Sistemas de Engenharia -

Automação e Instrumentação

Grupo 1

2012/2013

Gestão de Risco

5.5

Elaborado por: Francisco Branquinho

I. Introdução

Este documento tem como finalidade elaborar a análise de risco inerente ao "FEUP Formula Project", antevendo eventuais impactos negativos da sua materialização e criando soluções possíveis para os antever e contornar. Com esse propósito, recorreu-se à metodologia tipicamente conhecida para análises de risco, cuja base assenta nos seguintes passos: identificação, quantificação, resposta e monitorização / controlo. Cada uma destas etapas será explorada nas próximas páginas, sendo desenvolvida em duas dimensões distintas: organização / gestão interna da equipa e orientação técnica do projecto. Convém no entanto referir, que em toda esta análise se partiu do princípio que este projeto se propunha apenas a competir na classe 2 da competição "Formula Student", e, como tal, centrou-se principalmente na fase conceptual do mesmo.

II. Gestão interna da equipa – Gestão de risco

II.1 Identificação

Para uma análise objetiva e consistente neste contexto, é necessário, em primeiro lugar, selecionar os potenciais problemas que serão objeto de análise, ou seja, todos aqueles que representem riscos para o projeto e ameacem o seu sucesso. Nesse sentido, e atendendo a que este projeto será apresentado a um júri (numa data fixa) que avaliará as suas questões técnicas, identificaram-se como fulcrais os seguintes riscos:

- Incumprimento de prazos (pela equipa e seus elementos): relativo a todo e qualquer atraso que, durante o desenvolvimento do projeto, comprometa o seu avanço ou leve ao incumprimento de datas fixadas.

- Incumprimento de prazos (por fabricantes ou outros): relacionado com atrasos de outro tipo, que não digam diretamente respeito à equipa. Normalmente associado a produtos ou serviços prestados à equipa por outras organizações, que se revelem importantes para o decorrer do projeto.
- Falhas de comunicação e consensos internos (equipa): associados a impasses e indefinições que decorram da falta de entendimento do grupo e dificultem a tomada de decisões.
- Falhas de comunicação com o cliente (equipa): associado a uma comunicação deficiente com o cliente, que não contribua para a correta orientação do projeto ou o alcance dos resultados que este pretenda.
- Reajustes no planeamento (equipa): resultado de problemas que surjam no decorrer do projeto, como por exemplo, outras falhas já mencionadas atrás.
- Absentismo (equipa): situação de ausência forçada por doença ou outro motivo que suspendam temporariamente as tarefas de alguns elementos.
- Falhas com equipamentos de trabalho: associado a falhas de equipamento que prejudiquem a ordem natural dos trabalhos e protelem entregas ou cumprimento de prazos.
- Perda de informação: falhas relacionadas com as plataformas de trabalho que tenham como consequência a perda parcial ou total de documentos importantes para o projeto.

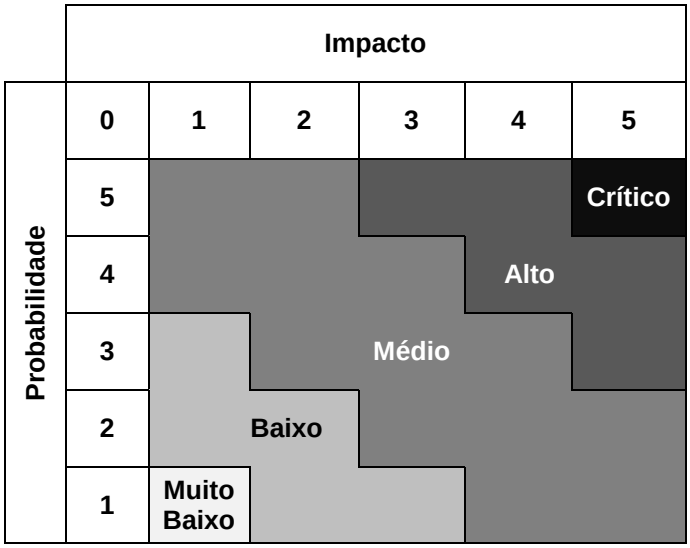
II.2 Quantificação

Uma vez identificados os riscos mais perigosos no âmbito do projeto, impôs-se então perceber qual a probabilidade da ocorrência de cada um, bem como o grau de importância / impacto que este teriam no seio da equipa e / ou no alcance dos seus resultados. Para facilitar esta análise atribuíram-se valores

