura 15).

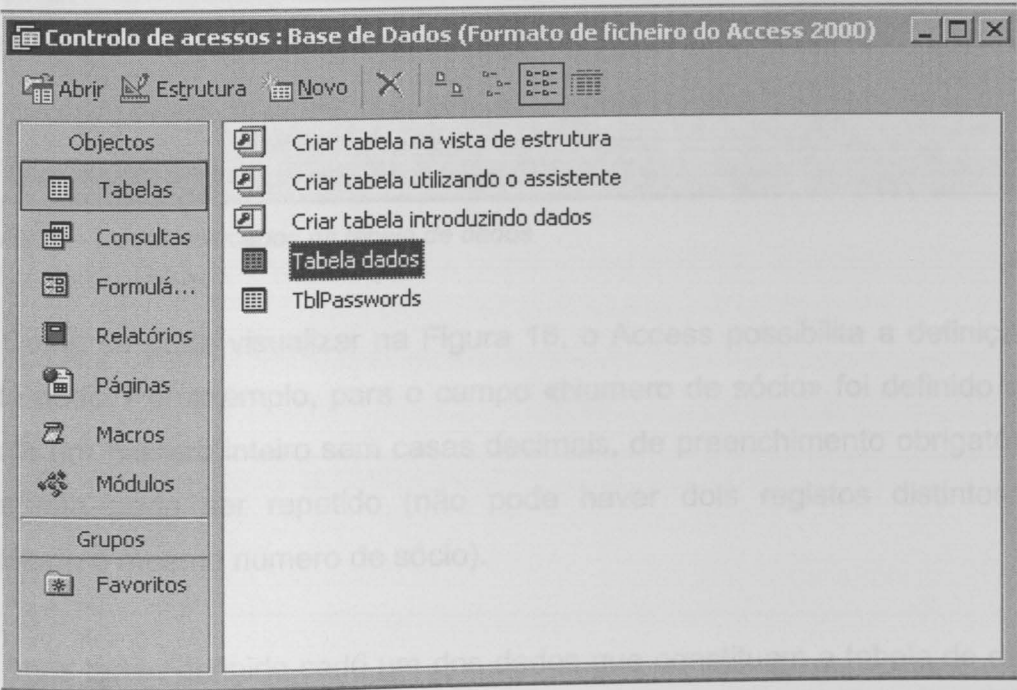


Figura 15 – Criação da tabela de dados

No caso concreto apenas foram colocados os dados que se podem visualizar na Figura 16, uma vez já servirem para exemplificar o funcionamento da aplicação a desenvolver.

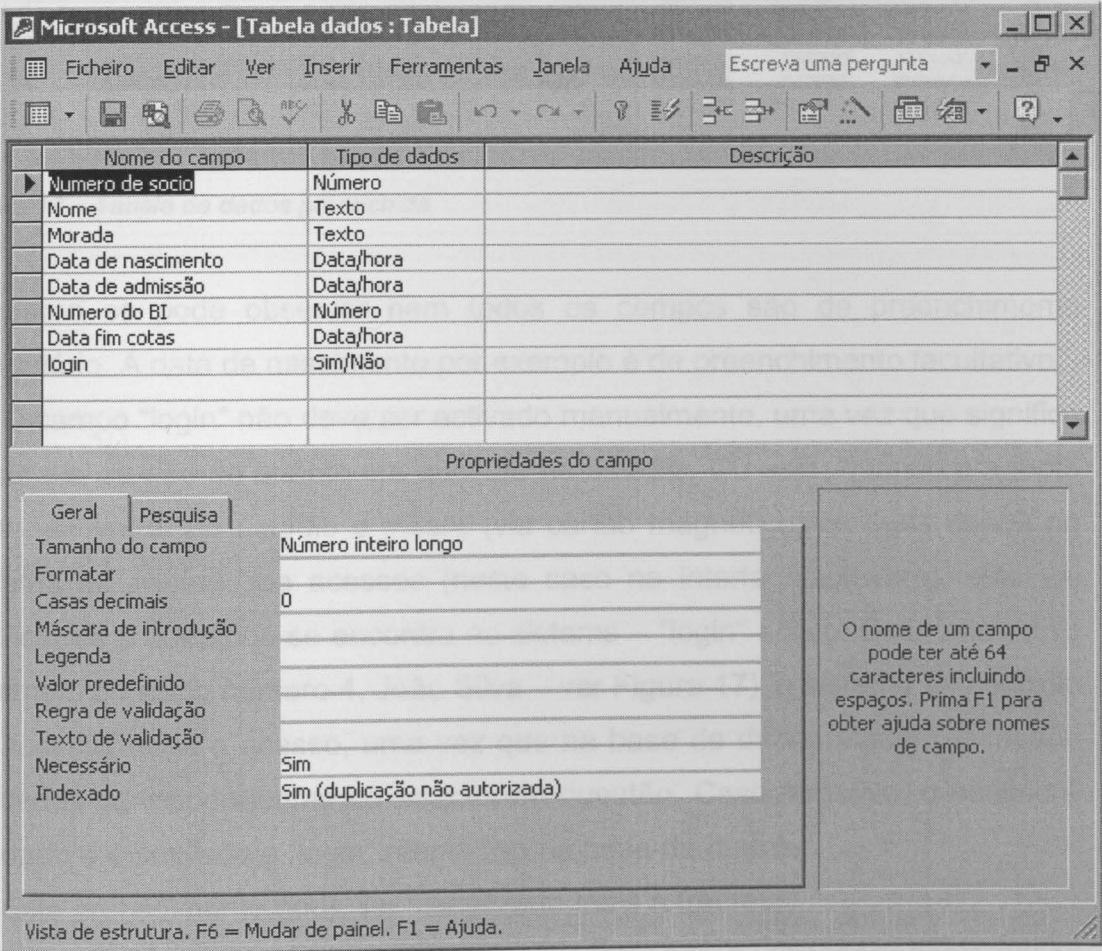


Figura 16 – Dados colocados na tabela de dados

Como se pode visualizar na Figura 16, o Access possibilita a definição de cada dado. Por exemplo, para o campo «Numero de sócio» foi definido como sendo um número inteiro sem casas decimais, de preenchimento obrigatório, o qual não pode ser repetido (não pode haver dois registos distintos que possuam o mesmo número de sócio).

Após ter-se definido cada um dos dados que constituem a tabela de dados, já é possível inserir os dados dos adeptos.

Na Figura 17 é possível visualizar a tabela de dados preenchida com os dados de cinco adeptos.

Tabela dados : Tabela							
Numero de socio	Nome	Morada	Data de nascimento	Data de admissoão	Numero do BI	Data fim cotas	login
1	Ana Maria	rua C	25/Jul/00	27/Jul/00	100040004	02/Dez/04	☐
3	Hugo Miguel	rua A	06/Jun/76	01/Out/80	10000006	30/Mai/05	☐
4	Joao Silva	rua B		15/Fev/76	20987690	12/Out/05	☒
109786	Pedro	avenida X	07/Jan/60	07/Jan/70	20776667	07/Dez/04	☐
2	Rui Pedro	rua D		01/Jan/87	10000001	12/Out/04	☐
							☐

Registo: 6 de 6

Figura 17 – Tabela de dados preenchida

Como se pode observar nem todos os campos são de preenchimento obrigatório. A data de nascimento por exemplo é de preenchimento facultativo.

O campo “login” não deve ser activado manualmente, uma vez que significa a entrada ou não do adepto em questão no estádio. Ou seja, quando o adepto pretende entrar no estádio e insere (via cartão magnético) os seus dados no sistema de controlo de acessos (neste caso na interface/software), este vai verificar se o adepto já se encontra no sistema – “login” activo. Caso afirmativo (exemplo do sócio número 4, João Silva – ver Figura 17), o sistema de controlo de acessos nega o acesso, uma vez que na base de dados alguém já inseriu os dados correspondentes ao adepto em questão. Caso negativo, o acesso é validado e é activado o “login” respectivo na base de dados.

Este procedimento pode ser visualizado mais à frente.

De seguida é necessário criar um formulário onde o utilizador/adepto possa preencher os seus dados (passar o cartão magnético ou o código de barras no respectivo leitor). Esse formulário pode ser visualizado na Figura 18.

Caso a informação do adepto em questão (jika o cartão magnético não for utilizado) já não foi introduzida no sistema, o acesso é validado.

Fisicamente, o adepto entra no estádio, mas a nível de aplicação/software, o “login” do respectivo adepto é activado e o operador pode visualizar os dados do utilizador/adepto (Figura 19).

The image shows a graphical user interface window titled "formInical : Form". At the top, there is a text input field labeled "numero de socio". Below this field, there are three buttons arranged horizontally: "Entrada no sistema" (with a folder icon), "Saída do sistema" (with a left arrow icon), and "Fechar" (with a right arrow icon). At the bottom of the window, there is a "Record:" label followed by navigation icons (back, forward, search, etc.) and the text "1 of 1".

Figura 18 – Formulário inicial

Para além do utilizador/adepto introduzir o número de sócio (dado escolhido para identificar dada um dos utilizadores/adeptos), também tem que escolher se vai entrar ou sair do sistema/estádio.

Numa situação real tal procedimento não faz sentido, isto é se não considerarmos a possibilidade do utilizador/adepto ter a possibilidade de sair do estádio e voltar a entrar, (por exemplo para ir ao parque automóvel buscar qualquer objecto), mas como a aplicação em questão pretende simular o controlo de acessos, há necessidade de colocar estas duas hipóteses “Entrada no sistema” e “Saída do sistema” no formulário principal.

Com este formulário, para além de se poder dar entrada ou saída do sistema, pretende-se também detectar/eliminar eventuais fraudes nas entradas do sistema/estádio (tal como a utilização do mesmo cartão mais de uma vez por diferentes utilizadores/adeptos).

Caso a informação do adepto em questão (lida do cartão magnético) não tenha já sido introduzida no sistema, o acesso é validado.

Fisicamente, o adepto entra no estádio, mas a nível de aplicação/software, o “login” do respectivo adepto é activado e o operador pode visualizar os dados do utilizador/adepto (Figura 19).

Tabela2

Numero de socio: 1

Nome: Ana Maria

Morada: rua C

Numero do BI: 100040004

Data fim cotas: 02-Dez-04

Actualizar dados Fechar

Record: 1 of 5

Figura 19 – Visualização dos dados do utilizador/adepto

Caso contrário, o acesso é negado e é visualizado a seguinte mensagem: «Esse utilizador já está no sistema» (Figura 20).

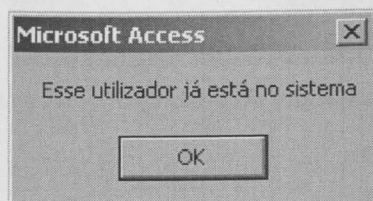


Figura 20 – Mensagem de erro (utilizador já se encontra no sistema)

Para o utilizador/adepto em questão, esta situação só será alterada quando der saída do sistema, ou seja quando for visualizada a mensagem da Figura 21. Só então o utilizador/adepto em questão poderá voltar a entrar no sistema.

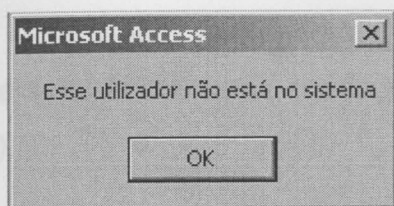


Figura 21 – Mensagem da saída do utilizador

A aplicação/software também possibilita a actualização dos dados dos utilizadores/adeptos por parte dos serviços administrativos.

Após a inserção dos dados do cliente – número de sócio – Figura 18 e posteriormente escolher a opção “Actualizar dados” do menu da Figura 19, é pedida uma password (palavra chave), Figura 22, ao utilizador/administrativo que pretende alterar os dados.

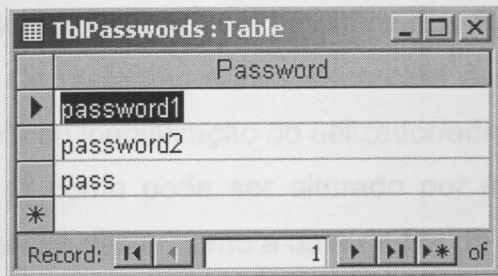
 A screenshot of a dialog box titled 'formPassword : Form'. It contains a label 'Introduza password' followed by a text input field. Below the input field is a button labeled 'Validar'. At the bottom, there is a record navigation bar showing 'Record: 1 of 1'.

Figura 22 – Formulário de introdução de password

 A screenshot of a dialog box titled 'formPassword : Formulário'. It contains a label 'Introduza password' followed by a text input field filled with asterisks (****). Below the input field is a button labeled 'Validar'. At the bottom, there is a record navigation bar showing 'Registo: 1 de 1'.

Figura 23 – Formulário preenchido com uma password correcta

Uma tabela contendo as passwords (palavras chave) validas para esta operação encontra-se criada na base de dados da aplicação/software (Figura 24).



Password
password1
password2
pass

Record: 1 of

Figura 24 – Tabela contendo as passwords válidas

Caso o utilizador tenha permissão (introdução de password válida) para proceder à actualização dos dados do utilizador/adepto em questão é visualizado o formulário da Figura 19, mas com a possibilitando a alteração dos dados do utilizador (Figura 25).

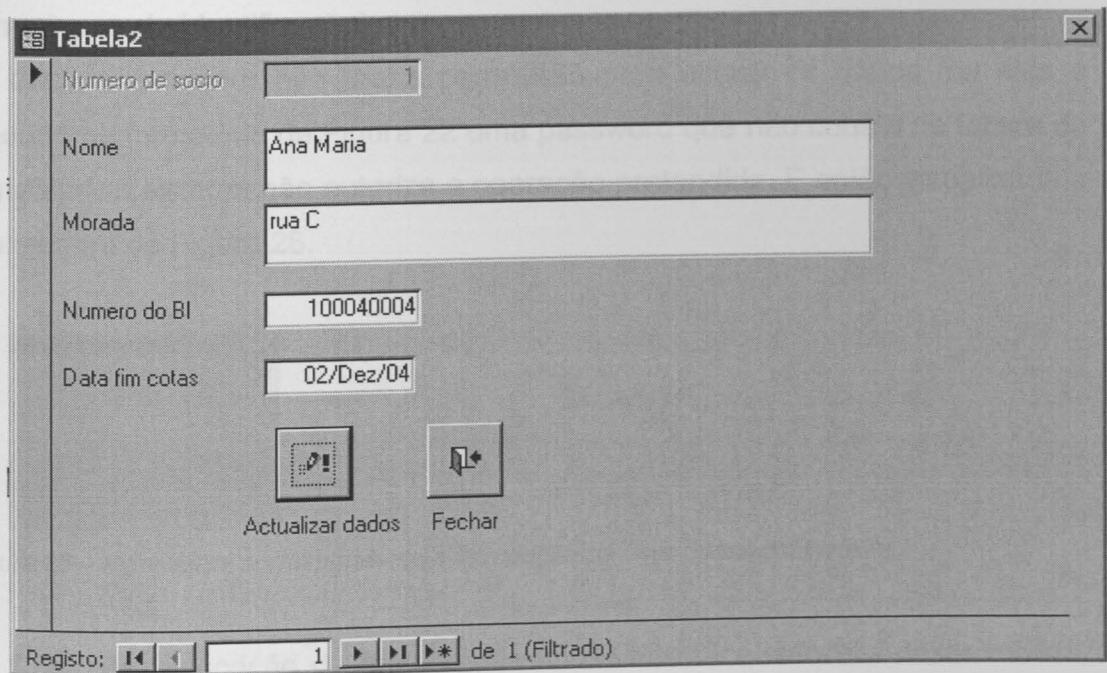


Tabela2

Numero de socio: 1

Nome: Ana Maria

Morada: rua C

Numero do BI: 100040004

Data fim cotas: 02/Dez/04

Actualizar dados Fechar

Registo: 1 de 1 (Filtrado)

Figura 25 – Formulário de alteração dos dados do utilizador

Obviamente o número de sócio não pode ser alterado, uma vez que a identificação do utilizador/adepto foi efectuada por este campo, o qual se mantém constante. De resto é um campo/dado que não sofre qualquer tipo de alteração desde que é criado na base de dados e consequentemente atribuído/associado a determinado utilizador/adepto.

Os restantes dados existentes na base de dados não podem servir como meio de identificação do utilizador/adepto, por diferentes razões.

O nome pode ser alterado por meio de casamento, a morada pode ser alterada assim como a data de fim de cotas (pagas).

Em relação quer à data de nascimento quer à data de admissão, não é possível identificar o utilizador/adepto, porque existe a possibilidade de pelo menos dois utilizadores/adeptos possuírem a mesma data – o que torna a identificação por esta característica inviável.

O número do bilhete de identidade é de facto único e pessoal, mas é considerado de âmbito privado, pondo assim de parte a sua utilização como método de identificação (para além de que crianças até determinada idade não possuem bilhete de identidade, o que as impedia de entrarem no sistema e acrescenta mais uma restrição à utilização do número do bilhete de identidade como forma de identificação).

Caso o utilizador não tenha permissão para alterar os dados, ou seja é inserido no formulário da Figura 22 uma password que não consta na tabela da Figura 24, o sistema não autoriza a operação pretendida. É então visualizada a mensagem da Figura 26.

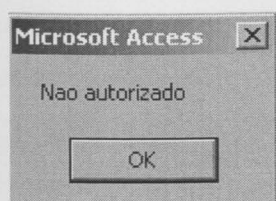


Figura 26 – Mensagem correspondente à introdução de uma password inválida

Com esta descrição do funcionamento da interface/software desenvolvida, dá-se por concluído esta breve apresentação.

3.7 Conclusão

Neste capítulo foi analisada a forma como os “módulos”: Controlo e Gestão de bilhetes, Controlo do fluxo de espectadores, Controlo do registo de cadastro de identificação de associados e Controlo de acessos, se encontram relacionados, ou seja foi demonstrada a integração existente entre eles.

Para cada módulo em particular é efectuada uma descrição dos componentes e das principais características que o constituem, possibilitando assim a compreensão do seu funcionamento.

É também apresentada uma interface/software desenvolvida para que seja possível, de alguma forma, visualizar/simular o funcionamento dos “módulos” anteriormente mencionados.

Após a análise quer dos “módulos” ou subsistemas de Controlo e de Gestão, quer de uma interface/software possível de ser implementada nesses “módulos”, há a necessidade de analisar a forma como a interface/software é controlada. Esse controlo é efectuado recorrendo a métodos de validação, métodos esses que podem recorrer a tecnologias biométricas, convencionais ou mistas, dependendo da aplicação em questão.

No próximo capítulo encontra-se a análise dos métodos de validação possíveis de implementar em sistemas de controlo de acessos.

Capítulo 4 – Métodos de validação

4.1 Introdução

Os sistemas de controlo de acessos podem conter diferentes métodos de validação. Neste capítulo são analisados os métodos de validação mais usuais em sistemas deste género, tendo como objectivo estabelecer critérios de selecção.

4.2 Métodos de validação e identificação biométricos

A análise dos métodos de validação e identificação biométricos é efectuada após uma breve introdução à biometria, nomeadamente o que se entende por biometria (quais os principais conceitos), bem como quais as principais características biométricas utilizadas nos sistemas de controlo de acesso.

