

- IMP Responda as perguntas 1 e 2 numa folha e às restantes noutra.
- Justifique todas as respostas.

1 - Sobre sistemas distribuídos.

1.1- [1v] Refira duas vantagens da utilização de distribuição na concepção de aplicações. Justifique.

1.2- [1v] Dê dois exemplos de fenómenos com origem na rede de comunicação que geram problemas ao nível das aplicações distribuídas. Justifique.

1.3- [1v] Discuta sucintamente o conflito abstração versus determinismo no âmbito do middleware.

2 - Considere que pretende desenvolver uma aplicação de controlo de um sistema industrial que contém um conjunto de robôs que cooperam entre si para realizar as funções desejadas, um servidor onde são armazenadas configurações e registos de operação e ainda uma estação de monitorização e controlo global. As interações entre os robôs são periódicas e relativamente rápidas, na ordem dos 20ms, difundidas entre todos (multicast), e envolvem a partilha de estado. Por outro lado, as trocas de configuração são esporádicas e pouco frequentes, e correspondem à troca de ficheiros entre os robôs e o servidor. Finalmente, a monitorização do estado dos robôs é feita recebendo na estação de monitorização o estado que os robôs partilham entre si, enquanto que os comandos de controlo são esporádicos e enviados pela estação de monitorização para cada robô separadamente.

2.1- [2v] Caracterize os requisitos dos fluxos de informação envolvidos na aplicação em termos de fiabilidade, pontualidade e sugira um protocolo de transporte/rede e um modelo de cooperação adequados.

	Fiabilidade	Pontualidade	Protocolo	Mod. cooperação
Interações entre robôs				
Configurações e logs				
Monitorização				
Comandos				

2.2- [1v] Os robôs funcionam intermitentemente, ligando-se e desligando-se durante o funcionamento do sistema. Para obter transparência de distribuição, dê um exemplo de um middleware standard que poderia usar e justifique sucintamente.

2.3- [2v] Para permitir relacionar os logs com a evolução do estado dos vários robôs foi utilizado um protocolo de sincronização de relógio do tipo master-slave, com o master instalado no servidor. O master envia uma mensagem de sincronização com o relógio global, periodicamente, com período T_s . Tendo em conta que a precisão dos cristais dos relógios locais de cada computador (de cada máquina) é de 10^{-5} , diga qual a frequência com que o master deve enviar a mensagem de sincronização para obter uma precisão global de 1ms. Despreze o atraso de rede e considere-a fiável. Que alteração faria para tolerar a perda de uma mensagem de sincronização e manter a precisão desejada?

2.4- [2v] Suponha que é adicionado ao servidor um blackboard para comunicação entre os robôs. Contudo, é necessário garantir a exclusão mútua no acesso ao blackboard. Indique um mecanismo adequado para o conseguir e explique sucintamente o seu funcionamento.

3 - Sobre a semântica de falhas de RPC/RMI *at-most-once* e a sua implementação.

3.1- [1v] Quais as garantias fornecidas por esta semântica?

3.2- [1v] Considere um sistema de RPC/RMI que use o protocolo UDP. Explique como esse sistema poderá garantir esta semântica na presença de **falhas quer nas comunicações quer no servidor**.

4 - [1.5v] Na análise e concepção de algoritmos tolerantes a falhas é comum usar quer modelos de sincronismo quer modelos de falhas.

Diga o que descreve cada um destes modelos e explique, considerando o problema do acordo distribuído, o interesse do seu uso naquelas tarefas.

5 - Considere *view synchronous multicast*.

5.1- [1v] Qual a diferença entre este tipo de *multicast* e a difusão fiável (*reliable multicast*) em grupos?

5.2- [1v] Considere um sistema em que os processos do grupo comunicam entre si através de canais ponto-a-ponto, fiáveis e do tipo FIFO. Explique em que medida o *crash* de processos dificulta a implementação de *view synchronous multicast*. Apresente duas possíveis maneiras de resolver o problema.

6 - [1v] Diga o que entende por replicação e explique as razões do seu uso em sistemas distribuídos.

7 - Considere o protocolo de replicação *quorum-consensus*.

7.1- [1.5v] Sejam N_R e N_W o tamanho dos *quorums* de leitura e de escrita e N o número de réplicas. Enuncie as desigualdades que deverão ser satisfeitas por estes parâmetros. Justifique.

7.2- [1v] Considere um modelo de falhas em que a única falha possível é a partição da rede. O protocolo *quorum-consensus* suporta o modelo de consistência sequencial neste modelo de falhas? Em caso negativo apresente uma possível execução ilustrando a violação desse modelo de consistência. Em caso afirmativo justifique.

8 - [1v] Em sistemas criptográficos assimétricos faz-se uso de dois tipos de chaves – chaves públicas e chaves privadas. Mostre, dando exemplos da sua aplicação na implementação de mecanismos de segurança, que qualquer destas chaves pode ser usada quer em operações para cifrar quer em operações de decifrar.