THE DILEMMA DIAGNOSER APPROACH AND ITS APPLICATION TO THE FAULT-TOLERANT CONTROL OF PLANETARY EXPLORATION ROVERS

Alexandre Carvalho Leite [(1)], Bernd Schäfer [(2)]

[(1)] IFF – Federal Fluminense Institute, Rua Dr. Siqueira, 273, 28030-130 Campos, Brazil, Email: alexandre@iff.edu.br
[(2)] DLR – German Aerospace Center, Münchner Straße, 20, 82253 Weßling, Germany, Email: bernd.schaefer@dlr.de

ABSTRACT

Most of the fault-tolerant control strategies found in the literature assume conclusive diagnosis, i.e. the current fault mode of the plant is well-known. Although, speculative diagnosis can be a more realistic approach while noise corrupted measurements and plant disturbances hamper the construction of a precise diagnosis statement. Speculative diagnosis consists in providing a set with the most probable fault modes in the control system. The idea of a set with probable fault modes is not new, but reconfiguration is not an easy task in this context. Prompt reconfiguration under lack of a conclusive statement is not properly approached in the current literature. The risks involved in such decision are evaluated and used in the modeling of the Dilemma Diagnoser. It is a decision maker coupling speculative diagnosis statements and control reconfiguration to achieve a safe decision in a particular sense, i.e. keep the control system stable and close to the desired reference. The problem is modeled as a bi-matrix game, the two players are the Diagnoser (choses among several available fault modes in a speculative set) and the Switcher (choses between reconfigure instantaneously or wait until the next diagnosis sample to make a decision). It can be solved by game theory using Mixed-Strategy Nash Equilibrium. A specific control strategy is also developed to recover a multi-wheeled rover from steering motor failures. This strategy is integrated with the Dilemma Diagnoser and applied to the case of the ExoMars Rover. Note that all methods presented here are applicable to all kinds of multi-wheeled rovers and are capable to cover all amplitudes and combinations of steering failures as long as sufficient driving power is available. The fault-tolerant controller is tested in the Planetary Exploration Laboratory (PEL) of the German Aerospace Center (DLR-Oberpfaffenhofen); the controller is embedded in the ExoMars B2 Breadboard Model. The results are satisfactory and allow the vehicle to follow a predefined path formed by waypoints whether faults are present or not. Tests were conducted to ensure robustness of the fault-tolerant control system while driving with satisfactory performance either on Kalk Sand (high sinkage) or Lava Sand (moderate sinkage). Our proposed techniques are capable to lead the faulty rover to the desired path smoothly and progressively decreasing both attitude and displacement errors. The main contributions of this work are: the introduction of the Dilemma Diagnoser, the proposition of an alternative control strategy for steering motor failures, and experimental validation of fault-tolerant controller.

1. INTRODUCTION

In practice, the pattern of a given fault cannot always be perfectly decoupled from symptoms of other faults or even a disturbed plant. This situation leads to inconclusive fault diagnosis [1], when in fact that behavior can be assigned to more than one fault mode. Fault Detection and Diagnosis (FDD) schemes are also subjected to false and missed alarms, both are results of a wrong fault detection which can be easily propagated through diagnosis and reconfiguration stages.

The current FDD theory is concerned with detection techniques, diagnosis procedures, control reconfiguration and fault accommodation. But the decisions are assumed as correct at each stage, from detection to reconfiguration. It means that some fault tolerant controller switching assumes a perfect diagnosis decision which, on the other hand, assumes a perfect detection decision. This correctness is assumed only in the symptom space, not in the time domain. Note that the actual time of occurrence of a fault is considered as unknown.

The occurrence of a fault in the nominal system S0 represents a dynamic behaviour Bf which is no longer consistent with the previous B0. This transition, as shown in figure 1 left, can be caused by a fault in a known set F = {F1; F2} or even by some perturbation to the fault free dynamic system. In the performance variables' space (space of variables which describe the performance of the controlled dynamic system) the transition means a degradation of the dynamic system's performance. A control reconfiguration must be able to avoid the achievement of the unacceptable performance region and, if possible, bring it back to the required performance region in figure 1 right.

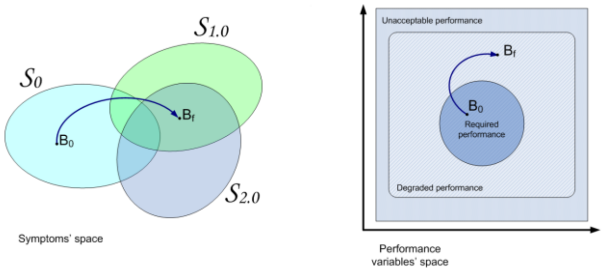


Figure 1. Anomalous behaviour of the initially fault free

Even after fault detection and diagnosis stages, the plant remains at some behavior Bf under the structure {P0; C0} (nominal plant P0 and nominal controller C0) until control reconfiguration takes place. The inconclusive diagnosis allows three switching choices (C0, C1 or C2), but just one of them is the correct one. As illustrated in figure 2, all three reconfiguration possibilities have their respective outcomes in face of a wrong decision. The respective drawbacks and benefits of each transition can be seen at the performance variables' space, figure 3.