Em primeiro lugar irão ser utilizadas tecnologias biométricas como meio de identificação e verificação do utilizador. Posteriormente irão ser apresentadas tecnologias não biométricas ou “convencionais”, ou seja as que não recorrem à biométrica como meio de identificação e validação do utilizador.

Biometria – definição

A biometria (a palavra biometria vem do grego 'bios' – vida e 'metr' – medir) consiste no reconhecimento dos indivíduos através de uma característica física ou comportamental, que são únicas de indivíduo para indivíduo. Entre as características medidas poderemos ter:

- Face;
- Impressão digital;
- Geometria da mão;
- Íris;
- Voz.

Na biometria é necessário efectuar uma distinção entre identificação, reconhecimento e verificação.

Identificação e reconhecimento são essencialmente sinónimos. Em ambos os processos, uma amostra biométrica é apresentada ao sistema biométrico, o qual tenta descobrir a quem pertence a amostra comparando-a com uma base de dados de amostras, biométricas com esperança de encontrar uma que combine/coincide. Esta técnica é chamada comparação **1:n**.

Verificação é uma técnica de comparação **1:1** na qual o sistema biométrico tenta verificar a identidade de um indivíduo. Neste caso, uma amostra biometrica é capturada e comparada com o "template" (molde/registo) previamente armazenado. Se as duas amostras coincidirem, o sistema biométrico confirma que o indivíduo é quem diz ser.

Os sistemas biométricos são essencialmente constituídos por quatro estados distintos – captura, extracção, comparação e validação, nos quais são igualmente aplicados os conceitos identificação, reconhecimento e verificação, ou seja, existem sistemas biométricos **1:n** e **1:1**.

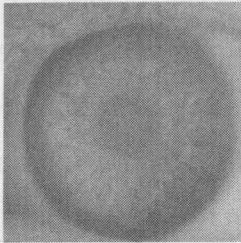
A principal distinção entre estes dois conceitos está relacionada com as questões/perguntas colocadas pelo sistema biométrico e como estas interagem com uma determinada aplicação.

Durante o estado identificação, o sistema biométrico pergunta, “**Quem é este?**” e estabelece a existência ou não do registo. Caso afirmativo, a identidade do indivíduo é a mesma a quem pertence o registo encontrado.

Durante o estado verificação, o sistema biométrico pergunta, “**Este indivíduo é quem diz ser?**” e tenta verificar a identidade do indivíduo com o “template” (molde/registo) previamente armazenado.

Após ter sido efectuada uma breve apresentação sobre o conceito de biometria e quais as diferenças entre validação e verificação em sistemas biométricos, vai-se de seguida analisar as principais características biométricas utilizadas em sistemas de controlo de acessos.

Íris



O reconhecimento da íris é uma tecnologia de autenticação baseada em biometria que oferece o maior grau de fiabilidade e precisão de todas as tecnologias utilizadas para identificação de indivíduos, uma vez que a estrutura de íris é única e mantendo-se estável/invariável no indivíduo durante toda a sua vida. Este facto foi constatado através de observações clínicas (oftalmológicas) efectuadas a um grande número de indivíduos (idades superiores a 2 anos).

Esta tecnologia consiste em analisar os círculos e padrões do olho humano, identificando assim o indivíduo sondado.

Processo de análise automático da íris:

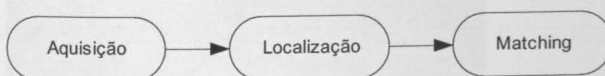


Figura 27 – Processo de análise automático da íris

O processo de análise/reconhecimento automático da íris pode ser subdividido em três etapas distintas – Figura 27.

A primeira etapa está relacionada com a aquisição de uma imagem que contenha a íris, a segunda com a localização da íris na imagem, enquanto que a terceira esta relacionada com o encontrar na base de dados existente, de um padrão de íris que coincida com a do indivíduo em questão.

1. Aquisição da imagem

Um dos principais desafios no processo de reconhecimento automático da íris é a aquisição de uma imagem, com boa qualidade da mesma, sem que o operador sofra qualquer tipo de incómodo.

A íris é um pequeno objecto preto, (cerca de 1 cm de diâmetro) e o operador é muito sensível no que respeita aos seus olhos, assim é necessário um trabalho de engenharia cuidadoso.

A imagem da íris (a adquirir) para além de estar centrada, deve ter resolução e contraste suficiente de forma a ser reconhecida pelo sistema.

Na maior parte dos casos, a imagem da íris é recolhida, por uma câmara, a uma distância muito curta do operador. O olho é iluminado por LED's ("light emitting diode") que envolvem a câmara, os LED's emitem um espectro visível de luz (não prejudicial ao olho humano), directamente para o centro do olho do operador. De seguida é retirada uma fotografia do olho – Figura 28.

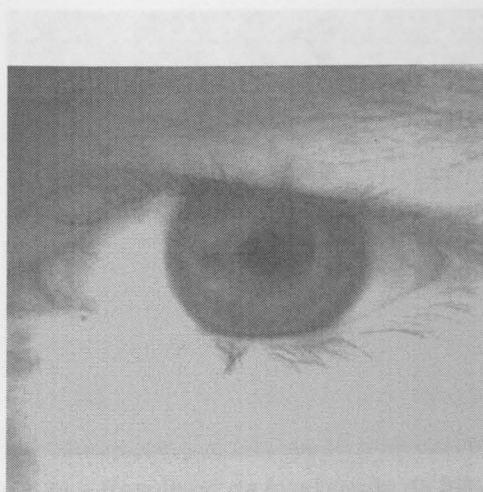


Figura 28 – Exemplo de uma imagem/fotografia do olho

2. Localização da íris na imagem

Antes de se converter a imagem em código, é necessário eliminar tudo o está para além da íris.

Tipicamente a fronteira entre a íris e o resto do olho encontra-se bem definida, contudo o limite superior e inferior é muitas vezes limitado/ocultado pelas pálpebras. Assim o contraste da imagem entre a íris (bastante pigmentada) e a pupila é bastante pequeno.

A localização propriamente dita é efectuada utilizando a primeira derivada da intensidade da imagem de forma a detectar o limite da íris. Tudo o que se encontra para fora desse limite é eliminado de forma a se obter uma nova imagem apenas contendo a íris.

A Figura 29 demonstra o resultado da localização da íris utilizando a Figura 28 como exemplo.

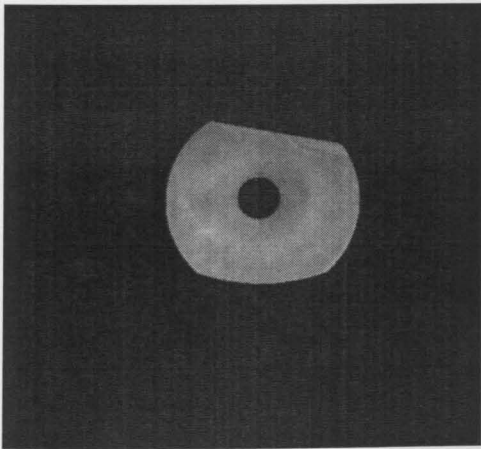


Figura 29 – Resultado da localização da íris

3. Determinação de semelhanças (“Matching”)

Após ter-se uma imagem apenas com a íris, esta nova imagem é processada e codificada num código de 512 bytes, o qual é guardado e usado para comparação com os códigos que se encontram na base de dados.

A imagem da íris não é guardada e só é usada uma vez.

Caso se encontre um código, na base de dados, que coincida com o código em questão, obtemos a identificação do indivíduo.

Reconhecimento facial



O reconhecimento de faces humanas é usado por todos nós na nossa rotina diária. Quer seja para identificar pessoas com quem nos cruzamos ou para saber qual o seu estado de espírito nesse momento, o reconhecimento é fundamental.

De facto, se o ser humano não tivesse a capacidade de reconhecer expressões faciais tais como alegria, ira ou surpresa, o relacionamento social seria bem mais difícil.

A capacidade de reconhecimento começa muito cedo, já que crianças com poucos meses de vida já reconhecem as pessoas que lhes são mais chegadas. Ao longo dos anos, essa capacidade é desenvolvida pelo cérebro humano, culminando na espantosa ferramenta de reconhecimento que quase todos os seres humanos adultos possuem. Mesmo que passem muitos anos ou a face apresente alterações significativas, tais como a presença de óculos, barba ou um corte de cabelo diferente, o reconhecimento acontece normalmente, sem grandes dificuldades.

Num sistema automático de reconhecimento de faces deve ter-se em conta alguns dos aspectos psicofísicos mais importantes da visão humana.

O objectivo de um sistema automático de reconhecimento de faces humanas:

Dado um sinal de vídeo ou uma fotografia de uma face, o sistema deve ser capaz de comparar a face de entrada com as faces armazenadas numa base de dados para determinar se a pessoa em causa faz parte da base de dados.

Apesar de ser um problema conceptualmente simples, a resolução automática deste problema é bastante complexa.

A complexidade deste problema está essencialmente associada à dificuldade em representar uma face de modo a abstrair as características que a diferenciam de outras faces, já que as faces apresentam poucas diferenças substanciais entre elas (todas as faces têm boca, olhos e nariz) e uma mesma face pode variar muito em pequenos intervalos de tempo, por exemplo para diferentes expressões.

Sendo assim, um sistema automático de reconhecimento deve concentrar-se nos aspectos mais relevantes e característicos de uma face, tais como os olhos, nariz ou boca, ao passo que a testa e o queixo têm normalmente pouca informação útil.

Sem dúvida que o elemento facial mais importante são os olhos que, muitas vezes, mesmo isolados, permitem reconhecer uma face. O inverso também se aplica, ou seja, uma face com os olhos ocultos torna-se difícil de identificar.

Constituição de um sistema automático de reconhecimento de faces humanas:

Um sistema de reconhecimento automático de faces é formado por três blocos fundamentais: detecção e localização da face, extracção de características faciais e reconhecimento da face.

A Figura 30 mostra como estão interligados estes blocos.

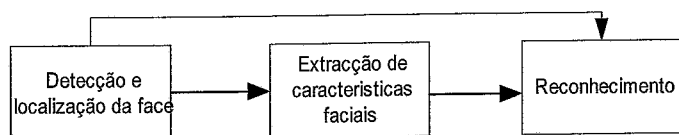


Figura 30 – Esquema de blocos básico de um sistema de reconhecimento de faces

O primeiro bloco deste sistema visa a detecção e localização da face numa imagem ou sequência de imagens.

A face a ser reconhecida, está integrada no ambiente que a rodeia, podendo ser este mais ou menos complexo.

Para levar a cabo a identificação, a face necessita de ser isolada da restante imagem para se poder aplicar sobre ela os passos seguintes.

a) Detecção e Localização da Face incluindo Extração de Características Faciais

O problema de detectar uma face e as suas principais características consiste em localizar os olhos, nariz, boca e contornos da face, bem como outros elementos faciais (por exemplo, as sobrancelhas).

Embora a maioria dos esforços para a detecção das características faciais sejam motivados pela necessidade de normalizar a face antes da fase de reconhecimento, alguns métodos usam estas características para fazer o seguimento da face ou para fazer a sua detecção em imagens mais críticas, por exemplo com partes da face obstruídas por outros objectos.

Existem muitos métodos para detectar e localizar uma face numa imagem.

b) Reconhecimento da Face

A última etapa de todo o processo de reconhecimento é o reconhecimento propriamente dito.

A maior parte dos sistemas de reconhecimento de faces trabalha com imagens, em que a face está numa posição frontal ou quase frontal e quase todos eles usam a mesma técnica, que consiste em fazer uma comparação com faces conhecidas, armazenadas numa base de dados. Esta comparação é feita usando uma medida de semelhança entre as mesmas no espaço usado para representar as faces. A face correspondente ao modelo que apresenta a menor distância é a identificada como a face a reconhecer desde que essa distância seja inferior a um determinado limite, caso contrário a face não é reconhecida.

Há três abordagens principais para a representação das faces conhecidas na base de dados – Figura 31:

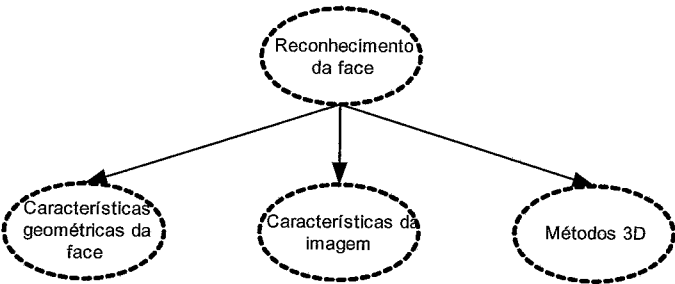


Figura 31 – Principais abordagens existentes para o reconhecimento de faces

A abordagem geométrica utiliza a configuração espacial das características faciais para representar a face.

As técnicas baseadas em características geométricas utilizam a dimensão e a distância entre os elementos constituintes da face (olhos, sobrancelhas, nariz, boca, etc.) ou quaisquer outros pontos para fazer a identificação da mesma. A configuração espacial dos elementos faciais é traduzida por um vector que contém medidas dos elementos faciais tais como distâncias, ângulos e curvaturas.

Este algoritmo utiliza as posições dos pontos de controlo para calcular um conjunto de distâncias a partir do qual se efectua o reconhecimento.

A definição do conjunto de características resume-se à escolha de um conjunto adequado de distâncias calculadas a partir de um conjunto de pontos.

Estes pontos de controlo devem variar pouco para imagens de faces da mesma pessoa, de forma a que os erros associados à extracção de características sejam o mais baixos possível.

O conjunto de características escolhido envolve 24 distâncias – Figura 32.

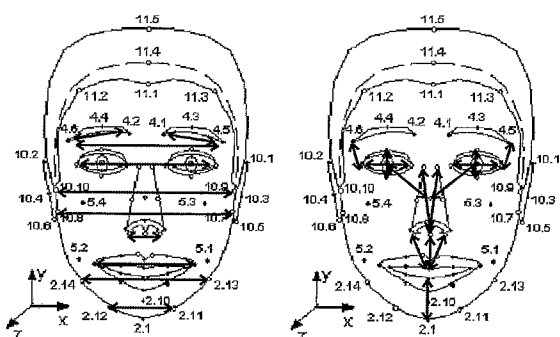


Figura 32 – Exemplo de alguns pontos de controlo e respectivas distâncias

A abordagem baseada na textura da imagem que usa informação inerente aos *pixels* que constituem a imagem da face. Este tipo de abordagem usa a imagem da face como um todo para o processo de reconhecimento ou seja as faces são representadas através de imagens ou através de características não geométricas obtidas a partir da imagem da face.

Os métodos baseados em informação 3D, podem utilizar qualquer uma das abordagens anteriores.

Nestes métodos coloca-se contudo a possibilidade da introdução de mais uma dimensão: a profundidade. O objectivo da introdução de mais uma dimensão consiste em desenvolver um sistema que funcione em condições mais flexíveis, tanto a nível de rotação e translação como ao nível da iluminação.

Geometria da mão



Este método é baseado no facto de quase todos os indivíduos terem a forma/contorno da mão diferente e que essa forma/contorno não se altera a partir de uma certa idade.

Os sistemas baseados em geometria da mão produzem estimativas de certas medidas da mão, tais como o comprimento e largura dos dedos – Figura 33.

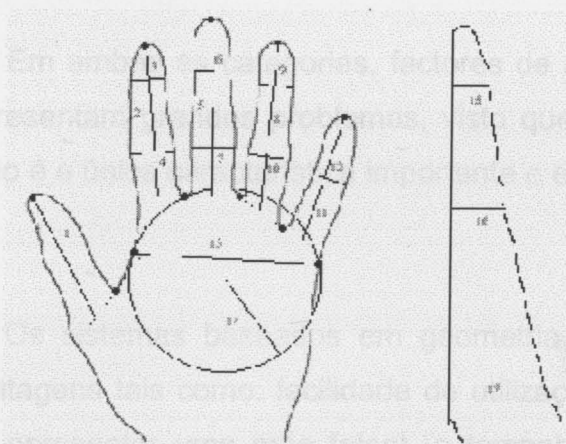


Figura 33 – Exemplo de certas medidas da mão

Estes sistemas utilizam scanners ópticos que efectuam a aquisição da imagem da mão.

Basicamente existem duas subcategorias de scanners ópticos.

Uma primeira categoria, onde os scanners criam uma imagem a preto e branco da forma/geometria da mão.

A imagem adquirida é então processada por um software (computador) próprio. Nesta categoria apenas é possível utilizar características com duas dimensões.

Na segunda categoria, são utilizados dois sensores (vertical e horizontal) para efectuar a aquisição da imagem da forma/geometria da mão. Assim temos características com três dimensões, o que implica mais informação e melhores resultados.

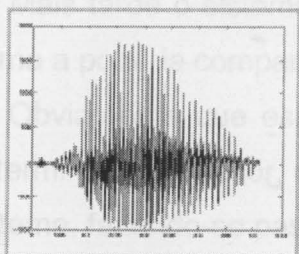
Após a aquisição da imagem, e como já foi referido anteriormente, esta imagem é então processada por um software (computador), o qual a converte (duas ou três dimensões) num código ("template") de 9 bytes. Esse código é que será comparado e posteriormente guardado, na base de dados.

Em ambas as categorias, factores de ruído como poeiras ou gordura, não apresentam grandes problemas, visto que o contorno da forma/geometria da mão é a única característica importante e esta não é afectada.

Os sistemas baseados em geometria da mão apresentam determinadas vantagens tais como: facilidade de utilização, resistência à fraude (dificuldade de apresentar uma mão falsa), o tamanho reduzido do "template" criado (9 bytes), aceitação por parte dos utilizadores (este método é mais facilmente aceite do que, por exemplo, o scanner óptico), etc.

Contudo, como a maior parte dos sistemas de validação, também apresenta desvantagens, tais como: custo (o preço varia com o fornecedor, mas o valor médio encontra-se compreendido entre os 1400€-2000€), ferimentos na mão (como na maioria dos sistemas biométricos, alterações fisiológicas podem

Voz



A voz é o meio de comunicação mais utilizado em todo o mundo. Por esta razão, não podia ser excluída desta breve análise (de alguns dos principais métodos de validação biométricos utilizados em sistemas de controlo de acessos).

O princípio da verificação da voz consiste na análise da voz do utilizador de forma a armazenar uma amostra ("voiceprint"), a qual será mais tarde utilizada para identificação e/ou verificação.

Há, portanto que distinguir verificação de voz e reconhecimento de voz, sendo que o objectivo da primeira é verificar "*quem disse isto*", enquanto que no caso do reconhecimento da voz, o objectivo é "*descobrir o que foi dito*".

Ambas as tecnologias estão ainda em fase de desenvolvimento, apesar de existirem já alguns sistemas de controlo de acessos que recorrem a estas tecnologias.

A verificação da voz esta orientada para as características da voz que produzem a fala propriamente dita e não para o som ou pronuncia. As características da voz dependem da dimensão da área vocal, boca, cavidades nasais e outros mecanismos no corpo humano associados à fala.

Como já foi mencionado anteriormente, este tipo de sistema, tipicamente solicita ao utilizador que pronuncie uma determinada frase, a qual é processada e armazenada num “template” (“voiceprint”).

