1
Introdução

Sistemas supervisores envolvendo software embarcados são encontrados com freqüência e são responsáveis pela supervisão de equipamentos que vão desde máquinas industriais e eletrodomésticos, a celulares e PDAs. Estes sistemas muitas vezes necessitam tomar decisões por si só, baseados no estado do ambiente no qual executam, e são incumbidos de realizar tarefas como controle, monitoração ou supervisão de processos. Muitos possuem severos requisitos de confiabilidade e tolerância a falhas, bem como características de sistemas de tempo real.

Esta pesquisa investiga o uso de tecnologias de ponta como *Design by Contract*[1], Agentes de Software[2], *Mock Objects*[3] e Componentes de Software[4] no auxílio ao desenvolvimento de sistemas de monitoramento e aquisição em tempo real. Explora-se, ainda, o conceito de sistemas orientados à recuperação[5]. Para realizar tal análise, é utilizado como estudo de caso um sistema de inspeção de dutos que foi implementado utilizando tais tecnologias.

1.1
Contextualização

Ao analisar as etapas de desenvolvimento de um software, é possível perceber que, apesar de existir um vasto número de ferramentas e técnicas avançadas que auxiliam no desenvolvimento, algumas etapas, em especial a fase de geração de código, ainda são manuais, ou seja, mesmo utilizando programas que geram partes ou esqueletos do código, o próprio desenvolvedor deve escrever grande parte código, em especial a parte relacionada ao negócio. Em um processo manual, existe uma propensão natural à ocorrência de faltas[1] de construção decorrente da inevitável falibilidade humana. Este problema se

[1]Uma falta é um defeito no software que, quando exercitado, provoca um erro. Um erro é um estado incorreto com relação à especificação, às expectativas do usuário, ou ao mundo real com que o qual o software interage. Ao observar a ocorrência de um erro este passa a ser uma falha.[6] Em outras palavras, uma falta é qualquer defeito que possa provocar erros, enquanto que uma falha é esse erro quando o mesmo acontece.

torna especialmente crítico quando o sistema tem requisitos de qualidade muito altos, como ocorre em sistemas embarcados, sistemas de controle de processos e sistemas de supervisão.

Uma alternativa para o desenvolvimento de sistemas com qualidade final maior do que a comumente alcançada é o desenvolvimento de sistemas orientados à recuperação. Sistemas orientados à recuperação devem se basear no fato de que falhas de hardware ou software e erros de operação do sistema são fatos com os quais é preciso conviver, e não problemas que possam ser adequadamente resolvidos e completamente eliminados durante o desenvolvimento do software.[5]

Segundo Patterson[5] os axiomas do desenvolvimento orientado à recuperação são:

- É impossível construir software que não contenha faltas.
- É utópico assumir que um software, mesmo que perfeito, não possa sofrer danos decorrentes de falhas de hardware, de agressões ou de outro software com o qual venha a conviver ou possa depender.
- É utópico assumir que seja possível prever todas as possíveis faltas de um software, sejam elas decorrentes do software em questão ou do contexto ao qual está inserido.
- Algumas falhas de software podem ser toleradas, desde que as suas conseqüências sejam minimizadas.

A partir dos axiomas apresentados, pode-se concluir que o objetivo final de um processo de desenvolvimento de software não deve ser a construção de um sistema livre de faltas, e sim um sistema cujo risco de ocorrência de falhas seja aceitável e no qual as conseqüências da ocorrência de uma falha também sejam aceitáveis, de tal forma que o usuário possa rapidamente e confiavelmente dar prosseguimento ao seu trabalho. A natureza e o risco aceitável das falhas dependem dos requisitos e do domínio do sistema em desenvolvimento. Os fatores que influenciam esta identificação são: existência de risco de vida; danos a equipamentos, à natureza ou ao próprio negócio; perda de dinheiro ou de trabalho realizado; tempo gasto para restaurar o sistema e para restaurar no sistema o estado imediatamente anterior àquele em que ocorreu a falha; dentre outros.

1.2
O Estudo de Caso

De acordo com [7] a atual rede de dutos para transporte de óleo, gás e outros fluídos existente no mundo é bastante extensa. Esta rede (heterogênea) possui muitos dutos antigos (com mais de quarenta anos de idade), ao passo que outros, mais recentes, foram construídos com o uso de técnicas modernas. A Figura 1.1 mostra uma rede de dutos para transporte de óleo.

Figura 1.1: Dutos de transporte de petróleo[8]

Os dutos sofrem desgaste com a ação do tempo, do clima e de outros fatores. Quando o desgaste é grande, podem ocorrer vazamentos, o que, em muitos casos, pode levar a sérios danos ao meio-ambiente, além dos conseqüentes gastos com multas e reparos. A Figura 1.2 mostra um duto que sofreu corrosão.

Figura 1.2: Duto com corrosão[9]

Para evitar problemas com o desgaste dos dutos, as empresas operadoras de dutos inspecionam periodicamente suas linhas[2]. Uma inspeção normalmente é realizada por empresas especializadas, as quais fazem uso de equipamentos instrumentados, munidos de sensores de variados tipos. Os sensores coletam dados sobre o estado do duto em questão, e tais informações posteriormente são analisadas por especialistas.