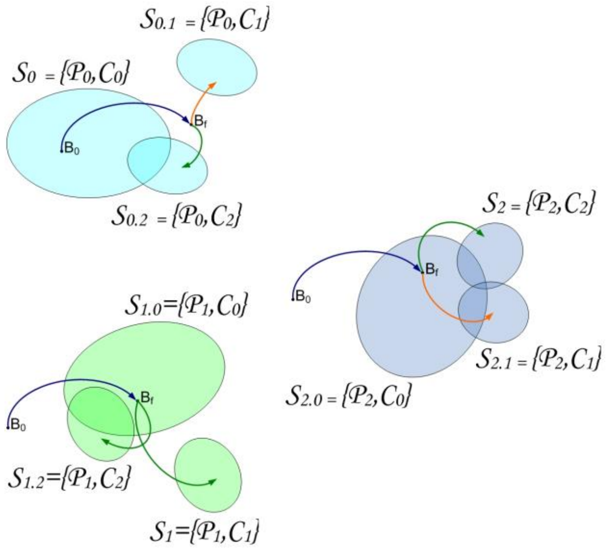


Figure 2. Switching possibilities after detection and inconclusive diagnosis

Note that, in this example, switching to C2 is the safest decision, because all the other wrong decisions would drive the system to an unacceptable performance region. We consider this decision as the low risk decision and the reconfiguration subsystem has no incentive to deviate from this decision to make the decision safer.

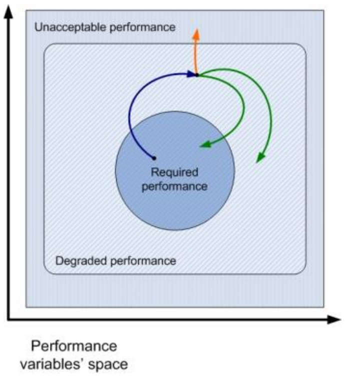


Figure 3. Effects of each transition in figure 2

The low risk decision is not a definitive diagnosis statement, it is just a palliative diagnosis statement considering only the (normally discarded) space of wrong decisions to choose the safest one. The general idea of this approach can be stated as follows:

Our approach offers conclusive diagnosis statements based on the risk of a wrong decision.

Section 2 describes the modeling of the problem, section 3 presents the main results of the Dilemma Diagnoser, section 4 shows an application example. The last section has conclusions and outlook of the next steps.

2. MODELING OF THE PROBLEM

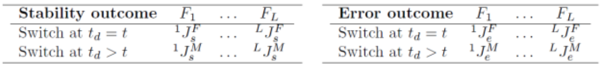
In an ideal fault tolerant control system we deal with several controlled dynamic systems, one for each fault mode. They are represented here as the pair {Pi; Ci}, where i (from 0 to N) is the index of each one of the fault modes, including the fault free case (i = 0) and the other N fault modes. These pairs are achieved when exact knowledge of the given system's operating mode holds. Although, we are not concerned with these operating modes, but with the other N(N - 1) operating modes resulting from wrong decisions. Decisions in the wrong decisions' space can drive the system to the unacceptable performance region, keep the system with degraded performance or bring it back to the required performance region. It means that there are risk levels inside the wrong decisions' space.

We quantify these risk levels according with two measures: 1) stability in sense of Lyapunov; 2) instantaneous quadratic error. These two metrics summarize the performance variables' space only during non-conclusive diagnosis statements. Enhanced description of performance requirements are left to the design of the individual controllers Ci. We consider the two measures as suitable quantities to "hold" the plant until sufficient information for conclusive diagnosis is available. This situation is called here as Dilemma Diagnosis and can be defined as follows.

Suppose an anomalous behavior Bf occurred at an unknown time tf. The behavior was detected at time td > tf and promptly diagnosed as Fu in F, where F is a finite set of known fault modes including the fault free case, and Fu is the currently unknown fault mode. The Dilemma Diagnosis is stated as the choice of one of the fault modes belonging to F considering its harm to the performance of the reconfigured control system in the case of a wrong choice.

Note that in the definition only wrong choices are considered, this is the origin of the term Dilemma used to name this definition. The harm to the performance of the wrongly reconfigured control system is measured using Lyapunov function and instantaneous quadratic error computation. Roughly speaking, a wrong diagnosis statement is safe if it is stable and reduces the instantaneous quadratic error of the controlled variables.
A wrong decision Fd in F should keep the dynamic system stable about some equilibrium point until a conclusive diagnosis statement Fu is chosen. The finite set F = {F0,..., FL} contains L (which can be less or equal to N) fault modes and the fault free case F0 inside the total range of N fault modes. Each wrong decision assigned to Fd corresponds to Missed Alarm and False Alarm.
Note that the outcomes of the wrong decisions are already propagated to the control reconfiguration stage. They are one step ahead time projections of the derivative of the Lyapunov function and instantaneous quadratic error for some controlled dynamic system pair {Pj ; Cj}. The time step to this extrapolation can be determined during the design of the Dilemma Diagnoser, treated in the next section.
The outcomes can be separated in two matrices according with the inconclusive diagnosis statement and the switching decision (reconfigure to Ci or keep C0), see table 1.