Mais tarde o sistema pede ao utilizador para pronunciar a mesma frase de forma a podê-la comparar.

Obviamente que este sistema é facilmente vulnerável, pois basta que um determinado utilizador, munido de uma gravação de um outro utilizador, iluda o sistema, fazendo-se passar pelo utilizador a quem pertence a gravação.

Mas este tipo de sistema apresenta ainda mais um problema, o ruído de fundo. Apesar do sistema admitir uma determinada variação quando efectua a comparação entre o “template” (“voiceprint”) existente e a frase que o utilizador esta a pronunciar, basta que o ruído de fundo seja superior ao limite suportado pelo sistema, para que o resultado seja afectado.

Contudo, em sistemas mais sofisticados e de forma a evitar a vulnerabilidade do sistema face à utilização de gravações por parte dos utilizadores, na fase de registo, é solicitado ao utilizador que pronuncie diversas frases, incluindo números. Assim, na fase de autenticação, o sistema pede ao utilizador que pronuncie uma frase à sorte (random) num determinado espaço de tempo.

Relativamente a vantagens, um sistema de controlo de acessos que utilize como método de validação a voz, tem como principal vantagem, o facto de não necessitar de nenhum tipo de hardware especial. Basta um microfone ligado ao computador. A qualidade do microfone irá influenciar a qualidade do som captado.

Impressão digital



A utilização da impressão digital como método de identificação é a tecnologia de autenticação baseada em biometria que a mais tempo é utilizada.

Desde a utilização de tinta, de forma a obter a impressão digital, à utilização de scanners de leitura óptica, a tecnologia foi evoluindo até ao ponto em que se tornou praticamente normal/banal a sua utilização no dia a dia.

Todos nós temos impressões digitais únicas e imutáveis. A impressão digital é constituída por uma série de cumes e depressões na superfície dos dedos – Figura 34.

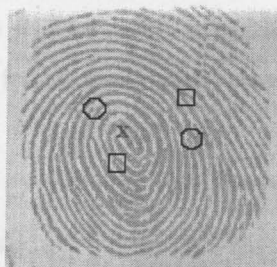


Figura 34 – Imagem de uma impressão digital com o centro e quatro pormenores/detalhes específicos

A unicidade de uma impressão digital pode ser determinada através da textura/padrão dos cumes e depressões assim como nos pormenores/detalhes. Estes pormenores/detalhes são características específicas de determinados cumes que ocorrem em bifurcações ou no final de depressões.

Assim as técnicas que utilizam a impressão digital podem ser divididas em duas categorias, a baseada nos pormenores/detalhes e a baseada em correlação.

No caso em que a técnica é baseada nos pormenores/detalhes, o primeiro aspecto a ser efectuado é a detecção da posição dos pormenores/detalhes no dedo, sendo de seguida marcado o posicionamento relativo de cada pormenor/detalhe.

4.3 Métodos de validação e identificação não biométricos "convencionais"

Na Figura 35 encontra-se alguns tipos de pormenores/detalhes possíveis de encontrar em impressões digitais.

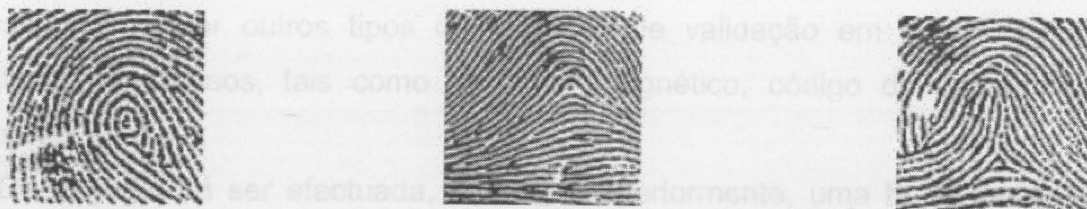


Figura 35 – Exemplos de pormenores/detalhes possíveis de encontrar em impressões digitais

O problema das técnicas baseadas em pormenores/detalhes é a dificuldade em extrair com precisão os pormenores/detalhes quando a impressão digital é de fraca qualidade (baixa resolução).

O método baseado em correlação surgiu para superar as limitações que as técnicas baseadas em pormenores/detalhes apresentavam. No entanto, este tipo de método também apresenta algumas restrições, tais como a necessidade da existência de um local exacto para o utilizador colocar o dedo – quando lhe for tirado a impressão digital – e é afectada pela rotação e translação da imagem da impressão digital.

Este método compara o padrão global dos pormenores/detalhes (cumes e depressões) de forma a verificar se o alinhamento das duas imagens –

impressão digital do utilizador em causa e o respectivo “template” (padrão/molde /registo) – coincidem.

O desempenho deste tipo de técnica depende na exactidão da detecção dos pormenores/detalhes bem como nas sofisticadas técnicas de “matching” (combinação) utilizadas para efectuar a comparação das duas imagens.

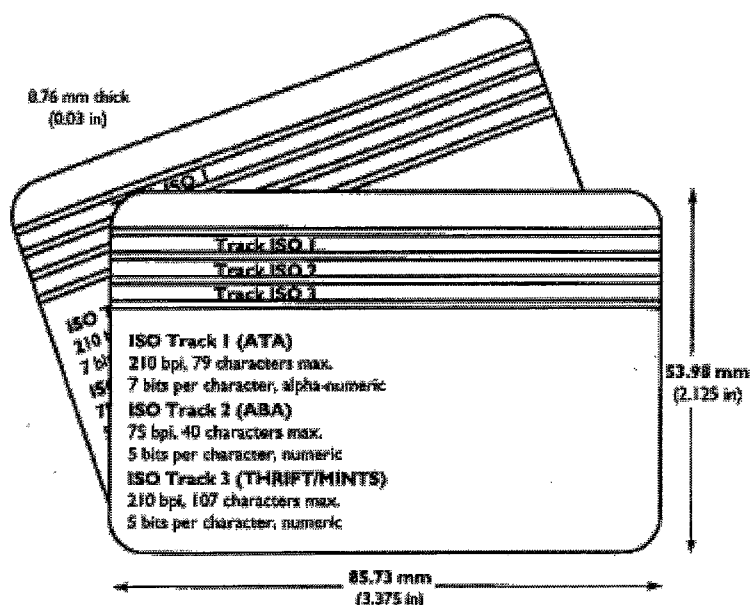
4.3 Métodos de validação e identificação não biométricos “convencionais”

Para além dos métodos biométricos acima mencionados, também é possível encontrar outros tipos de métodos de validação em sistemas de controlo de acessos, tais como o cartão magnético, código de barras ou etiquetas RFID.

De seguida irá ser efectuada, tal como anteriormente, uma breve análise destes dois métodos de validação.

Para estes métodos, uma vez que são suportados com tecnologia convencional, são apresentadas as características estabelecidas de forma normalizada.

Cartão magnético



O cartão magnético bem como o código de barras são os métodos de validação mais frequentes em sistemas de controlo de acessos, pois trata-se de tecnologias já à muito conhecidas/dominadas e de fácil acesso e implementação.

O cartão magnético é constituído por uma banda magnética, a qual contém a informação que se pretende que o cartão possua.

Cada cartão magnético possui três pistas distintas, nas quais há a possibilidade de gravar a informação desejada.

A pista 1 (IATA) foi desenvolvida por a Associação Internacional de Transportes Aéreos (“International Air Transport Association”) para automatizar sistemas de venda de bilhetes e reserva. Também é tipicamente utilizada em aplicações de os cartões de crédito.

A pista 2 (ABA) foi desenvolvida por a Associação Americana de Banqueiros ("American Bankers Association") para automatizar as transacções financeiras. Esta pista é muitas vezes utilizada para controlo de acessos bem como par aplicações que requeiram apenas um código de identificação.

A pista 3 (THRIFT) foi desenvolvida nomeadamente pela indústria de créditos e empréstimos para aplicações que requerem a constante actualização de informações em cada transacção em que são envolvidas. Um exemplo destas aplicações é o cartão de débito.

Em relação à capacidade de cada pista, a pista 1 pode armazenar 79 caracteres alfanuméricos, a pista 2 40 caracteres numéricos, enquanto que a pista 3 pode armazenar até 107 caracteres numéricos.

Código de barras



A tecnologia de código de barras foi desenvolvida visando a entrada de dados automatizados e a abolição de erros humanos de digitação.

Um leitor próprio incide um feixe de luz no símbolo e capta a luz reflectida. A imagem recebida é comparada com uma tabela interna e decodificada.

Após a decodificação, o leitor retorna/envia para o computador os dígitos que compõem o símbolo lido, como se tivessem sido digitados no teclado. Assim, o código tem sua entrada no computador de forma muito rápida e sem erros.

A tecnologia de código de barras está destinada a quase todo tipo de aplicação onde se deseje automatizar a identificação de produtos, mercadorias, pessoas, documentos, etc.

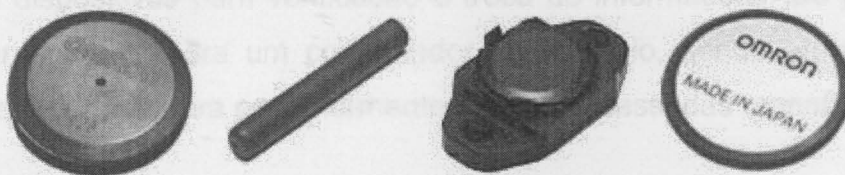
Tem sido extremamente útil no comércio, nos bancos, na indústria e na identificação de pessoal (controlo de acessos), através de crachás, em portarias e marcação de ponto.

Com o tempo foram desenvolvidos muitos tipos de codificação para gerar símbolos com barras. Os mais conhecidos são:

CodaBar	Code 49	Data Code	Planet Code
CodaBlock	Code 93	Interleaved 2 of 5	Plessex Code
Code 1	Code 128	Maxi Code	PDF 417
Code 16	UPC	MSI Code	PostNet
Code 11	EAN	Nw-7 Code	Telepen
Code 39	Vericode	e outros	

Em relação ao código de barras como meio de validação em sistemas de controlo de acesso, pode-se dizer que o seu funcionamento é idêntico ao do cartão magnético. Em vez de existir uma banda magnética, onde a informação é armazenada, a mesma informação é codificada num código, o código de barras.

Etiqueta RFID



Introdução

As etiquetas (“tags”) RFID são métodos muito populares de identificar, monitorar e controlar objectos, animais ou pessoa.

Contrariamente à tecnologia de código de barras, a tecnologia RFID tem a capacidade de providenciar a informação em tempo real, com maior alcance de leitura e sem a necessidade de existir contacto.

RFID é uma expressão generalizada para a tecnologia que utiliza comunicações em rádio frequência no intercâmbio dos dados entre um dispositivo de memória portátil e um computador.

Um sistema RFID compreende um receptor/leitor equipado com uma antena e um conjunto de etiquetas (“tags”) RF, cada uma com antena própria, que suportam a informação (Figura 36).

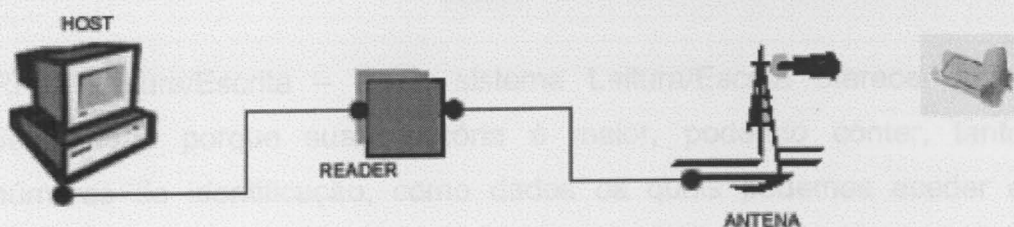


Figura 36 – Constituição de um sistema RFID

O modo de funcionamento é simples, o leitor, via antena, transmite um sinal de rádio de baixa frequência para a etiqueta. O chip integrado nesta é activado com a energia recebida do sinal, estabelecendo-se um diálogo rápido entre dois dispositivos para verificação e troca de informações. De posse destas, o leitor envia-as para um computador de controlo, sendo armazenadas numa base de dados para posteriormente serem processadas e analisadas.

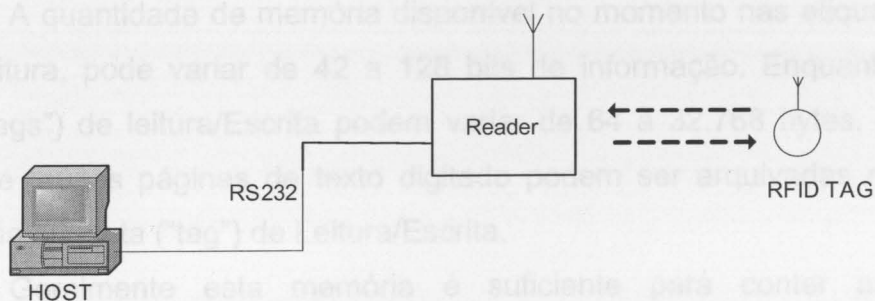


Figura 37 – Funcionamento de um sistema RFID

Existem dois tipos básicos de Identificação por Rádio Frequência, cada um com capacidade e aplicações diferentes:

- 1) RFID Leitura – O mais simples dos dois é o RFID “Read Only”, no qual as etiquetas (“tags”) contêm memória limitada e um código fixo de identificação. A memória dessas etiquetas (“tags”) pode ser alterada e elas funcionam como um código de barras, identificando o objecto ao qual estão anexos.
- 2) RFID Leitura/Escrita – Já o sistema Leitura/Escrita oferece maior flexibilidade porque sua memória é maior, podendo conter, tanto números de identificação, como dados os quais podemos aceder e actualizar a qualquer hora.

As etiquetas (“tags”) podem ser energizadas através de uma bateria interna (geralmente chamados de TAG activo) ou por acoplamento indutivo (TAG passivo).

Os “TAGs” passivos não necessitam de manutenção e a sua vida útil é praticamente ilimitada. A vida útil dos “TAGs” activos pode estar limitada à vida da bateria que os energiza, embora alguns deles sejam fornecidos com baterias extras.

A quantidade de memória disponível no momento nas etiquetas (“tags”) de Leitura, pode variar de 42 a 128 bits de informação. Enquanto as etiquetas (“tags”) de leitura/Escrita podem variar de 64 a 32.768 bytes, o que significa que muitas páginas de texto digitado podem ser arquivadas na memória de uma etiqueta (“tag”) de Leitura/Escrita.

Geralmente esta memória é suficiente para conter as informações necessárias, deixando ainda espaço para o possível crescimento do sistema.

A comunicação por rádio frequência apresenta vantagens sobre as tecnologias similares como código de barras.

Ambientes industriais mais rústicos, muitas vezes danificam as etiquetas de códigos de barras, ou ainda tornam difícil a sua leitura pelos scanners e assim não funcionam com a fiabilidade necessária.

Os sistemas RFID por sua vez, podem operar na presença de poeira, fluidos, altas temperaturas ou vibração. As etiquetas (“tags”) RF são mais caras que a etiquetas de códigos de barras porem podem ser reutilizados e o seu tempo de vida operacional é muito longo.

A velocidade de um sistema RFID Somente Leitura é comandada pelo comprimento do código, pela velocidade da transferência dos dados para a etiqueta (“tag”), pela faixa operacional, pela frequência RF da portadora da etiqueta (“tag”) para o link da antena e pela técnica de modulação utilizada na transferência de dados. Esses dados variam conforme o produto específico utilizados em cada aplicação.

Os sistemas Leitura/Escrita, tipicamente de baixa frequência, operam à velocidade de 100 ou 200 bytes por segundo, contudo poderemos ter etiquetas

com uma transferência de 3.000 bytes por segundo – etiquetas RFID
Leitura/Escrita de alta velocidade e baixa frequência.

Uma consideração muito importante ao seleccionar um sistema RFID é a frequência da faixa da portadora utilizada na transferência de informações entre etiqueta e antena. A FCC (Comissão de Comunicação Federal) restringe as operações à faixa ou muito baixas (50 a 500 kHz) ou de micro ondas (0,9 a 2,5 GHz).

4.4 Conclusão

Neste capítulo foi efectuada uma análise dos principais métodos de validação possíveis de implementar em Sistemas de Controlo de Acessos.

A possibilidade de recorrer a tecnologias biométricas, convencionais ou mistas implica uma análise destes tipos de tecnologias em separado.

Assim, para cada tipo de tecnologia é efectuada uma análise as principais características ou componentes que a constituem.

Pela diversidade de tecnologias existentes, a escolha do(s) método(s) de validação a implementar nos sistemas de controlo de acessos depende essencialmente das especificações de cada caso concreto, tais como o local, quantidade de utilizadores e grau/nível de segurança pretendido.

Cada tipo de tecnologia, biométrica ou convencional, encontra-se mais destinada a um determinado tipo de sistema de controlo de acessos, podendo mesmo haver o caso em que as duas tecnologias se complementem.

Como conclusão deste capítulo é encerrada a análise dos “módulos” de Controlo e de Gestão.

No processo de desenvolvimento de um Sistema de Controlo de Acessos, pela sua complexidade e dimensão é apropriado validar o modelo com recurso à simulação em funcionamento do sistema. Este assunto é objecto dos próximos capítulos.

Capítulo 5 – Ambiente de simulação

5.1 Introdução

A necessidade de recorrer à simulação torna-se uma realidade sempre que se pretende analisar um sistema cuja dimensão, complexidade e sensibilidade assim o justifiquem. As consequências que um sistema real poderia sofrer sempre que se pretendesse estudar, alterar ou introduzir qualquer tipo de parâmetro poderia levar ao mau funcionamento ou mesmo à quebra/ruptura do mesmo.

Uma vez que os modelos de simulação podem ser quase tão detalhados quanto os sistemas reais, novas políticas e procedimentos operacionais, regras de decisão, fluxos de informações podem ser avaliadas sem que o sistema real seja perturbado.

Com o avanço da informática, (hardware e softwares robustos), torna-se cada vez mais frequente associar o conceito de optimização ao modelo de simulação, associando assim os objectivos da optimização às vantagens da simulação.

Em outras palavras, pode-se determinar o “objectivo óptimo” de um modelo de simulação incluindo aspectos probabilísticos, através do uso de variáveis não determinísticas ou estocásticas.

Como pode ser visualizado no próximo capítulo, mais precisamente no ponto 6.3, usualmente recorre-se à simulação como método de validação de um determinado modelo, uma vez que esse modelo representa o sistema ou o processo que se pretende analisar/validar.

Uma questão que nestes casos se coloca é qual o tipo de software mais apropriado para efectuar a simulação pretendida.

Neste capítulo vai apresentar-se o software escolhido para simular o sistema de controlo de acessos, assim como o porquê dessa escolha.

5.2 O software utilizado

O software utilizado para proceder à validação e simulação do modelo que representa o sistema de controlo de acessos em questão foi o simulador **Arena**, uma vez tratar-se de um software capaz de simular/validar o funcionamento dos aspectos que se consideram críticos neste tipo de sistema – ou seja as filas de espera associada a cada entrada no estádio.

Uma descrição detalhada das suas características face ao modelo de funcionamento do sistema a simular ilustra a propriedade desta escolha.