O equipamento mais utilizado atualmente para inspeção de dutos é o inspetor interno de dutos, que recebe a denominação de PIG[3]. O PIG é um robô autônomo instrumentado com sensores dos mais variados tipos que percorre o duto internamente, com o objetivo de coletar informações relativas ao estado do duto em questão (Figura 1.3).[10, 11, 12]

Figura 1.3: PIG sendo inserido em um duto[13]

No entanto, nem todas as linhas permitem o uso do PIG. Existem dois casos principais onde o PIG não pode ser utilizado: quando o PIG não pode passar por algum ponto do duto (curvas muito acentuadas, grande variação de diâmetro ou bifurcações); e quando o duto não foi projetado para receber um PIG (o duto não possui uma estrutura que permita colocar e retirar o PIG). Tais linhas são chamadas de "linhas não-PIGáveis". Para essas linhas, um dos equipamentos

[2]Uma linha é um duto ou conjunto de dutos que transporta fluidos entre duas localidades.

[3]Este equipamento tem o nome de PIG (porco), pois como o fluxo do duto não é interrompido (é o fluxo do duto que movimenta o PIG), o PIG realiza a inspeção imerso no fluido. Por este motivo, no fim da inspeção o equipamento está muito sujo, ou seja, "emporcalhado".

utilizados atualmente para inspeção é o inspetor externo de dutos (IED), um robô que percorre o exterior de dutos, abraçando-os (Figura 1.4).

Figura 1.4: Inspetor externo de dutos (IED)[14]

O fato do IED ser usado externamente traz à tona algumas questões que inviabilizam o uso do mesmo sistema usado em PIGs. Por exemplo, ao contrário do PIG, o IED precisa ser montado e desmontado a cada obstáculo (suportes, junções, curvas acentuadas, etc. - Figura 1.5) encontrado.

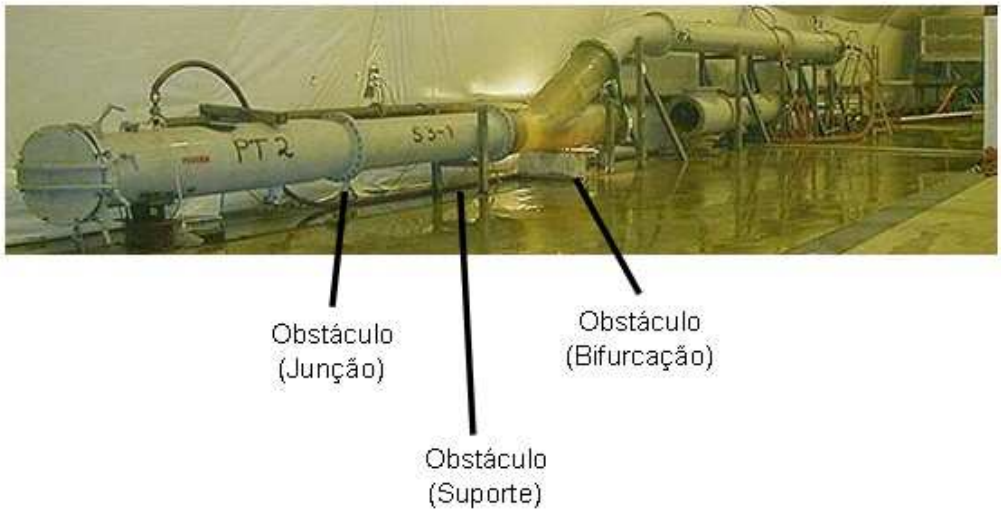

Figura 1.5: Obstáculos em um duto[12]

Devido a estes motivos, surgiu a necessidade de se desenvolver um novo sistema para ser usado na inspeção de dutos realizada com o IED, o que foi feito neste trabalho. Este sistema, chamado Ext-View, é um sistema de monitoramento e aquisição em tempo real, desenvolvido utilizando diversas tecnologias como *Design by Contract*, agentes de software, *bluetooth*, software

embarcado, dentre outras. Ele é formado por dois subsistemas: um software embarcado que executa na ferramenta de inspeção; e um software supervisor que executa em um computador pessoal (ou notebook).

Os requisitos de qualidade existentes neste sistema são extremamente altos, pois o atraso ou a falha no envio ou no recebimento dos dados coletados, ou a demora no tratamento de um sensor defeituoso, acarretará perda de informações que podem fazer com que um sinal importante não seja corretamente enviado e/ou tratado a tempo. Falhas que inviabilizem o uso são inaceitáveis, assim como o tempo médio entre falhas deve ser o mais alto possível. O Ext-View pode ser considerado um exemplo prático onde é possível testar o uso de tecnologias e conceitos modernos, combinando-os de tal forma a atingir os requisitos. Neste trabalho foram desenvolvidos tanto o software supervisor quanto o software embarcado. O software embarcado foi desenvolvido de modo que possa ser reutilizado em outros sistemas semelhantes, devido ao fato de que futuramente será desenvolvido um outro sistema de inspeção de dutos para portáteis (celulares e PDAs). Como o software embarcado tem as mesmas funções em ambos os sistemas, apenas um software embarcado será desenvolvido, e será utilizado pelos dois sistemas. Por esse motivo o software embarcado terá que ser capaz de interagir com software supervisores desenvolvidos em linguagens diferentes para plataformas diferentes.

1.3 Organização da Dissertação

O restante deste trabalho está organizado da seguinte forma: O Capítulo 2 apresenta uma revisão bibliográfica das tecnologias envolvidas neste trabalho. No Capítulo 3 serão discutidos alguns trabalhos relacionados. O Capítulo 4 apresenta a arquitetura adotada no sistema desenvolvido, enquanto que o Capítulo 5 apresenta detalhes sobre a sua implementação. As conclusões e os trabalhos futuros serão apresentados no Capítulo 6.