numa escala de 0 a 5 para cada um dos parâmetros (probabilidade e impacto). Os valores estimados para cada caso figuram no quadro abaixo:

Risco analisado	Probabilidade	Impacto
Incumprimento de prazos (equipa)	4	4
Incumprimento de prazos (outros)	2	4
Falhas comunicação (equipa)	3	2
Falhas de comunicação (cliente)	2	2
Reajustes de planeamento	4	4
Absentismo	4	5
Falhas de equipamento	1	3
Perdas de informação	2	5

A par desta “dosagem”, elaborou-se igualmente um quadro com o fim de relacionar a probabilidade e o impacto de cada um dos pontos atrás referidos, refletindo a gravidade do risco inerente numa escala de muito baixo a crítico.



II.3 Resposta

Depois de "graduados" os diferentes riscos que podiam afetar a organização da equipa – e o consequente cumprimento dos seus objetivos – seguiu-se o passo seguinte: articular uma resposta. Nesta terceira etapa procurou-se encontrar soluções para os riscos classificados, estudando procedimentos possíveis para os prever ou contornar em tempo útil. Tal foi conseguido depois de uma nova análise, que, caso a caso, nos conduziu a "antídotos" mais ou menos fiáveis para os respetivos riscos. Por ordem de impacto, as respostas definidas foram as seguintes:

- Absentismo (risco **crítico**): todo e qualquer tipo de ausência deve ser comunicada previamente ao líder do grupo, de acordo com o M. de Qualidade da equipa e nos termos que este configura como necessários. Caso tal aviso – prévio – não seja possível, um célere reajuste dos recursos disponíveis é imperioso para distribuir trabalho pelos restantes elementos do grupo, sem prejuízo dos prazos estabelecidos.
- Incumprimento de prazos – equipa (risco **alto**): planeamento equilibrado e criterioso das várias semanas de trabalho, considerando o volume tarefas atribuídas a cada elemento e sua disponibilidade geral. Penalizações associadas a atrasos ou falhas nas entregas.
- Reajustes no planeamento (risco **alto**): atribuição de cargos interdisciplinares a alguns elementos da equipa para rápida realocação de recursos e desempenho de novas funções.
- Perdas de informação (risco **médio**): todos os documentos elaborados devem ser guardados em pelo menos três locais distintos (dois online para partilha com o grupo – Dropbox e Facebook – e um no disco pessoal), de modo a precaver falhas inesperadas de sistema. Por outro lado, cada elemento da equipa deve manter em sua posse apenas uma cópia dos documentos essênciais ao desenvolvimento da parte que lhe compete, e não de todo o projeto.

- Incumprimento de prazos – outras entidades (risco **médio**): escolha ponderada e sustentada das entidades externas a colaborar com a equipa, depois de uma análise exaustiva das suas condições de entrega (produtos) e / ou operação no terreno (serviços). Estudo e elaboração de um *backup plan*, no qual constem alternativas para todas as vertentes de apoio externo ao projeto.
- Falhas de comunicação e consenso – equipa (risco **médio**): aferir semanalmente as dificuldades de entendimento e consenso no seio grupo, recorrendo a votação geral caso alguma decisão importante seja impossível.
- Falhas com equipamentos de trabalho (risco **baixo**): selecionar à partida qual ou quais os equipamentos de trabalho que dão melhor garantias de fiabilidade, analisando as suas potencialidades e qualidade dos seus resultados.
- Falhas de comunicação com o cliente (risco **baixo**): promover um contacto mais frequente com o cliente para cultivar a proximidade do mesmo com o projeto, e obter assim respostas mais sólidas quanto à sua orientação. “One step ahead” – leitura do planeamento antes das reuniões e, sempre que possível, retirar do cliente informação importante para as duas fases subsequentes. Se, por algum motivo, uma ficar bloqueada, um reajuste de planeamento permitirá manter o ritmo de trabalho e evitar prejuízos no cumprimento de prazos