O posicionamento do Arena no universo das linguagens de programação e dos simuladores será então o seguinte:

Linguagens de Programação – Linguagens desenvolvidas para aplicações generalistas, não sendo impossível usá-las para simulação, implicam um grande esforço de programação. Podem ser consideradas a base de todos os programas existentes. Exemplos destes tipos de linguagem são: Fortran, Pascal, C, etc.

Linguagens de Simulação – Linguagens de programação de alto nível para simuladores. São linguagens concebidas com rotinas específicas para facilitar a construção de modelos de tipo genérico como por exemplo para abordagens por eventos, por processos, mistas das duas anteriores e ainda simulação de modelos contínuos. Estas linguagens têm já módulos definidos para criação e gestão das listas de eventos futuros, geradores de distribuições e ferramentas de tratamento estatístico. Exemplos destes tipos de linguagem são: GPSS, SIMAN V, SIMSCRIPT e SLAM.

Linguagens de Simulação orientada a objectos – Linguagens de programação baseadas em estruturas de dados e rotinas que as ligam e as fazem evoluir. Tem como principal vantagens face às anteriores uma maior disciplina de programação e por isso mais facilidade na verificação e correcção

de problemas. Um objecto consiste num conjunto de variáveis que descrevem o seu estado em cada momento e num conjunto de procedimentos que descrevem as acções que é capaz de executar. Exemplos destes tipos de linguagens são: SIMULA, MODSIM, etc.

Simuladores – Programas desenvolvidos especialmente para execução de programas de simulação. Nestes programas não é necessário o conhecimento de nenhuma linguagem de programação. São programas mais ou menos flexíveis dependendo da sua capacidade de modelar sistemas pertencentes a áreas de actuação empresarial diferentes. Exemplos destes programas são: SIMFACTORY, ProModel, AutoModel, Taylor II, ARENA, etc.

Simuladores específicos – Baseados nos programas vistos atrás, são programas configurados para sistemas em que são usados, que exigem do utilizador, somente uma introdução de dados relativos ao sistema em causa. A sua flexibilidade é reduzida. Exemplo de um destes simuladores específicos baseados em Arena é o CALLCENTER.



Introdução ao Arena

O Arena é um dos muitos simuladores existentes pertencendo ao grupo dos simuladores que aliam a facilidade e rapidez de execução de aplicações à flexibilidade necessária para permitir o seu uso em áreas muito distintas como por exemplo serviços, transportes, distribuição e sistemas de produção.

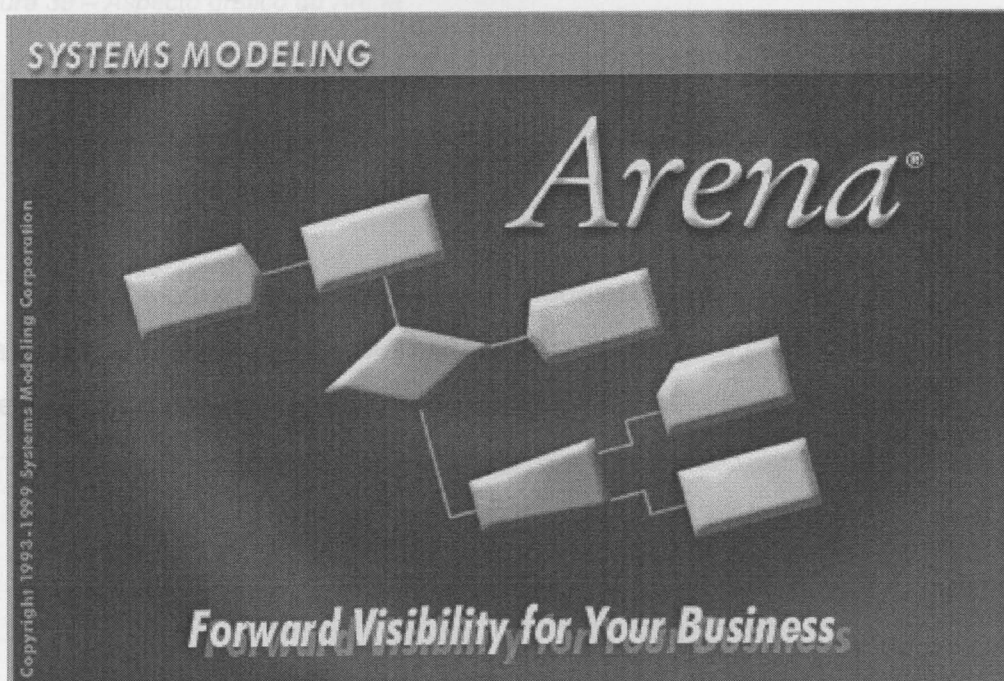


Figura 38 – Software utilizado na simulação

Características do Arena

O Arena foi desenvolvido pela “Systems Modeling Corporation” (adquirida pela Rockwell Automation) e é formado por um simulador (SIMAN), que executa e guarda os resultados dos cálculos efectuados e por uma animação (CINEMA) que permite ao utilizador a visualização da evolução física da simulação.

O objectivo do Arena é permitir o uso da ferramenta SIMAN/CINEMA sem o esforço necessário para aprendizagem e aplicação da linguagem de programação. Além destes dois componentes inclui também ferramentas estatísticas para tratamento de dados de entrada e de saída.

O Arena trabalha sobre ambiente Windows, ou seja os seus menus equivalentes em função e aspecto gráfico aos existentes nos programas de Windows (Figura 39).

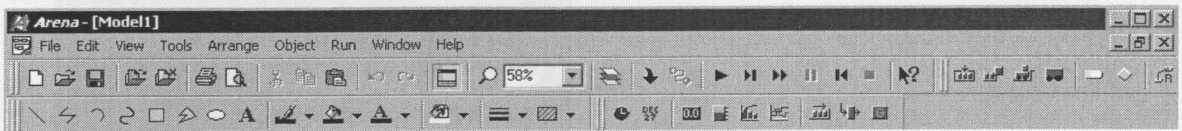


Figura 39 – Aspecto gráfico do Arena

Módulos a utilizar na simulação

O Arena é constituído por diversos módulos. A finalidade deste capítulo não é a análise de todos esses módulos, assim apenas se vão analisar os módulos que irão ser utilizar na simulação do modelo em estudo (Capítulo 6).

Módulo “Arrive” ou de Chegada



Figura 39 – Módulo “Arrive”

Este é o elemento de “nascimento” das entidades, a sua janela esta dividida em três áreas: “Enter Data”, “Arrival Data” e “Leave Data”.

o valor 1, de modo a que só seja gerada uma entidade de cada vez.

⇒ “First Creation” – número de entidades criadas no início da simulação – normalmente deixa-se por preencher, o que significa que não se quer especificar. Por defeito será criada a 1ª entidade no início da simulação.

⇒ “Time Between” – tempo entre chegadas – permite escolher a distribuição de chegada entre as diversas distribuições existentes.

⇒ “Max Batches” – dimensão máxima do grupo – o valor por defeito, caso não seja preenchido, é infinito.

Figura 40 – Caixa de dialogo do módulo "Arrive"

Na área "Enter Data" é colocado na caixa de escrita o nome que se pretende dar à estação.

Na área "Arrival Data" vai preencher-se as caixas de escrita:

- ⇒ "Batch Size" – dimensão do grupo – normalmente é preenchido com o valor 1, de modo a que só seja gerada uma entidade de cada vez.
- ⇒ "First Creation" – número de entidades criadas no início da simulação – normalmente deixa-se por preencher, o que significa que não se quer especificar. Por defeito será criada a 1ª entidade no início da simulação.
- ⇒ "Time Between" – tempo entre chegadas – pode-se escolher a distribuição de chegada entre as diversas distribuições existentes.
- ⇒ "Max Batches" – dimensão máxima do grupo – o valor por defeito, caso não seja preenchido, é infinito.

⇒ “Mark Time Attribute” – significa que cada entidade criada terá como atributo o nome que colocarmos nesta caixa de texto.

Na área “Leave Data” só se vai fazer “pick” à opção “Connect”, de modo a que as entidades que entram no sistema prossigam imediatamente para o servidor ou para a sua fila de espera, sem tempos de percurso (“Route Time”) associados à opção “Route”.

Módulo “Server” ou de Serviço (Recurso)

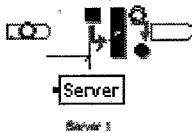


Figura 41 – Módulo “Server”

Uma vez arrastado este módulo para a área de animação, clicando sobre a palavra “Server” fica disponível para alteração a caixa de dialogo deste módulo. Tal como a anterior divide-se em três áreas: “Enter Data”, “Servar Data” e “Leave Data” (Figura 42).

Figura 42 – Caixa de diálogo do módulo "Server"

Na área "Enter Data" é colocado na caixa de escrita o nome que se pretende dar à estação.

Na área "Server Data" vai preencher-se as caixas de escrita:

- ⇒ "Resource" – nome do recurso que será atribuído pelas entidades que passem pelo sistema.
- ⇒ "Capacity Type" – tipo de capacidade do recurso – normalmente aceita-se a opção por defeito. Esta opção significa que o recurso tem capacidade constante.
- ⇒ "Capacity" – capacidade – normalmente aceita-se a opção por defeito 1. Significa que só se tem um servidor deste tipo.
- ⇒ "Resource Statistics" – estatísticas relacionadas com o recurso – normalmente aceita-se a opção por defeito.
- ⇒ "Process Time" – tempo de processamento – pode-se escolher a distribuição que corresponde ao tempo de processamento do recurso entre as diversas distribuições existentes.

Na área “Leave Data” só se vai fazer “pick” à opção “Connect”, de modo a que não exista mais nenhum tempo associado além do tempo de operação e do eventual tempo de espera caso o servidor esteja ocupado.

Módulo “Inspect” ou de Inspeção

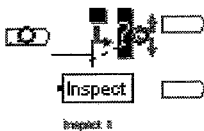


Figura 43 – Módulo “Inspect”

Este módulo, tal como o módulo “Server” permite configurar um posto de trabalho, mas com a particularidade de permitir também uma tomada de decisão. A maioria dos seus parâmetros de configuração são semelhantes ao do módulo “Server”, no entanto na opção “Server Data” aparece uma janela com o nome “Failure Probability” que se destina a inserir a probabilidade de determinada decisão ser tomada, os valores a inserir terão que pertencer ao intervalo $[0,1]$.

Uma vez que as entidades poderão, função da decisão tomada, seguir caminhos distintos, existem neste módulo duas opções de encaminhamento, “Pass Inspection Leave Data” para as entidades que passem no critério de decisão e “Fail Inspection Leave Data” para as entidades que falhem no critério de decisão. Para efeitos de simulação é indiferente saber qual o critério de decisão, o importante é saber qual a probabilidade de uma determinada decisão ter de ser tomada. Ambas as opções de encaminhamento de entidades funcionam do mesmo modo que “Leave Data” do módulo “Server”.

Módulo “Depart” ou de Saída



Figura 44 – Módulo “Depart”

Uma vez arrastado este módulo para a área de animação, clicando sobre a palavra “Depart” fica disponível para alteração a caixa de dialogo deste módulo. Tal como a anterior divide-se em três áreas: “Enter Data”, “Count” e “Tally” (Figura 45).

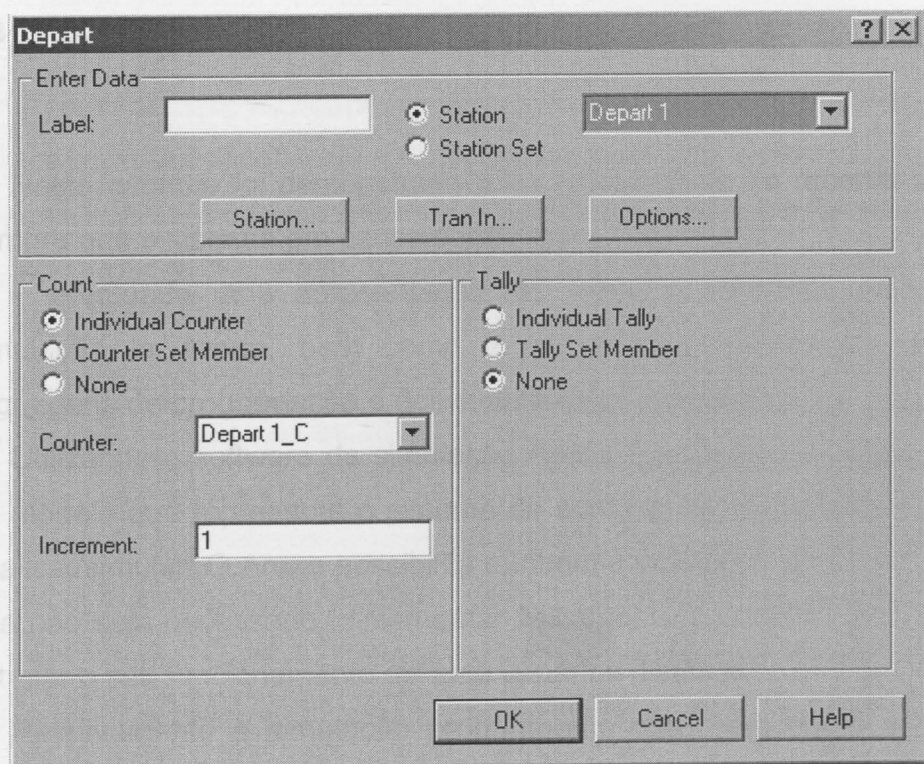


Figura 45 – Caixa de diálogo do módulo “Depart”

Na área “Enter Data” é colocado na caixa de escrita o nome que se pretende dar à estação.

Na área “Count”, que se destina a contar as entidades que saem do sistema, faz-se as seguintes alterações:

⇒ “pick” a opção “Individual Counter”, o que significa que se vai contar as entidades que saem do sistema. Por defeito este contador tem o nome “Depart 1 _C” e é incrementado uma unidade cada vez que uma entidade sai do sistema.

Na área “Tally”, que se destina a recolher os dados dos atributos das entidades assim que elas saem do sistema vai deixar-se com as características por defeito.

5.3 Conclusão

Neste capítulo foi demonstrada a necessidade de se recorrer à simulação sempre que o sistema em causa o justifique.

É efectuada uma apresentação do software escolhido para efectuar a simulação, o **Arena**, bem como o seu posicionamento no universo das linguagens de programação e dos simuladores existentes.

Utilizando o software de simulação Arena é possível proceder à simulação do modelo que representa o sistema de controlo de acessos que se pretende analisar/simular. O Arena possibilita também a validação do modelo de forma a que não seja necessário implementar fisicamente o sistema, afim de se poder estudar o seu funcionamento perante cenários distintos.

Relativamente à simulação propriamente dita, bem como os respectivos resultados obtidos através da simulação poderão ser visualizados no próximo capítulo.

Capítulo 6 – Funcionamento do Sistema de simulação

6.1 Introdução

Após efectuada a apresentação do software utilizado na simulação, o **Arena**, torna-se necessário modelar o Sistema de Controlo de Acessos para o ambiente de simulação.

Como foi dito no capítulo anterior, vai simular-se a entrada no estádio de futebol via torniquete, para tal torna-se necessário definir o modelo que represente o sistema em questão.

Independentemente do modelo de simulação em causa, a existência de filas de espera é uma realidade à qual nenhum modelo consegue eliminar por completo. Assim, neste capítulo vai efectuar-se uma breve análise às filas de espera e como estas estão directamente relacionadas com o desempenho do sistema de controlo de acessos.

Também se vai analisar a aplicação da simulação ao modelo que representa o sistema de controlo de acessos ao estádio (mais precisamente à entrada no estádio via torniquete) afim de se poder comparar os resultados obtidos na simulação com os valores teóricos previamente calculados.

6.2 Filas de espera

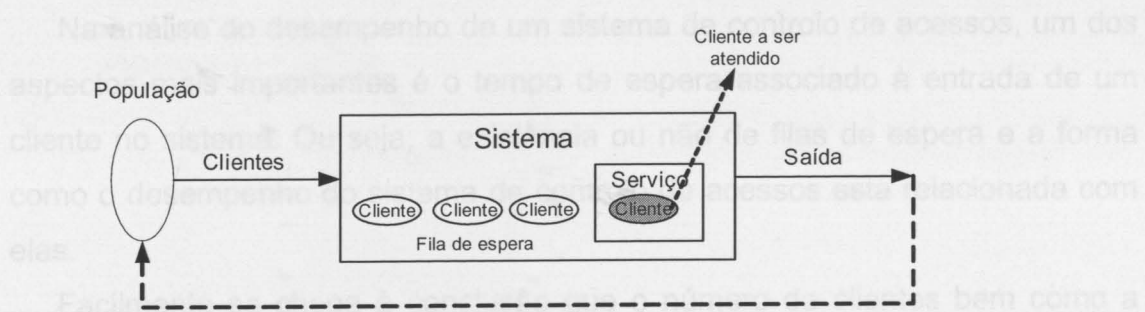


Figura 46 – Estrutura de um sistema de fila de espera

As filas de espera são uma realidade sempre que o número de clientes é superior ao número de servidores. Como o servidor demora algum tempo a atender cada cliente (tempo de serviço), em muitas situações os clientes vão encontrar o servidor ocupado e terão de aguardar em fila de espera (FIFO – “First In First Out”).

Algumas noções básicas:

- ⇒ Clientes – pessoas, veículos ou outras entidades físicas ou conceptuais que necessitam de um serviço, pelo qual podem ter de esperar numa fila física ou conceptual (a fila pode só existir conceptualmente, por exemplo senhas com números de atendimento).
- ⇒ Fonte ou população – gera os clientes que vão chegar ao sistema.
- ⇒ Fila – constituída pelos clientes que se encontram à espera de ser atendidos (não inclui o(s) cliente(s) em atendimento).
- ⇒ Serviço ou atendimento – pode ser constituído por um ou mais postos de atendimento.

Fila + Serviço = Sistema

Na análise do desempenho de um sistema de controlo de acessos, um dos aspectos mais importantes é o tempo de espera associado à entrada de um cliente no sistema. Ou seja, a existência ou não de filas de espera e a forma como o desempenho do sistema de controlo de acessos esta relacionada com elas.

Facilmente se chega à conclusão que o número de clientes bem como a quantidade de pontos de acessos existentes no sistema influenciam directamente o tempo de espera (a existência de filas de espera e seu comprimento) que o cliente tem que passar no sistema, isto é considerando o tempo de processamento da informação constante (não depende do número de clientes/serviços).

Idealmente, o sistema de controlo de acessos seria constituído por “n” pontos de acesso, sendo “n” o número de clientes que acedem ao sistema. Neste caso o desempenho seria 100%, ou seja não existiam filas de espera (todos os clientes eram atendidos mal chegassem ao sistema), o cliente apenas teria de esperar o tempo suficiente para que o sistema processasse a sua informação.

Obviamente, esta não é uma solução viável/lógica, uma vez ser impossível que um sistema de controlo de acessos possua tais requisitos /especificações.

Medidas de desempenho

Em sistemas constituídos por filas de espera, o desempenho do sistema pode ser expresso consoante os seguintes critérios/medidas:

- ⇒ Comprimento médio de fila (L_q)
- ⇒ Número médio de clientes no sistema (L)
- ⇒ Tempo médio de espera na fila (W_q)
- ⇒ Tempo médio de espera no sistema (W)
- ⇒ Taxa média de ocupação (e desocupação) do serviço (percentagem de tempo durante o qual o serviço está ocupado)

Nomenclatura

De forma a simplificar/abreviar, vai utilizar-se a seguinte nomenclatura:

$\Rightarrow \lambda$ – Taxa de chegada

$\Rightarrow \frac{1}{\lambda}$ – Intervalo médio entre duas chegadas consecutivas

$\Rightarrow \bar{\lambda} = \sum_{n=0}^{\infty} \lambda n P_n$ – Taxa média de entrada no sistema

$\Rightarrow \mu$ – Taxa de serviço (número médio de clientes que cada servidor tem capacidade para atender por unidade de tempo)

$\Rightarrow \frac{1}{\mu}$ – Tempo médio de serviço

$\Rightarrow s$ – Número de servidores

$\Rightarrow \rho$ – Taxa de ocupação

Caracterização das distribuições das chegadas e do atendimento

A maioria dos modelos analíticos de filas de espera supõe chegadas seguindo uma distribuição de Poisson e um tempo de atendimento caracterizado por uma distribuição exponencial negativa – distribuições que mais frequentemente caracterizam as filas de espera reais.

O sistema em questão, controlo de acessos a um estádio de futebol não é excepção.

Distribuição de Poisson

Função densidade de probabilidade de X:

$$f(x) = \frac{(\alpha)^x e^{-\alpha}}{x!} \quad x = 0, 1, 2, \dots$$

Parâmetro da distribuição de X:

α – número médio de acontecimentos por unidades de tempo;

t – comprimento do intervalo de tempo em análise;

x – número de acontecimentos durante o intervalo t.

Média: $E(X) = \alpha t$

Variância: $\text{Var}(X) = \alpha t$

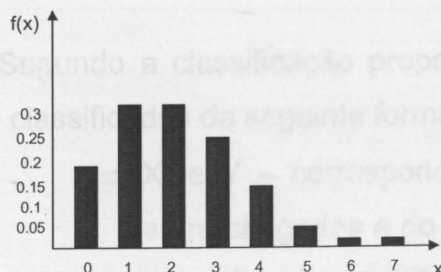


Figura 47 – Função densidade de probabilidade de uma variável com distribuição de Poisson

Distribuição exponencial negativa

Função densidade de probabilidade de T:

$$f(t) = \alpha e^{-\alpha t} \quad \text{se } t \geq 0 \quad \vee \quad 0 \quad \text{se } t < 0$$

$$\text{Média : } E(T) = \frac{1}{\alpha}$$

$$\text{Variância : } \text{Var}(T) = \frac{1}{\alpha^2}$$

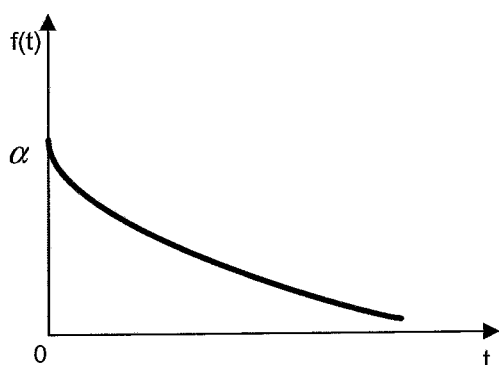


Figura 48 – Função densidade de probabilidade de uma variável com distribuição exponencial negativa

Classificação das filas de espera – X / Y / Z / A

Segundo a classificação proposta por Kendal para filas de espera, estas são classificadas da seguinte forma – X / Y / Z / W, onde:

- ⇒ X, e Y – correspondem às distribuições do intervalo de tempo entre chegadas e do tempo de serviço, respectivamente. Caso se trate de uma distribuição exponencial negativa ⇒ M; caso se trate de uma distribuição não especificada (qualquer distribuição) ⇒ G; caso se trate de chegadas ou atendimentos determinísticos ⇒ D.
- ⇒ Z – número de servidores em paralelo.
- ⇒ W – outras características do sistema, tais como comprimento da fila ilimitado ou população finita. Caso o modelo base não possua qualquer restrição adicional, ⇒ deixar em branco ou inserir o símbolo ∞ ; caso o comprimento da fila seja limitado, não podendo o número de elementos no sistema exceder K, ⇒ K; caso se trate de uma população finita ⇒ N.

Características do modelo M/M/1

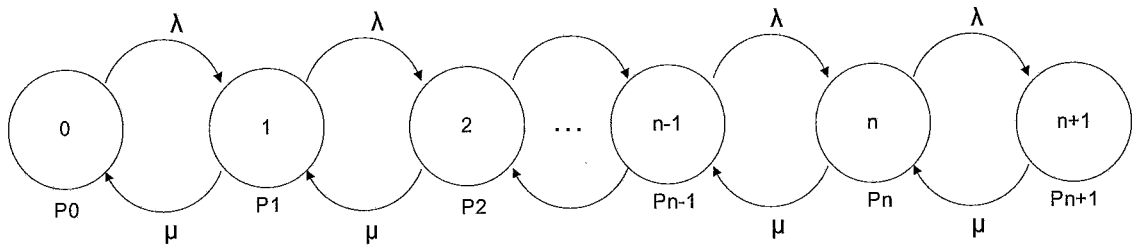


Figura 49 – modelo básico com um servidor – M/M/1

Considerar que o sistema de controlo de acessos corresponde ao modelo M/M/1.

Chegadas: Poissoniana

Taxa: λ clientes por unidade de tempo

População = ∞

Fila máxima = ∞

Tempo de atendimento: Exponencial negativo

Taxa: μ clientes por unidade de tempo e servidor

N.º de servidores = 1

$$\rho = \frac{\lambda}{\mu}, \text{ com } \rho < 1$$

Taxa de ocupação = ρ

Taxa de desocupação = $1 - \rho$

P_i = fracção de tempo em que o sistema se encontra no estado i .

Estado 0

N.º de entradas no estado 0 por unidade de tempo = μP_1

N.º de saídas do estado 0 por unidade de tempo = λP_0

$$\text{Equilíbrio} \Leftrightarrow \mu P_1 = \lambda P_0 \Leftrightarrow P_1 = \frac{\lambda}{\mu} P_0$$

Estado 1

$$N.^{\circ} \text{ de entradas} = \lambda P_0 + \mu P_2$$

$$N.^{\circ} \text{ de saídas} = \lambda P_1 + \mu P_1$$

$$\text{Equilíbrio} \Leftrightarrow \lambda P_0 + \mu P_2 = \lambda P_1 + \mu P_1 \Leftrightarrow P_2 = \frac{\lambda}{\mu} P_1 + \frac{1}{\mu} \Leftrightarrow P_2 = \frac{\lambda}{\mu} P_1 = \left(\frac{\lambda}{\mu}\right)^2 P_0$$

Estado n

$$P_n = \left(\frac{\lambda}{\mu}\right)^n P_0 \text{ onde } P_0 \text{ é obtido impondo a condição } \sum_{n=0}^{\infty} P_n = 1 \Leftrightarrow$$

$$\Leftrightarrow \sum_{n=0}^{\infty} \rho^n P_0 = 1 \Leftrightarrow \frac{1}{P_0} = \sum_{n=0}^{\infty} \rho^n, \text{ sendo este último somatório uma progressão}$$

geométrica de razão ρ , que será convergente se $\rho < 1$, sendo nesse caso a

soma dada por $\frac{1}{1-\rho}$:

$$\text{Então } \frac{1}{P_0} = \frac{1}{1-\rho} \Leftrightarrow P_0 = 1-\rho \text{ e } P_n = \rho^n (1-\rho)$$

Assim as características do modelo M/M/1:

$$L_q = \sum_{n=1}^{\infty} (n-1) P_n = \frac{\lambda^2}{\mu(\mu-\lambda)}$$

$$L = \sum_{n=0}^{\infty} n P_n = L_q + \frac{\lambda}{\mu} = \frac{\lambda}{\mu-\lambda}$$

$$W_q = \frac{L_q}{\lambda} = \frac{\lambda}{\mu(\mu-\lambda)}$$

$$W = W_q + \frac{1}{\mu} = \frac{L}{\lambda} = \frac{1}{\mu-\lambda}$$

Calculo teórico das características do sistema

De seguida vai calcular-se as principais características correspondentes às filas de espera do sistema de controlo de acessos ao estádio de futebol, ou seja o modelo analítico do sistema.

Os valores calculados utilizando as fórmulas acima demonstradas serão depois comparados com os resultados da simulação do modelo equivalente.

Definições e características do sistema:

A entrada no estádio, é efectuada por 63 torniquetes distribuídos por todo o estádio. Em média por cada torniquete passam 800 adeptos.

Vai calcular-se o número médio de adeptos na fila, o número médio de adeptos no sistema, o tempo médio de espera na fila e o tempo médio de espera no sistema. Para isso considera-se que os adeptos chegam à fila do respectivo torniquete segundo uma distribuição de Poisson com média de 7 adeptos por minuto. O tempo médio de atendimento (torniquete) de um cliente é de 5 segundos.

$$\lambda = 7 \text{ adeptos por minuto}$$

$$\mu = \frac{1}{5/60} = 12 \text{ adeptos por minuto}$$

$$Lq = \sum_{n=1}^{\infty} (n-1)Pn = \frac{\lambda^2}{\mu(\mu-\lambda)} = \frac{7^2}{12(12-7)} = 0.817 \text{ adeptos}$$

$$L = \sum_{n=0}^{\infty} nPn = Lq + \frac{\lambda}{\mu} = \frac{\lambda}{\mu-\lambda} = \frac{7}{12-7} = 1.4 \text{ adeptos}$$

$$Wq = \frac{Lq}{\lambda} = \frac{\lambda}{\mu(\mu-\lambda)} = \frac{7}{12(12-7)} = 0.117 \text{ minutos} \equiv 7 \text{ segundos}$$

$$W = Wq + \frac{1}{\mu} = \frac{L}{\lambda} = \frac{1}{\mu-\lambda} = \frac{1}{12-7} = 0.2 \text{ minutos} \equiv 12 \text{ segundos}$$

De seguida, vai recorrer-se à simulação de forma a se poder confirmar os resultados teóricos acima obtidos.

6.3 Simulação

Sistemas e Modelos

Em primeiro lugar convém diferenciar perfeitamente os conceitos de Modelo e Sistema.

Sistema será então todo e qualquer objecto (ou processo), ou conjunto de objectos, que actuam e interactuam com vista à concretização de alguma função e sobre o qual se pretende realizar um determinado estudo. Um seu Modelo será uma qualquer representação desse objecto no qual se irá executar tal estudo.

Tal como um Sistema, um seu Modelo terá também um conjunto de dados de entrada (“inputs”) controláveis e um conjunto de dados de saída (“outputs”) observáveis que resultam da transformação aplicada pelo processo em estudo. Variando os “inputs” e “outputs” em estudo obteremos modelos alternativos de um mesmo sistema.

Conceito de simulação

Simular é imitar o funcionamento de um processo ou sistema real durante um determinado tempo. Simular envolve a criação de um modelo artificial do sistema em estudo. Sobre este modelo serão então efectuadas diversas experiências do tipo “E se ...?” com vista a testar uma diversidade de hipóteses sem que para isso seja necessário afectar o sistema que de facto se pretende estudar. Simulando pode-se mesmo correr o risco de testar hipóteses

potencialmente arriscadas sem que daí surja qualquer problema já que não se está a agir sobre o sistema mas sim sobre um modelo deste.

Em alguns casos poderá ser possível executar experiências com o Sistema real, certamente com grandes vantagens, uma vez que nestes casos não é necessário preocupar-se com o facto de o Modelo ser ou não uma representação fiel do Sistema, já que este é estudado directamente. No entanto é necessário que estas experimentações não vão influenciar negativamente e permanentemente o Sistema.

Fases de realização de um projecto de simulação

Num processo de simulação há diversas fases que se deve considerar para que o projecto fique completo.

- ⇒ Formulação do problema – identificar o objectivo do projecto.
- ⇒ Estudo – levantamento de todas as características possíveis de funcionamento de determinado sistema.
- ⇒ Modelação – construção do Modelo que irá servir de base à experimentação. Reproduzindo as características de funcionamento consideradas importantes e definindo quais os dados que será interessante coleccionar e analisar.
- ⇒ Validação – verificar que o sistema se comporta como o sistema real, ou que pelo menos serve para tirar conclusões sobre ele. Um bom princípio é, para sistemas já existentes, comparar os resultados da simulação do modelo de base com os do próprio sistema.
- ⇒ Desenho de experiências – planeamento das experiências que vai ser necessário fazer sobre o modelo de acordo com o objectivo que se pretende atingir.
- ⇒ Simulação – correr as várias experiências planeadas, extrair e analisar os dados disponíveis. Nesta fase, e de acordo com os dados

que se vão obtendo, poderá ser necessário planear e executar novas experiências.

- ⇒ Apresentação de resultados – fase de projecto essencial à venda do mesmo.
- ⇒ Implementação – esta fase é crucial para a credibilidade do projecto já que uma implementação deficiente pode falsear todo um projecto.

Vantagens da simulação

- ⇒ Um modelo de simulação é executado enquanto um modelo analítico é resolvido. A visibilidade do que se passa no modelo de simulação é maior do que no modelo analítico.
- ⇒ Novas operações, métodos de trabalho, novas sequências de operações podem ser experimentados sem prejudicar a operação normal do sistema real.
- ⇒ O tempo de simulação pode ser mais rápido ou mais lento que o tempo real de modo a que se possa concentrar o estudo no fenómeno que interessa.
- ⇒ Podem ser analisadas as operações de estrangulamento de modo a determinar qual das suas fases é responsável pelos atrasos;
- ⇒ Pode auxiliar a determinar como um sistema se comporta de facto em oposição ao modo como toda a gente acredita que ele se comporta;
- ⇒ Uma vez criado, um modelo pode ser utilizado inúmeras vezes para avaliar projectos e políticas propostos;
- ⇒ Hipóteses sobre como ou por quê certos fenómenos acontecem podem ser testadas para confirmação;
- ⇒ Podem-se compreender melhor quais variáveis são as mais importantes em relação à performance e como as mesmas interagem entre si e com os outros elementos dos sistemas;

- ⇒ Um estudo de simulação costuma mostrar como realmente um sistema opera, em oposição à maneira com que todos pensam que ele opera;
- ⇒ Novas situações sobre as quais se tenha pouco conhecimento e experiência podem ser tratadas, de tal forma que se possa ter, teoricamente, alguma preparação diante de futuros eventos.

Desvantagens da simulação

- ⇒ A construção de modelos requer treino especial e experiência. Dois modelos construídos por analistas diferentes, mas com igual competência, podem ter pontos comuns mas vão certamente ter também muitas diferenças.
- ⇒ Os resultados de uma simulação podem ser por vezes difíceis de serem interpretados.
- ⇒ Os modelos de simulação podem consumir bastantes recursos. Ignorando alguns recursos necessários pode-se estar a comprometer a validade dos resultados obtidos.

Conclusão

No caso concreto de um sistema de controlo de acessos a um estádio de futebol é-se obrigado a recorrer à simulação, uma vez não ser possível dispor de um sistema real onde se possa testar hipóteses de funcionamento distintas (sem por em perigo o funcionamento normal do sistema).

Assim é criado um modelo que represente o sistema de controlo de acessos de um estádio de futebol, mais concretamente um modelo que simule a entrada no estádio, constituído por um torniquete e o respectivo tempo de serviço.

6.4 Cálculo das características do sistema recorrendo à simulação

Como já foi mencionado no início deste capítulo, o software utilizado para efectuar a simulação foi o **Arena**.

A Figura 50 representa o modelo que se pretende que simule a fila de espera correspondente à entrada no estádio, através de um torniquete.

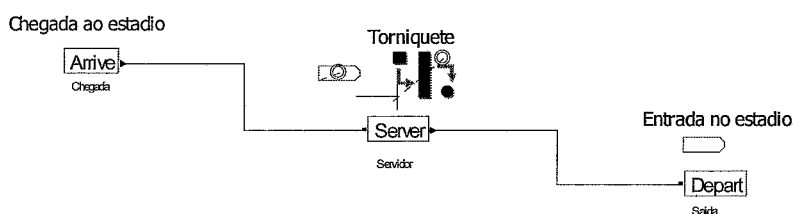


Figura 50 – Modelo do sistema

Como se pode observar no modelo acima (Figura 50), este é constituído por três módulos que representam as três principais etapas que envolvem o sistema de controlo de acessos, mais precisamente da entrada no estádio de futebol.

Está-se a falar da chegada ao estádio, no modelo de simulação representada pelo módulo “Arrive”, torniquete ou validação representada pelo módulo “Server” e finalmente a entrada no estádio representada através do módulo “Depart”.

O módulo “Arrive” (Figura 51), bem como os restantes módulos são preenchidos com os resultados obtidos no cálculo teórico das características do sistema.



Figura 51 – Módulo "Arrive"

Assim para o módulo "Arrive", a informação necessária retirada do ponto 0 é a distribuição das chegadas (Poisson) e a respectiva taxa de chegada ($\lambda = 7$ adeptos por minuto), mais precisamente o intervalo médio entre duas chegadas consecutivas ($\frac{1}{\lambda} = \frac{1}{7} = 0,142857$ minutos) uma vez que o campo correspondente à distribuição da chegada é "Time Between", o que corresponde ao intervalo médio entre duas chegadas.

Os restantes campos possíveis de serem preenchidos, apenas se vai preencher o campo "Batch Size" com um valor unitário. Este campo corresponde ao número de adeptos que se pretende que cheguem ao sistema de uma vez (chegadas individuais ou em grupos de "n" adeptos).

Assim, o módulo "Arrive", devidamente preenchido encontra-se na Figura 52.

Arrive [?] [X]

Enter Data

☒ Station **Arrive 1** [v]
☐ Station Set

[Station...] [Options...]

Arrival Data

Batch Size:
First Creation:
Time Between: **POIS(0.142857)** [v]
Max Batches:
Mark Time Attribute: [v]

[Assign...] [Animate...]

Leave Data

[Tran Out...] [Count...]

☐ Route
☒ Connect

Next Label:

[OK] [Cancel] [Help]

Figura 52 – Preenchimento do módulo "Arrive"

O segundo módulo, correspondente ao tempo de atendimento do serviço, ou seja, o tempo que o torniquete demora a validar um adepto pode ser visualizado na Figura 53.

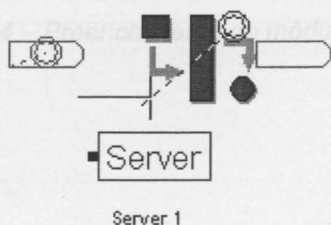


Figura 53 – Módulo "Server"

Do ponto 0 é retirada a informação referente ao tempo médio de atendimento de um cliente ($\mu = \frac{1}{\frac{5}{60}} = 12$ adeptos por minuto).

Contudo o campo a preencher no módulo “Server”, “Process Time”, corresponde ao tempo médio de serviço $\frac{1}{\mu} = \frac{1}{12} = 0,083333$ e segue uma distribuição exponencial.

Dos restantes campos possíveis de serem preenchidos apenas vai-se preencher o campo “Capacity”, o qual representa a capacidade que o serviço/torniquete apresenta, com um valor unitário.

O módulo “Server”, devidamente preenchido encontra-se na Figura 54.