II.3 Monitorização e controlo

Por fim, para encerrar este capítulo de análise – relativo às questões de organização interna da equipa – foram equacionados diferentes métodos de monitorização, com vista a auscultar a equipa e verificar se as respostas definidas para cada risco surtiam o efeito desejado. Em rota convergente, definiu-se também para cada caso um registo de *feedback*, em função do qual, um diferente tipo de realimentação fosse possível para o controlar.

Risco analisado	Monitorização / Controlo
Incumprimento de prazos (equipa)	Registo das datas de entrega dos vários elementos do grupo e atribuição de penalizações para falhas nos prazos estipulados. Penalizações atribuídas com base na escala em anexo (*).
Incumprimento de prazos (outros)	Contacto próximo e frequente com todas as entidades das quais dependa o avanço do projeto, para um acompanhamento contínuo de todos os processos. Registo dos avanços ou recuos dos colaboradores para aferir a qualidade de produtos ou serviços prestados à equipa.
Falhas de comunicação (equipa)	Registar divergências de opinião em relação a questões nucleares do projeto e implementar métodos de decisão alternativos que acolham todo o grupo na decisão tomada.
Falhas de comunicação (cliente)	Verificar se a comunicação com o cliente está a estabelecer-se nos contornos desejados e está a ser salvaguardada a orientação correta do projeto (atendendo aos requisitos). Elaborar um histórico de contactos e directrizes importantes dadas pelo cliente e conferir com as do projeto.
Reajustes de planeamento	Avaliação informal extraordinária dos elementos que desempenham cargos que não lhes dizem diretamente respeito, para perceber se são cumpridos os objetivos traçados.
Absentismo	Registo da presença ou ausência dos elementos nos compromissos da equipa (reuniões, apresentações, etc) e publicação dos mesmos no repositório online: *Dropbox*. Penalizações atribuídas com base na escala em anexo (*).

Falhas de equipamento	Registar falhas (e aparente justificação) dos dispositivos usados e averiguar a sua origem junto da assistência técnica competente.
Perdas de informação	Consultar periodicamente os repositórios de documentação online e verificar se os dados permanecem inalterados. Efetuar *back-ups* com frequência mensal.

III. Especificação técnica – Gestão de risco

III.1 Identificação

À semelhança da análise realizada na secção anterior (II), também na parte técnica do projeto se usou a mesma abordagem para a gestão do risco. Contudo, atendendo à complexidade do mesmo e aos vários sub-sistemas que integra, resolveu-se agrupar os riscos em subconjuntos mais restritos, de modo a individualizar a análise e conseguir assim ter uma visão mais periférica das ameaças e perigos a que projeto estivesse exposto.

➢ Sistema de Armazenamento de energia

- Insegurança na operação (baterias): A utilização de baterias lítio polímero apresenta riscos no que respeita à sua incorrecta utilização Se for sujeita a sobrecargas e também se for curto-circuitada através da circulação de correntes muito elevadas, existe o risco de incendiar ou explodir.
- Falta de autonomia (sistema de energia): associado principalmente à prova de Endurance (22km), na qual é solicitada maior quantidade de energia ao sistema de armazenamento. Perigo da capacidade do

sistema de armazenamento de energia dimensionada não suprir totalmente as necessidades do condutor para a conquista da prova.

➢ Sistema de monitorização

- Sobrecarga da rede: relacionado com situações em que o sistema de monitorização do veículo não responda, devido a excesso de comunicações em simultâneo.
- Falha do sistema de corte central: associado a situações de perigo eminente para o condutor ou para outros, em que o sistema de corte não atue por falha mecânica ou elétrica.
- Falha da actuação em caso de curto-circuito: relacionado com situções de defeito, sobrecarga ou avaria, cuja consequência possa ser a falha geral do sistema de monitorização.

➢ Sistema de controlo

- Erros na estimação / sensorização: problemas que afetam a rede de campo, (e seus sensores) que prejudicam a estimação correta de valores importantes para a equipa e condutor no decorrer da prova.
- Falha no sensor rotativo (encoder): carateriza-se por erros de leitura no sensor rotativo, que podem derivar ou não da sua própria avaria.
- Tempo de resposta do controlador superior ao tempo de ciclo: originados por atrasos na rede de comunicação, que conduzam a uma resposta inadequada – ou fora de tempo – do sistema de controlo.
- Erros de programação: associado a *bugs* que não se detetem atempadamente na programação do sistema de controlo, e comprometam a funcionalidade do sistema na prática.

➢ Sistema de tracção

- Sobreaquecimento do motor (danificação de enrolamentos, etc):

- Desmagnetização do motor:
- Falhas no sistema de arrefecimento (fugas água):
- Perda de aderência (estabilidade do veículo):
- Sobre-tensões ou curto-circuitos no conversor:
- Sobre-aquecimento ou danificação de semicondutores do conversor:
- Aplicação de binário excessivo no eixo
- Ultrapassagem do tempo limite (**12**s) acima da potência nominal

III.2 Quantificação

Numa escala de 0 a 5 definiu-se o peso relativo para cada risco descrito atrás, classificando-o quanto à probabilidade de ocorrer e impacto que teria na prova. Os valores estimados para cada caso figuram no quadro abaixo:

Risco analisado	Probabilidade	Impacto
Insegurança na operação (baterias)	2	5
Falta de autonomia (sistema de armazenamento de energia)	3	5
Sobrecarga da rede de comunicação	1	3
Falha do sistema de corte central	2	5
Falha de atuação em caso de CC	2	5
Erros de estimação / sensorização	3	4
Falha no sensor rotativo (encoder):	2	4
Tempo de resposta superior ao tempo de ciclo	2	3
Erros de programação	1	4

Sobreaquecimento do motor (danificação de enrolamentos, etc.)	3	5
Desmagnetização dos imanes do motor	3	5
Falhas no sistema de arrefecimento (fugas água)	2	5
Sobre-tensões ou CC no conversor:	2	5
Sobre-aquecimento ou danificação de semicondutores do conversor:	2	5
Aplicação de binário excessivo no eixo	1	5

III.3 Resposta

Recorrendo ao mesmo quadro que foi usado anteriormente (de impacto / probabilidade na secção II), classificaram-se os riscos descritos acima e aferiu-se o grau de prioridade na resposta de cada um. Em função dessa prioridade, foram então estudadas as possíveis soluções para dar resposta aos potenciais riscos classificados. Por ordem de impacto, definiram-se então as seguintes:

- Insegurança na operação das baterias (risco **alto**): utilização dum BMS (Battery Management System) responsável pela leitura da temperatura, a corrente e tensão para avaliar o funcionamento correto da bateria.
- Falta de autonomia (risco **alto**): procura de uma melhor eficiência do sistema: durante a travagem, controlar o motor elétrico de maneira a converter a energia cinética em energia eléctrica e, deste modo, realimentar o sistema de armazenamento de energia. Para isso, usar conversores no controlo das fontes de energia, permitindo assim o funcionamento em fluxo bi-direccional de corrente, não só fornecendo energia ao motor, como também aproveitando a energia do motor na frenagem recuperativa.