The image shows a screenshot of the "Server" dialog box in the Arena simulation software. The dialog is divided into several sections:

- Enter Data:** Contains a "Label" text box (empty) and a "Station" dropdown menu (set to "Servidor"). There is a "Tran In..." button.
- Server Data:** Contains a "Resource" dropdown menu (set to "Servidor_R"), a "Capacity Type" dropdown menu (set to "Capacity"), a "Capacity" text box (set to "1"), a "Process Time" dropdown menu (set to "EXP0[0.083333]"), and a checked "Resource Statistics" checkbox. Below these are buttons for "Options...", "Resource...", "Queue...", and "Animate...".
- Leave Data:** Contains a "Tran Out..." button, a "Count..." button, radio buttons for "Route" (selected) and "Connect", and a "Next Label" text box (empty).
- Bottom:** Contains "OK", "Cancel", and "Help" buttons.

Figura 54 – Preenchimento do módulo “Server”

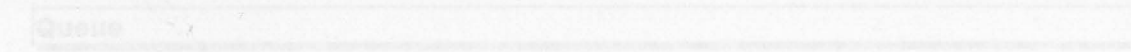
O último módulo a ser implementado é a entrada no estádio, ou seja a saída do sistema de controlo de acessos.

O módulo do Arena que representa a saída do sistema pode ser visualizado na Figura 55.

Após a simulação ter terminado, obteve-se o seguinte valor para o tempo médio de espera na fila $L_q = 0,1158 = 6,95 \text{ segundos}$ (Figura 57).



Figura 55 – Módulo "Depart"



No módulo “Depart” não há necessidade de preencher qualquer campo, uma vez que não requer qualquer tipo de informação. A sua função é apenas dar saída das entidades/adeptos do sistema.

A captura de tela mostra a janela de configuração do módulo "Depart". A janela tem o título "Depart" e contém as seguintes opções:

- Enter Data:**
 - Label: Campo de texto vazio.
 - ☒ Station: Selecionado.
 - ☐ Station Set.
 - Dropdown menu: "Depart 1".
 - Buttons: "Station...", "Tran In...", "Options..."
- Count:**
 - ☐ Individual Counter.
 - ☐ Counter Set Member.
 - ☒ None.
- Tally:**
 - ☐ Individual Tally.
 - ☐ Tally Set Member.
 - ☒ None.
- Buttons:** "OK", "Cancel", "Help".

Figura 56 – Preenchimento do módulo "Depart"

Figura 56 – Evolução do tempo médio de espera na fila

Agora que o modelo já esta definido e devidamente parametrizado, pode-se proceder à simulação propriamente dita.

Assim e após a simulação ter terminado, obteve-se o seguinte valor para o tempo médio de espera na fila $L_q = 0,1158 \equiv 6,95 segundos$ (Figura 57).

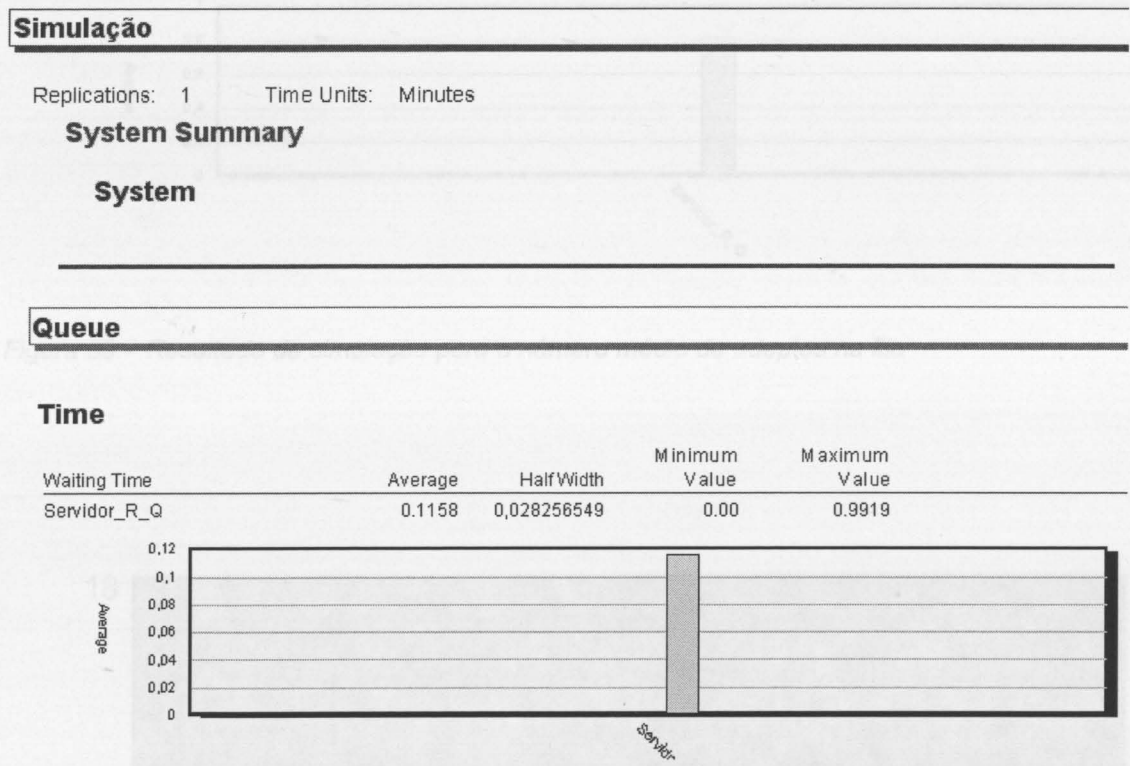


Figura 57 – Resultado da simulação para o tempo médio de espera na Fila

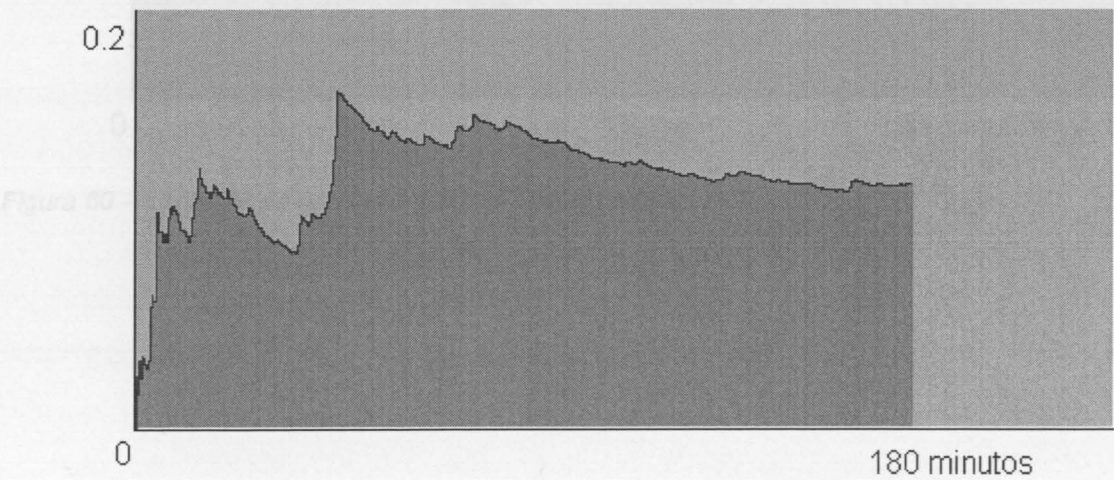


Figura 58 – Evolução do tempo médio de espera na fila

6.5 Em relação ao número médio de adeptos na fila Wq, o valor obtido através da simulação foi de $Wq = 0,8131$

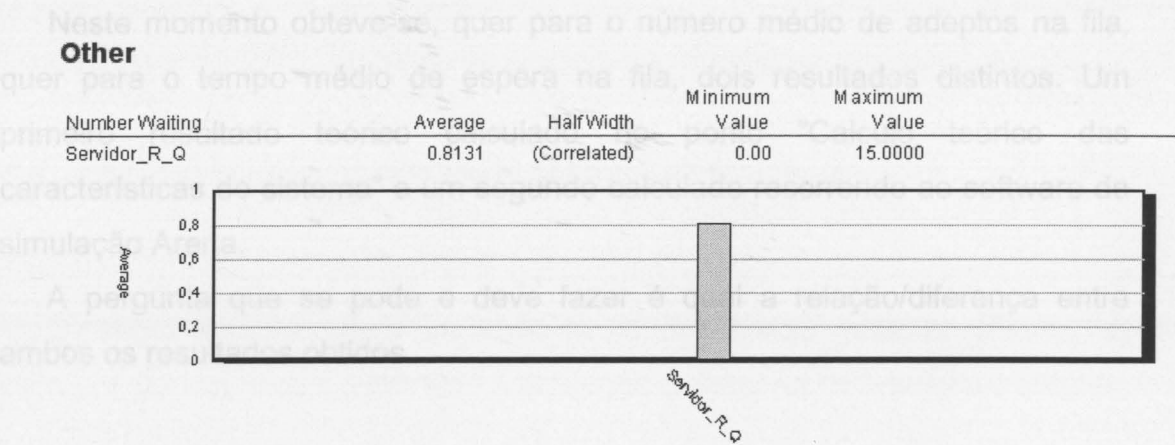


Figura 59 – Resultado da simulação para o número médio de adeptos na fila

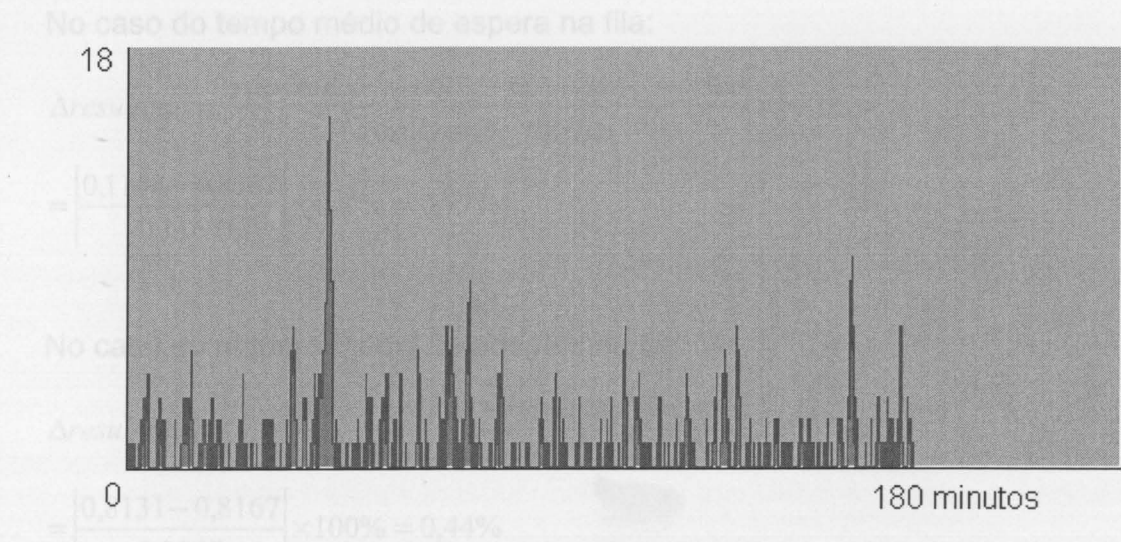


Figura 60 – Evolução do número médio de adeptos na fila

Nos dois casos, pode-se concluir que os resultados obtidos teoricamente e recorrendo à simulação são praticamente idênticos, uma vez que diferença entre ambos não chega a 1%.

Pode-se também concluir que o modelo criado no Arena se encontra de acordo com as especificações do sistema descrito (real), ou seja o modelo

6.5 Análise dos resultados obtidos

Neste momento obteve-se, quer para o número médio de adeptos na fila, quer para o tempo médio de espera na fila, dois resultados distintos. Um primeiro resultado teórico calculado no ponto “Calculo teórico das características do sistema” e um segundo calculado recorrendo ao software de simulação Arena.

A pergunta que se pode e deve fazer é qual a relação/diferença entre ambos os resultados obtidos.

Assim, e partindo do princípio que o resultado teórico obtido se encontra correcto, vai calcular-se $\Delta resultado$ ou seja a diferença entre ambos (em percentagem).

No caso do tempo médio de espera na fila:

$$\begin{aligned}\Delta resultado &= \left| \frac{\text{resultado}_{\text{prático}} - \text{resultado}_{\text{teórico}}}{\text{resultado}_{\text{teórico}}} \right| \times 100\% = \\ &= \left| \frac{0,1158 - 0,1167}{0,1167} \right| \times 100\% = 0,77\%\end{aligned}$$

No caso do número médio de adeptos na fila:

$$\begin{aligned}\Delta resultado &= \left| \frac{\text{resultado}_{\text{prático}} - \text{resultado}_{\text{teórico}}}{\text{resultado}_{\text{teórico}}} \right| \times 100\% = \\ &= \left| \frac{0,8131 - 0,8167}{0,8167} \right| \times 100\% = 0,44\%\end{aligned}$$

Nos dois casos, pode-se concluir que os resultados obtidos teoricamente e recorrendo à simulação são praticamente idênticos, uma vez que diferença entre ambos não chega a 1%.

Pode-se também concluir que o modelo criado no Arena se encontra de acordo com as especificações do sistema descrito (real), ou seja o modelo

criado corresponde ao sistema de controlo de acessos e o software utilizado é adequado para proceder simulação desejada.

Figura 62 – Módulo "Inspect"

6.6 Análise de um modelo mais próximo da realidade

De seguida vai alterar-se o modelo de simulação apresentado na Figura 50, para um modelo mais aproximado à realidade e observar os resultados obtidos.

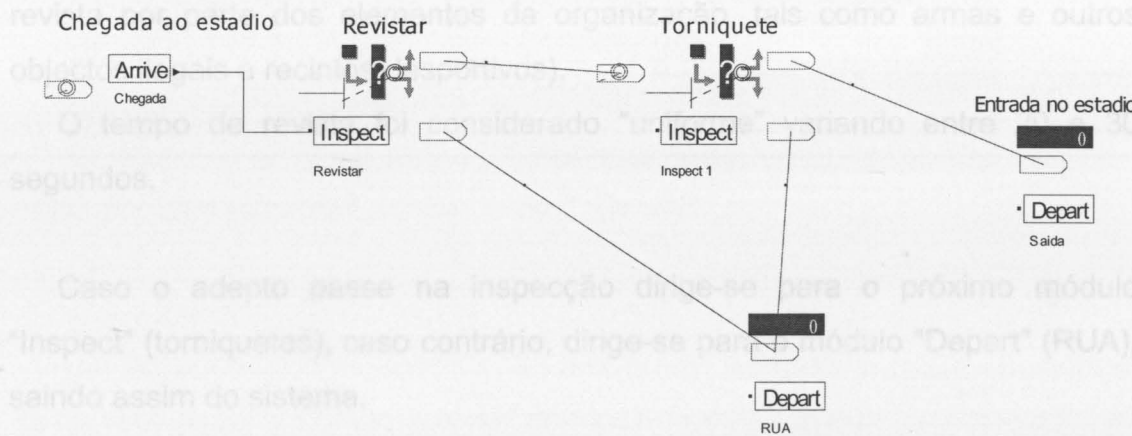


Figura 61 – Modelo mais próximo da realidade

O novo modelo é constituído por cinco módulos, dois quais apenas dois se mantêm idênticos ao modelo anterior. Estes são os módulos "Arrive" e "Depart" (Saída), uma vez que a distribuição da chegada ao estádio se mantém inalterada face ao modelo anterior.

Foi adicionado um módulo "Inspect" que representa o revistar dos adeptos por parte da organização, Figura 62.

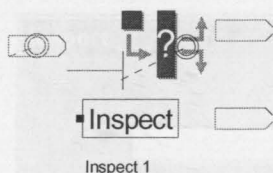


Figura 62 – Módulo "Inspect"

Como se pode observar na Figura 63, o módulo "Inspect" origina duas saídas possíveis, "Pass Inspection Leave Data" e "Fail Inspection Leave Data".

O critério de escolha, entre as duas depende da taxa de probabilidade de falha colocada em "Failure Probability". Neste caso particular foi colocada uma taxa de falha/insucesso de 10%, a qual representa a taxa de adeptos que têm o acesso negado no acto de revista (detecção de irregularidades no acto de revista por parte dos elementos da organização, tais como armas e outros objectos ilegais a recintos desportivos).

O tempo de revista foi considerado "uniforme" variando entre 20 e 30 segundos.

Figura 63 – Preenchimento do módulo "Inspect" (Revistar)

Caso o adepto passe na inspecção dirige-se para o próximo módulo "Inspect" (torniquetes), caso contrário, dirige-se para o módulo "Depart" (RUA), saindo assim do sistema.

Este módulo representa o tempo de atendimento do serviço, ou seja, o tempo que o torniquete demora a validar um adepto. A diferença face ao módulo "Server" é a possibilidade de definir uma taxa de falha/insucesso. Neste caso foi considerada com um valor de 10%, ou seja 10% dos adeptos vêem o acesso negado na fase de validação dos ingressos (ingressos válidos para outros sectores do estádio ou mesmo ingressos falsos).

Caso o acesso seja validado, o adepto entra no estádio através do módulo "Depart" (Saída), caso contrário dirige-se para o módulo "Depart" (RUA), saindo assim do sistema.

Na Figura 64 pode-se visualizar o preenchimento do módulo "Inspect" (Torniquete).

Inspect

Enter Data
 Label: Station: **Revistar**

Server Data
 Resource: **Revistar_R**
 Capacity Type: **Capacity**
 Capacity: **1**
☒ Resource Statistics
 Process Time: **UNIF[0.2 ,0.5]**
 Failure Probability: **0.1**

Pass Inspection Leave Data

☒ Route ☒ StNm ☐ Seq ☐ Expr
☐ Connect
 Station: **Inspect 1**
 Route Time: **0.**

Fail Inspection Leave Data

☒ Route ☒ StNm ☐ Expr
☐ Connect
 Station: **RUA**
 Route Time: **0.**

Figura 63 – Preenchimento do módulo "Inspect" (Revistar)

Um segundo módulo "Inspect" foi adicionado ao modelo (pode considerar-se que substituiu o módulo "Server" do modelo da Figura 50).

Este módulo representa o tempo de atendimento do serviço, ou seja, o tempo que o torniquete demora a validar um adepto. A diferença face ao módulo "Server" é a possibilidade de definir uma taxa de falha/insucesso. Neste caso foi considerada com um valor de 10%, ou seja 10% dos adeptos vêem o acesso negado na fase de validação dos ingressos (ingressos validos para outros sectores do estádio ou mesmo ingressos falsos).

Caso o acesso seja validade, o adepto entra no estádio através do módulo "Depart" (Saída), caso contrário dirige-se para o módulo "Depart" (RUA), saindo assim do sistema.

Na Figura 64 pode-se visualizar o preenchimento do módulo "Inspect" (Torniquete).

Figura 64 – Preenchimento do módulo "Inspect" (Torniquete)

O último módulo a adicionar ao modelo foi o módulo "Depart" (RUA), o qual representa a saída do sistema dos adeptos que tiveram o acesso negado em alguma das duas fases de controlo/inspecção.

Figura 66 – Evolução do tempo médio de espera na fila "Inspect"1

Análise dos resultados obtidos

Agora que o modelo já está definido e devidamente parametrizado, pode proceder-se à simulação propriamente dita.

Os resultados obtidos para o número médio de adeptos na fila e para o tempo médio de espera na fila encontram-se na Figura 65.

Replication 1

Start Time: 0,00

Stop Time: 351,56

Time Units: Minutes

Queue

Waiting Time	Average	Half Width	Minimum	Maximum
Inspect 1_R_Q	0.00115028	(Correlated)	0	0.2240
Revistar_R_Q	104.59	(Correlated)	0	212.15

Number Waiting	Average	Half Width	Minimum	Maximum
Inspect 1_R_Q	0.00292837	(Insufficient)	0	2.0000
Revistar_R_Q	297.49	(Correlated)	0	604.00

Figura 65 – Resultados Lq e Wq

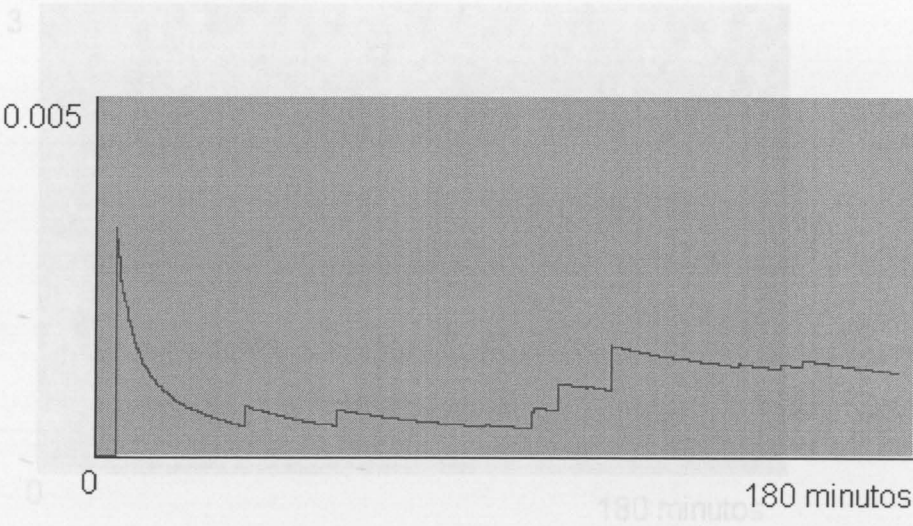


Figura 66 – Evolução do tempo médio de espera na fila “Inspect”1

Figura 69 – Evolução do número médio de adeptos na fila “Inspect” 1

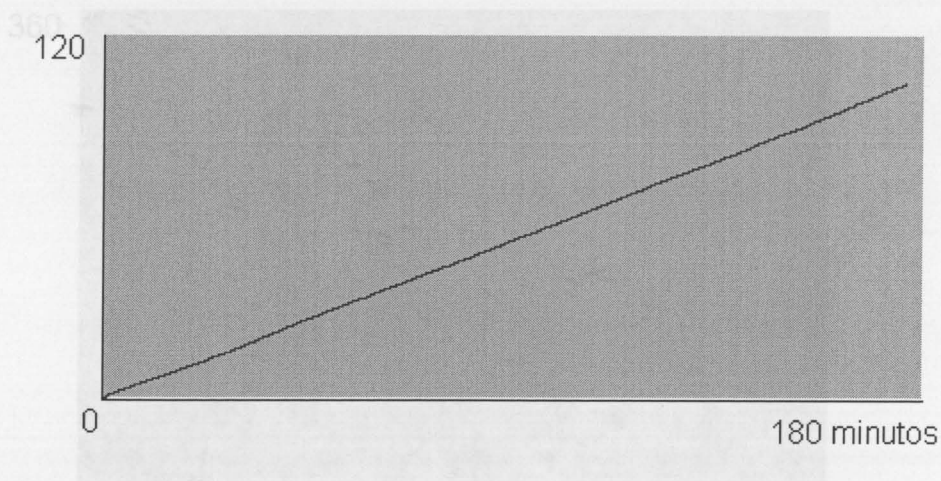


Figura 67 – Evolução do tempo médio de espera na fila Revistar

Figura 68 – Evolução do número médio de adeptos na fila Revistar

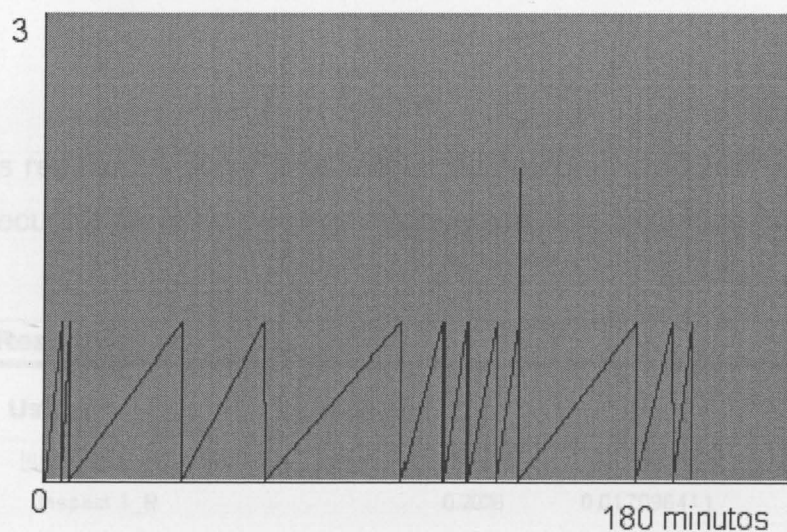


Figura 68 – Evolução do número médio de adeptos na fila "Inspect" 1

	Average	Half Width	Minimum	Maximum
Inspect 1_R	0.2000	0.000000000	0	1.0000
Revistar_R	0.9999	0.000000000	0	1.0000
Number Served	Average	Half Width	Minimum	Maximum
Inspect 1_R	1.0000	(Insufficient)	1.0000	1.0000
Revistar_R	1.0000	(Insufficient)	1.0000	1.0000
Scheduled Utilization	Value			
Inspect 1_R	0.2000			
Revistar_R	0.9999			
Total Number Seized	Value			
Inspect 1_R	1.0000			
Revistar_R	1.0000			

Figura 70 – Resultados taxa de ocupação

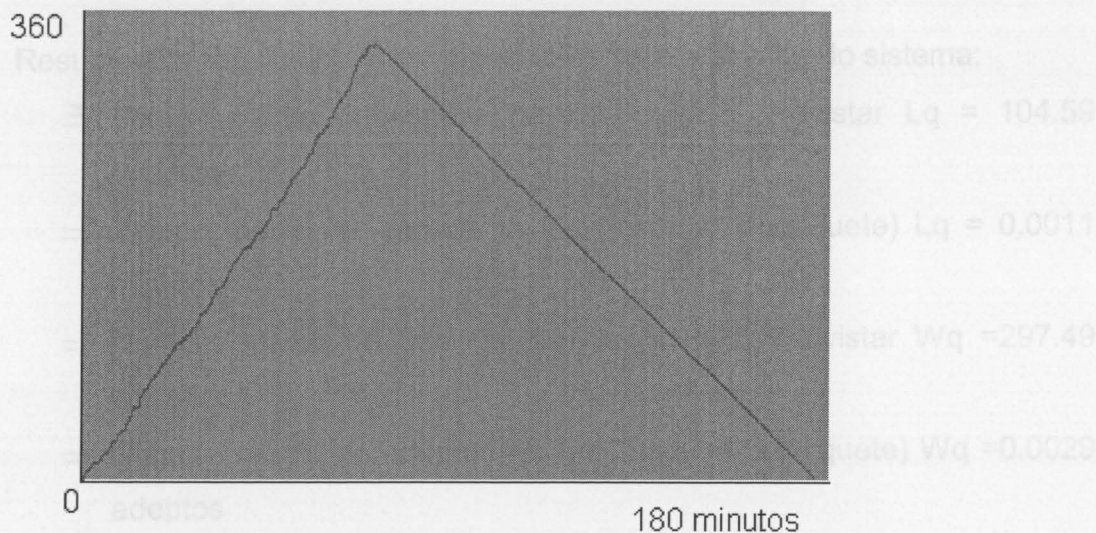


Figura 69 – Evolução do número médio de adeptos na fila Revistar

Os resultados sobre a utilização dos recursos, ou seja a taxa de ocupação dos recursos (revistar adeptos e torniquete) encontram-se na Figura 70.

Resource				
Usage				
Instantaneous Utilization	Average	Half Width	Minimum	Maximum
Inspect 1_R	0.2026	0,017096411	0	1.0000
Revistar_R	0.9999	0,000000000	0	1.0000
Number Busy	Average	Half Width	Minimum	Maximum
Inspect 1_R	0.2026	0,017096411	0	1.0000
Revistar_R	0.9999	0,000000000	0	1.0000
Number Scheduled	Average	Half Width	Minimum	Maximum
Inspect 1_R	1.0000	(Insufficient)	1.0000	1.0000
Revistar_R	1.0000	(Insufficient)	1.0000	1.0000
Scheduled Utilization	Value			
Inspect 1_R	0.2026			
Revistar_R	0.9999			
Total Number Seized	Value			
Inspect 1_R	895.00			
Revistar_R	1,000.00			

Figura 70 – Resultados taxa de ocupação

Resumo dos resultados mais importantes para a análise do sistema:

- ⇒ Tempo médio de espera na fila “Inspect” Revistar $L_q = 104.59$ minutos
- ⇒ Tempo médio de espera na fila “Inspect” (torniquete) $L_q = 0.0011$ minutos
- ⇒ Número médio de adeptos na fila “Inspect” Revistar $W_q = 297.49$ adeptos
- ⇒ Número médio de adeptos na fila “Inspect” (torniquete) $W_q = 0.0029$ adeptos
- ⇒ Taxa de ocupação do recurso “Inspect” Revistar $= 99.99\% \cong 100\%$
- ⇒ Taxa de ocupação do recurso “Inspect” (torniquete) $= 20.26\%$
- ⇒ Número de adeptos revistados = 1000, numa amostra de 1000
- ⇒ Número de adeptos validados pelo torniquete = 895

Como se pode observar, o problema do modelo encontra-se no módulo “Inspect” (Revistar), uma vez que a taxa de ocupação se encontra nos 100% (completamente saturado).

O tempo de espera médio na fila ultrapassa os 100 minutos, o que leva a que o número médio de adeptos na fila de espera (297 adeptos) seja muito elevado, impensável numa situação real.

Em relação ao módulo “Inspect” (torniquete), a taxa de ocupação situa-se nos 20%, o que se pode considerar um valor baixo para o tipo de equipamento.

O tempo médio de espera na fila e o número médio de adeptos na fila são praticamente nulos, o que demonstra mais uma vez o bom rendimento/desempenho do equipamento.

Uma solução possível é aumentar o número de módulos “Inspect” (Revistar), uma vez não se poder diminuir o tempo de revista.

Na realidade encontram-se vários (cerca de 3 ou 4) elementos – dependendo do jogo e da secção do estádio – da organização cuja função é revistar os adeptos antes de se dirigirem para o respectivo torniquete.

Assim, o modelo correspondente a ter-se três módulos “Inspect” (Revistar) encontra-se na Figura 71.

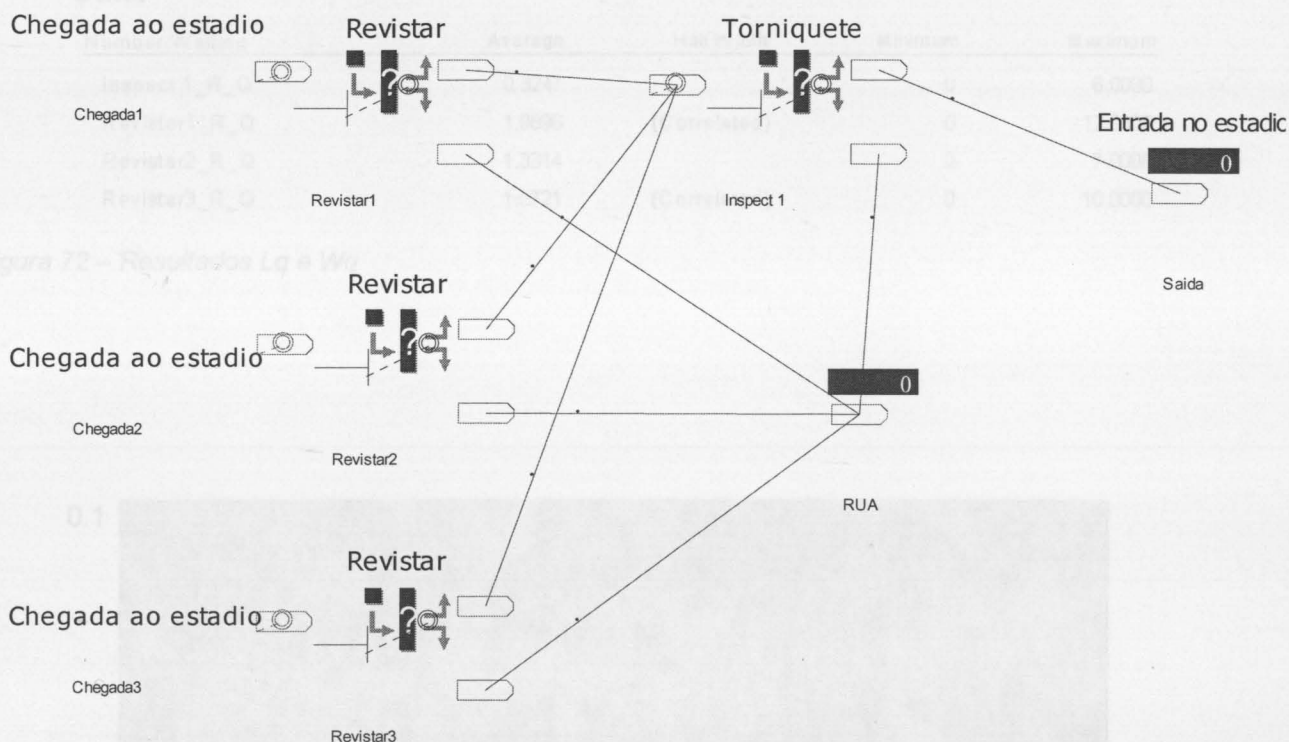


Figura 71 – Modelo com três módulos “Inspect” (Revistar)

Os resultados obtidos para o número médio de adeptos na fila e para o tempo médio de espera na fila encontram-se na Figura 72.

Queue

Time

Waiting Time	Average	Half Width	Minimum	Maximum
Inspect 1_R_Q	0.05169290	0,016210719	0	0.6225
Revistar1_R_Q	0.8608	(Correlated)	0	3.9540
Revistar2_R_Q	0.5760		0	2.0831
Revistar3_R_Q	0.6801	(Correlated)	0	3.4735

Other

Number Waiting	Average	Half Width	Minimum	Maximum
Inspect 1_R_Q	0.3247		0	6.0000
Revistar1_R_Q	1.9896	(Correlated)	0	12.0000
Revistar2_R_Q	1.3314		0	7.0000
Revistar3_R_Q	1.5721	(Correlated)	0	10.0000

Figura 72 – Resultados Lq e Wq

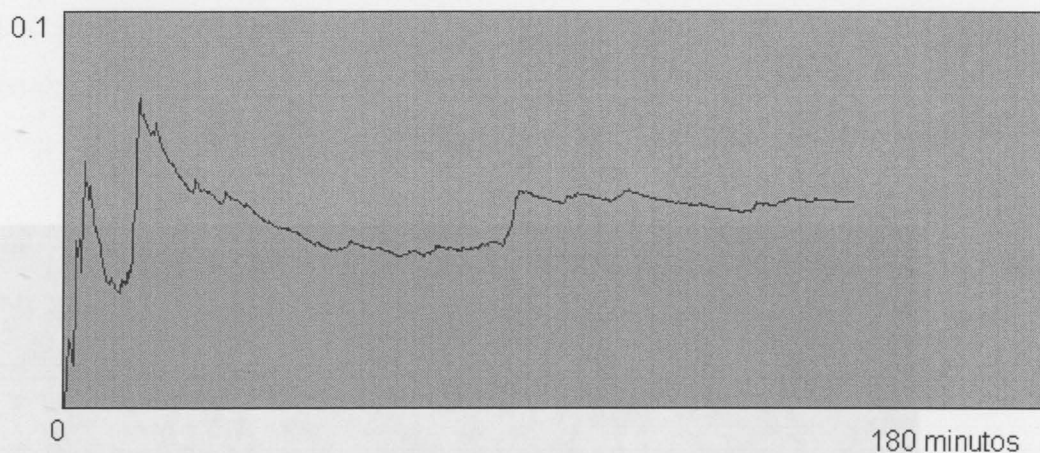


Figura 73 – Evolução do tempo médio de espera na fila "Inspect" 1

Figura 75 – Evolução do número médio de adeptos na fila "Inspect" 1

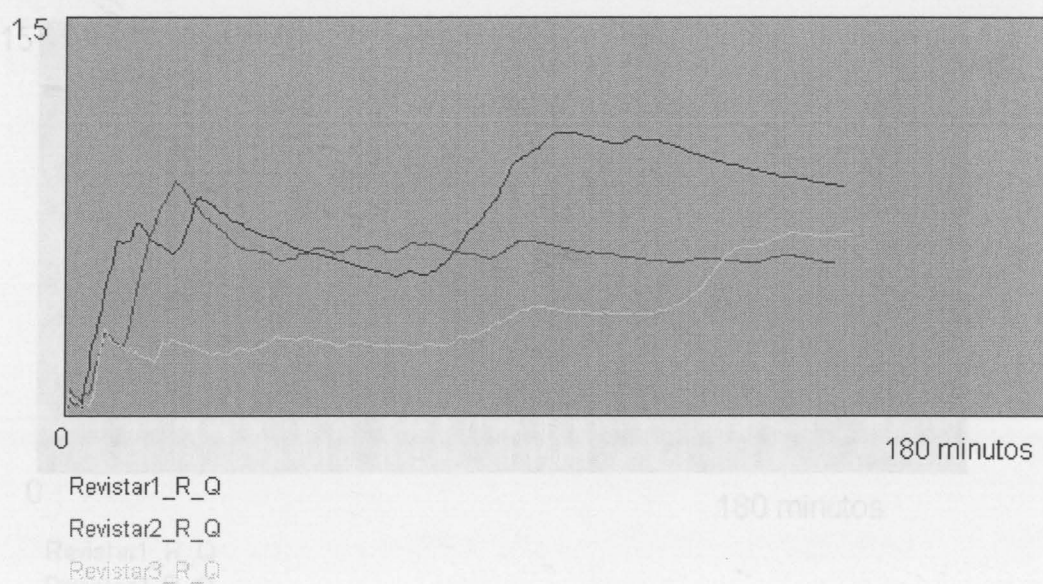


Figura 74 – Evolução do tempo médio de espera nas filas Revistar

Figura 75 – Evolução do número médio de adeptos nas filas Revistar

Os resultados sobre a utilização dos recursos, ou seja a taxa de ocupação dos recursos (revistar adeptos e tomiquete) encontram-se na Figura 77.