- Sobrecarga da rede de comunicação (risco **médio**): utilização de um *logger* que registe as comunicações efetuadas na rede, de modo a inspecionar os processos que estiveram na origem da sobrecarga – caso esta ocorra.
- Falha no sistema de corte central (risco **baixo**): sinalização da avaria no habitáculo do condutor, através do painel central do veículo.
- Falha de atuação do sistema de monitorização em caso de CC (risco **médio**): sinalização de CC para o condutor e atuação simultânea de um sistema de proteção autónomo que salvaguarde a segurança do veículo, seus subsistemas e condutor.
- Erros de sensorização (risco **alto**): deve ser avaliado em duas dimensões distintas: 1, na parte que diz respeito ao controlo do motor e 2, à monitorização do veículo – genericamente. No primeiro caso, para a maioria dos sensores usados, o sistema de corte central deve ser atuado em caso de avaria ou defeito. Caso seja o sistema do monitorização que esteja em causa, apenas uma proteção elétrica local e independente do resto do sistema deve atuar, de modo a preservar o funcionamento são do resto do veículo e a sua performance. (Monitorização: leitura de valores individualmente de cada sensor para verificar se estes se incluem na gama de valores definida para cada um)
- Erros de estimação (risco **alto**): simulação virtual do modelo usado, de modo a registar o seu *feedback* e aferir fiabilidade da estimação efetuada. Validação períodica dos estimadores usados.
- Falhas do encoder (risco **alto**): uso dum subsistema – não com um, mas – com 3 encoders, que seja capaz de detetar a falha de algum deles por comparação dos valores obtidos entre eles. Caso ocorra, o veículo deve atuar o sistema de corte central.
- Tempo de resposta do controlador superior ao tempo de ciclo (risco **médio**): associado a atrasos de comunicação na rede e sujeito mais tarde a reflexão…

- Erros de programação (risco **baixo**): inspeção, verificação e teste exaustivo do código implementado em todas as fases do projeto.
- Sobreaquecimento do motor (risco **alto**): sensorização da temperatura interna do motor e definição de um valor limite máximo; que, se atingido (admitindo o correto funcionamento do sistema de refrigeração), deve acionar o sistema de corte central.
- Desmagnetização do motor (risco **crítico**): leitura da tensão aplicada ao motor por via de comunicação com o controlador, que, se persistente ou prolongada (na ordem de alguns segundos), leva a atuação do sistema de corte central.
- Falhas no sistema de arrefecimento (risco **alto**): utilização de sensores para leitura de pressão do líquido de refrigeração, bem como da sua temperatura. Comunicação da falha ao condutor através da rede de comunicação do veículo.
- Sobreaquecimento ou danificação de semicondutores do conversor por sobretensões ou CC (risco **médio**): leitura das correntes que circulam no conversor e consequente acionamento do sistema de corte central caso estas ultrapassem um valor máximo definido.
- Aplicação de binário excessivo no eixo:

III.4 Monitorização e controlo

Por fim, e novamente à semelhança do capítulo II, foram estudados diferentes métodos de monitorização e controlo do risco, com vista a auscultar a equipa e verificar se as respostas definidas para cada risco surtiam o efeito desejado. Paralelamente, definiu-se para alguns casos um registo de *feedback*, em função do qual, um diferente tipo de realimentação fosse possível para o controlar.

Risco analisado	Monitorização / Controlo
Insegurança na operação (baterias)	Utilização de BMS, responsáveis pela medição

	de tensão e temperatura de cada célula. Determinação do Estado de carga das baterias. Transmite a informação recolhida aos restantes-sub-sistemas, através de uma infra-estrutura de comunicações Não permitem que as células sejam carregadas acima de um limite máximo de tensão (4,2V). Não permitem o funcionamento das células abaixo de um limite mínimo de tensão (2,7V) Não permitem o funcionamento das células acima de um nível máximo de temperatura.
Falta de autonomia (sistema de armazenamento de energia)	Funcionamento do sistema de armazenamento de energia e do sistema de tracção em fluxo-bidireccional de energia. Aplicação de um algoritmo de gestão de energia por forma a tirar o melhor rendimento de cada fonte.

Conclusão

Anexo