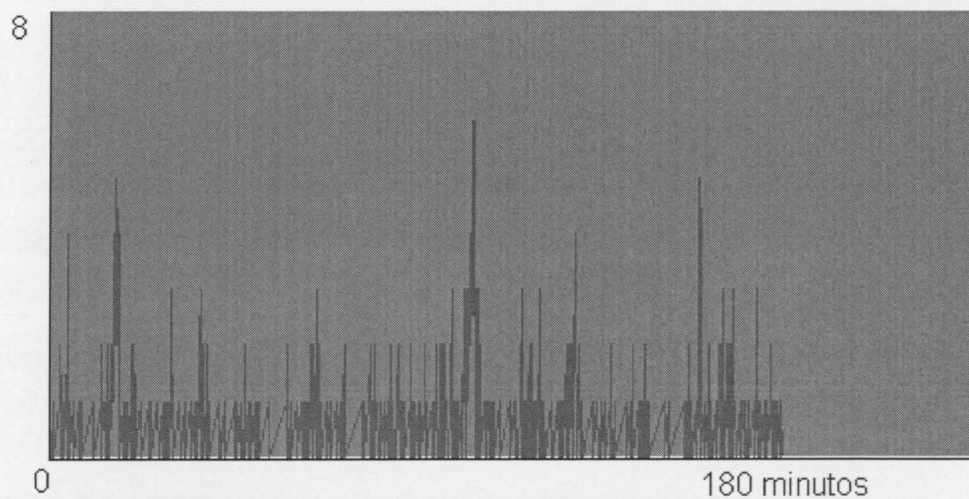


Figura 75 – Evolução do número médio de adeptos na fila "Inspect" 1

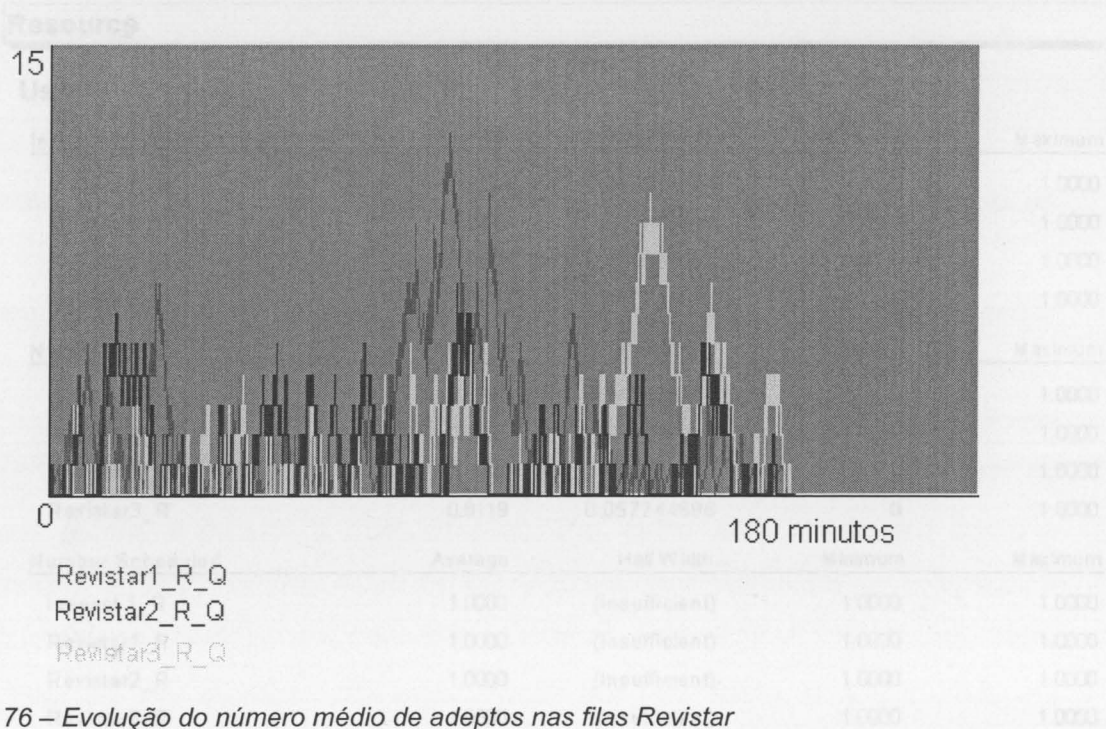


Figura 76 – Evolução do número médio de adeptos nas filas Revistar

Figura 77 – Resultados taxa de ocupação

Os resultados sobre a utilização dos recursos, ou seja a taxa de ocupação dos recursos (revistar adeptos e torniquete) encontram-se na Figura 77.

- ⇒ Tempo médio de espera na fila Revistar2 Lq = 0.576 minutos
- ⇒ Tempo médio de espera na fila Revistar3 Lq = 0.6801 minutos
- ⇒ Tempo médio de espera na fila "Inspect" (torniquete) Lq = 0.0517 minutos
- ⇒ Número médio de adeptos na fila Revistar1 Wq = 1.9896 adeptos
- ⇒ Número médio de adeptos na fila Revistar2 Wq = 1.3314 adeptos
- ⇒ Número médio de adeptos na fila Revistar3 Wq = 1.5721 adeptos
- ⇒ Número médio de adeptos na fila "Inspect" (torniquete) Wq = 0.3247 adeptos
- ⇒ Taxa de ocupação do recurso Revistar1 = 80.63%
- ⇒ Taxa de ocupação do recurso Revistar2 = 80.17%
- ⇒ Taxa de ocupação do recurso Revistar3 = 81.19%
- ⇒ Taxa de ocupação do recurso "Inspect" (torniquete) = 52.53%

Resource

Usage

Instantaneous Utilization	Average	Half Width	Minimum	Maximum
Inspect 1_R	0.5253	0,045618754	0	1.0000
Revistar1_R	0.8063	(Correlated)	0	1.0000
Revistar2_R	0.8017	0,076861253	0	1.0000
Revistar3_R	0.8119	0,057744696	0	1.0000
Number Busy	Average	Half Width	Minimum	Maximum
Inspect 1_R	0.5253	0,045618754	0	1.0000
Revistar1_R	0.8063	(Correlated)	0	1.0000
Revistar2_R	0.8017	0,076861253	0	1.0000
Revistar3_R	0.8119	0,057744696	0	1.0000
Number Scheduled	Average	Half Width	Minimum	Maximum
Inspect 1_R	1.0000	(Insufficient)	1.0000	1.0000
Revistar1_R	1.0000	(Insufficient)	1.0000	1.0000
Revistar2_R	1.0000	(Insufficient)	1.0000	1.0000
Revistar3_R	1.0000	(Insufficient)	1.0000	1.0000

Figura 77 – Resultados taxa de ocupação

Resumo dos resultados mais importantes para a análise do sistema:

- ⇒ Tempo médio de espera na fila Revistar1 $L_q = 0.8608$ minutos
- ⇒ Tempo médio de espera na fila Revistar2 $L_q = 0.576$ minutos
- ⇒ Tempo médio de espera na fila Revistar3 $L_q = 0.6801$ minutos
- ⇒ Tempo médio de espera na fila "Inspect" (torniquete) $L_q = 0.0517$ minutos
- ⇒ Número médio de adeptos na fila Revistar1 $W_q = 1.9896$ adeptos
- ⇒ Número médio de adeptos na fila Revistar2 $W_q = 1.3314$ adeptos
- ⇒ Número médio de adeptos na fila Revistar3 $W_q = 1.5721$ adeptos
- ⇒ Número médio de adeptos na fila "Inspect" (torniquete) $W_q = 0.3247$ adeptos
- ⇒ Taxa de ocupação do recurso Revistar1 = 80.63%
- ⇒ Taxa de ocupação do recurso Revistar2 = 80.17%
- ⇒ Taxa de ocupação do recurso Revistar3 = 81.19%
- ⇒ Taxa de ocupação do recurso "Inspect" (torniquete) = 52.53%

Conclusão

Como era de esperar com o aumento do número de módulos “Inspect” Revistar, quer o número médio de adeptos na fila quer o tempo médio de espera na fila diminuem drasticamente.

Das taxas de ocupação dos recursos Revistar, pode-se concluir que apesar de apresentarem valores elevados, cerca de 80%, não se justifica o aumento do número de módulos “Inspect” Revistar uma vez que quer o tempo médio de espera dos adeptos na fila é inferior a um minuto, quer o número médio de adeptos na fila é inferior a dois adeptos. Por outro lado, tendo em conta a informação obtida no ponto “Calculo teórico das características do sistema”, e efectuando uma análise dos recursos humanos necessários envolvidos, está-se a falar de três membros da organização por torniquete, o que implica um total de $(3 \times 63) = 189$ elementos da organização cuja função é o revistar dos adeptos.

Uma vez que quer o número médio de adeptos na fila de espera, quer o tempo médio de espera na fila se encontram em valores aceitáveis para eventos de esta natureza, a solução proposta deve ser aceite, sem que se justifique o aumento de elementos da organização cujas funções sejam o revistar dos adeptos.

6.7 Conclusão

Este capítulo analisa, compara e valida pelos resultados obtidos dos três modelos de simulação distintos, o modelo obtido.

A necessidade de se obter um modelo de simulação que se aproxime ao máximo do sistema real é de extrema importância, uma vez que é o sistema real, quer pela sua dimensão e complexidade não permite efectuar o estudo pretendido.

Independentemente do modelo de simulação utilizado, a existência de filas de espera é uma realidade em sistemas deste tipo: Sistemas de Controlo de Acessos a Estádios de futebol.

Assim o desempenho do Sistema depende directamente das filas de espera e dos processos que lhe estão associados, o que justifica o estudo deste capítulo.

Numa primeira fase e considerando o modelo analítico correspondente ao Sistema de Controlo de Acessos ideal, ou seja apenas considerando a existência do torniquete, mais precisamente o seu tempo de funcionamento, calcula-se o tempo médio de espera na fila bem como o número médio de adeptos na fila.

Posteriormente é efectuada uma comparação entre os resultados obtidos anteriormente, com os obtidos recorrendo ao modelo de simulação correspondente.

A diferença entre ambos foi praticamente nula, o que permite validar o modelo de simulação adoptado.

Uma vez que o sistema real é composto por processos que não foram considerados na obtenção do modelo analítico, torna-se necessário recorrer a um novo modelo, que se aproxime mais da realidade. Assim, numa segunda fase é incluído no modelo de simulação anterior um módulo denominado Revistar, tornando-o mais próximo do sistema real.

Os resultados obtidos quer para o tempo médio de espera na fila quer para o número médio de adeptos na fila não foram considerados satisfatórios, uma vez apresentarem valores demasiado elevados para serem aceites numa situação real. O motivo de tal situação deve-se ao facto da taxa de ocupação

do módulo Revistar se encontrar com o valor máximo possível, o que implica um aumento do tempo de espera, que por sua vez implica o aumento do número de adeptos na fila.

Após detectado o motivo do mau desempenho do modelo de simulação, optou-se por incluir mais dois módulos Revistar em paralelo com o módulo Revistar do modelo de simulação anterior.

Os resultados da simulação correspondentes a este terceiro modelo já são considerados satisfatórios uma vez que se encontram na ordem de grandeza dos valores apresentados num sistema de controlo de acessos real deste tipo.

Capítulo 7 – Conclusão

Esta dissertação analisa os Sistemas de Controlo e Gestão passíveis de serem implementados numa organização, enquadrados na existência de Sistemas de Informação capazes de integrar os diversos subsistemas que normalmente suportam essas organizações.

A escolha de analisar um caso particular de uma organização, mais propriamente um Estádio de futebol, deveu-se ao facto de se tratar de uma organização que engloba os diversos Sistemas de Controlo e de Gestão que se pretende analisar, para além de que as especificações neste tipo de organização abrangem uma grande parte dos requisitos existentes em outros tipos de organizações.

Assim foi efectuada uma análise aos diversos Sistemas de Controlo e de Gestão existentes num Estádio de futebol, bem como à integração necessária entre os diversos sistemas e subsistemas de forma a que a organização possa ser moderna e competitiva no mercado onde se situa.

As especificações dos diversos sistemas e subsistemas anteriormente analisados, em particular do Sistema de Controlo de Acessos, obrigam a efectuar uma análise dos métodos de validação mais usuais em sistemas deste tipo.

Paralelamente foi necessário também efectuar um levantamento das diversas tecnologias disponíveis com este tipo de sistemas, uma vez que a especificação do sistema de controlo a implementar depende, obviamente, das tecnologias disponíveis, bem como das respectivas restrições inerentes ao projecto em questão.

Com esta análise foi possível identificar à partida dois grandes tipos de tecnologias: a biométrica e a convencional – bem como um terceiro tipo o qual conjuga ambas as tecnologias anteriores: a mista.

Alcançados os dois objectivos anteriores, foi definido um terceiro objectivo, o qual tinha como finalidade obter e validar um modelo que representasse o Sistema de Controlo de Acessos a um Estádio de Futebol real, uma vez que

quer a complexidade, quer a dimensão do sistema em questão não permitem a análise directa do sistema.

Foi, inicialmente, determinado um modelo analítico correspondente ao Sistema de Controlo de Acessos ideal, o qual apenas considera a existência do torniquete, ou seja, do tempo de atendimento a ele associado.

A determinação deste modelo depende directamente das equações das filas de espera – distribuições das chegadas e do atendimento – as quais foram motivo de análise.

A necessidade de validar o modelo em questão, bem como os resultados obtidos é a etapa seguinte no projecto de simulação.

Assim houve necessidade de recorrer a um ambiente de simulação apropriado que possibilitasse a validação, bem como a análise do desempenho do modelo.

A existência de diversas linguagens de programação e simuladores, implicou uma apresentação sucinta destas, de forma a permitir optar pela solução que melhor se enquadrasse no caso em questão. Essa opção recaiu na aplicação Arena – uma descrição detalhada das suas características face ao modelo de funcionamento do sistema a simular ilustra a propriedade desta escolha.

A validação do modelo analítico foi então possível, uma vez que os resultados provenientes do modelo de simulação correspondente foram idênticos.

A determinação de outros dois modelos de simulação permitiu aproximar o modelo anterior da realidade, bem como possibilitou a análise da resposta do sistema perante situações distintas – quantidade de “módulos” Revistar.

Esta análise permitiu concluir que o desempenho do sistema real depende de determinados factores, tais como o tempo de espera ou o número de adeptos na fila de espera, os quais não teriam sido possíveis analisar sem recorrer à simulação, uma vez que se trata de um sistema de grande dimensão e complexidade.

Esta dissertação a partir das diversas análises efectuadas aos sistemas de controlo de acessos permitiu concluir que:

- ⇒ Existem diversas tecnologias que facilitam a integração no Sistema de Informação. As características do Sistema, no qual o sistema de controlo de acessos se pretende integrar, restringem o método de validação a implementar.
- ⇒ Foi efectuado, baseado no cartão magnético/código de barras, um estudo das tecnologias apropriadas de modo a seleccionar o método de validação. Deve-se optar por tecnologias convencionais sempre que se esteja perante sistemas com um elevado número de utilizadores.
- ⇒ O Planeamento dos acessos exige uma cuidadosa análise das filas de espera e processos associados. O tempo de espera e a quantidade de pessoas em espera é determinante para o bom desempenho do sistema.

O projecto da quantidade de pontos de entrada e dos processos associados a cada porta de entrada é optimizável a partir da utilização apropriada de um ambiente de programação e simulação. Neste trabalho foi usado o Arena. Na verdade o desempenho do sistema nos diversos cenários é conhecido por antecipação permitindo comparar soluções, uma vez que os resultados por simulação são muito próximos dos resultados analíticos.

A conclusão de um projecto como este estava associada à satisfação de um conjunto de requisitos, que têm como objectivo trazer algum valor acrescentado à investigação na área do Controlo de Acessos.

Finaliza-se com a esperança de ter contribuído para o enriquecimento do conhecimento no domínio do Controlo de Acessos e das tecnologias existentes neste tipo de sistemas.



Bibliografia

Alter S., Information Systems: A management perspective, Addison-Wesley, 1992.

Auer T., Beyond IS implementation: A Skill-based approach to IS use, Proceedings of the 3rd European Conference on Information Systems, Athens-Greece, 1995.

Earl M. J., Management Strategies for Information Technology, Prentice Hall, 1989.

McFarlan F. W., Information Technology changes the way you compete, Harvard Business Review, July-August, 1983.

Neto E., Ling L. Lee, Sistema de Reconhecimento Facial Baseado em Análise de Componentes Principais, 1997.

Bianchi R., Visão Computacional Aplicada ao Controlo de Micro Robôs, 2001.

Barbosa A., Rastreamento do Movimento de Características Faciais Importantes, 2001.

Guia A., Segurança à porta: A biometria, 2002.

Daugman J., How Iris Recognition Works, www.CL.cam.ac.uk/users/jgd1000.

Wildes P. Richard and Iris Recognition: An Emerging Biometric Technology.

Chellappa R., Wilson C. L., and Sirohey S., Human and machine recognition of faces: A survey, IEEE, vol. 83, May 1995.

Chung Chang-Kyung, An Biometric Identification System by Extracting Hand Vein Patterns, Journal of Korean Physical Society, Vol. 38, N.º 3, March 2001.

Kumar A., Wong D., Shen H., and Jain A., Personal Verification using Palmprint and Hand Geometry Biometric, 2003.

Monrose F., Reiter M. K., Li Qi, and Wetzel S., Cryptographic Key Generation from Voice, IEEE 2001.

Pankanti S., Bolle R., and Jain A., Biometrics: The Future of Identification, IEEE 2000.

Sandmann H., and Senaga M., Bastet – Sistema de Reconhecimento Facial, 2001.

Ross A., Reisman J., and Jain A., Fingerprint Matching using feature space Correlation, 2002.

Caderno de encargos do Estádio de futebol do Dragão.

Proposta da Alcatel para o Estádio Municipal de Coimbra.

Proposta da INDRA CPC para o Estádio de futebol do Dragão.

Catálogo número S907-E1-1, Electromagnetic Inductive RFID System, disponível no site <http://www.omron.com/card/rfid/>.

Os diversos tipos de código de barras e seu funcionamento disponível no site: http://www.clubecobol.com.br/cc_cod_barras.asp.

A presença da Novabase SGPS nos Estádios de futebol, disponível no site <http://www.novabase.pt/showNews.asp?idProd=resentrevistajvrano>.

Presença da Novabase SGPS no Euro 2004, disponível no site <http://semanainformatica.xl.pt/661/actualidade/a03-00-00.shtml>.

Características técnicas e descrição de funcionamento do cartão magnético, disponível no site <http://www.teleponto-sa.pt/produtosservicos/produtos/leitormagnetico/leitormagnetico.htm>.

Definição de conceitos relacionados com biometria e métodos biométricos existentes, disponível no site <http://www.biopersona.com/irism.asp>.

Informação técnica sobre torniquetes utilizados em Estádios de Futebol, disponível no site <http://www.skydata.com>.

Introdução às filas de espera, disponível no site <http://www.dei.isep.ipp.pt/~andre/documentos/tfe.html>.



FACULDADE DE ENGENHARIA

UNIVERSIDADE DO PORTO

BIBLIOTECA



0000078333