Table 1. Outcome matrices with returning stability and error penalties according to diagnosis and switching decisions



Stability outcome	F_1	$\dots$	F_L
Switch at $t_d = t$	${}^1J_s^F$	$\dots$	${}^LJ_s^F$
Switch at $t_d > t$	${}^1J_s^M$	$\dots$	${}^LJ_s^M$

Error outcome	F_1	$\dots$	F_L
Switch at $t_d = t$	${}^1J_e^F$	$\dots$	${}^LJ_e^F$
Switch at $t_d > t$	${}^1J_e^M$	$\dots$	${}^LJ_e^M$

A Dilemma Diagnoser provides the pair <td; Fd> as statement, which are switching time and safest conclusive diagnosis in the subspace of wrong decisions and in the sense of Lyapunov stability and instantaneous quadratic error. The value of Fd is only useful when td = t; in other words, when the controller is allowed to reconfigure to one of the fault modes. The Dilemma Diagnoser should be able to find a compromise solution of Js and Je, it is possible through game theory approaches as the previous matrices represent a bimatrix game. Even in game theory different definitions of equilibrium solution can be used. Next section shows the complete design of the outcomes Js and Je as well as a proposed solution by means of mixed-strategy Nash equilibria.

3. DESIGN OF THE DILEMMA DIAGNOSER (DD)

A DD is allowed to switch among several fault modes after each single decision based on outcomes Js and Je. It leads to a common practical problem of switching control, high frequency switchings. To overcome this problem, we introduce the sampling period T to the DD. Each decision of the DD is active during T seconds and evaluated at the end of this period, the numerical value of T is defined by the designer.
The time derivative estimate of the Lyapunov function is used as a measure of stability (Js). This estimate can be computed inside the sampling period of the DD and is the same used in [2]. The state transition matrix which transports the state vector x(t) to x(t + T) is Φ (t + T). It leads to the following definition of the estimated derivative of Lyapunov function

$$\dot{\tilde{V}}(t) = x^T(t)(\Phi^T(t,t+T)P\Phi(t,t+T) - P)x(t) \tag{1}$$

A general description of the used state transition matrices is

$$\begin{aligned} \Phi_{ip}(t,t+T) &= e^{(A_i+B_iL_p)T}, \forall i \neq p : i,p \in \{0,\dots,L\} \\ &= \Phi(\mathcal{P}_i,\mathcal{C}_p) \end{aligned} \tag{2}$$

where Ai and Bi are system and actuator matrices describing linearly the dynamics of the system in state space. Lp is the matrix with the gains of the linear state feedback controller for the p^th fault mode.
Je is also based in the same transition matrices, the instantaneous quadratic error about the state space's origin is calculated as

$$e^Te = x^T\Phi^T\Phi x \tag{3}$$

The outcomes in table 1 are summarized as follows

$$\begin{aligned} {}^iJ_s^F &= \max_{\substack{i\in\{1,\dots,L\} \\ j\in\{0,\dots,L\}}} (x^T(\Phi^T(\mathcal{P}_{i\neq j},\mathcal{C}_i)P\Phi(\mathcal{P}_{i\neq j},\mathcal{C}_i) - P)x) \\ {}^iJ_e^F &= \max_{\substack{i\in\{1,\dots,L\} \\ j\in\{0,\dots,L\}}} (x^T\Phi^T(\mathcal{P}_{i\neq j},\mathcal{C}_i)\Phi(\mathcal{P}_{i\neq j},\mathcal{C}_i)x) \\ {}^iJ_s^M &= x^T(\Phi^T(\mathcal{P}_i,\mathcal{C}_0)P\Phi(\mathcal{P}_i,\mathcal{C}_0) - P)x, \forall i \in \{1,\dots,L\} \\ {}^iJ_e^M &= x^T\Phi^T(\mathcal{P}_i,\mathcal{C}_0)\Phi(\mathcal{P}_i,\mathcal{C}_0)x, \forall i \in \{1,\dots,L\} \end{aligned} \tag{4}$$

The computation of the positive definite matrix P can be solved by Linear Matrix Inequality solution methods.

4. APPLICATION EXAMPLE – THE EXOMARS ROVER

The PEL of DLR is a test environment for the characterization of soil and dynamic tests with a full rover in hard and soft sand. A bevameter is used to characterize soil properties and a testbed filled with two types of sand. Soft sand and hard sand are placed side by side but not mixed; their occupied volume is soft sand (5,5m width, 4m width, 0.5m height) and hard sand (5,5m width, 6m width, 0.5m height). It is equipped with a passive tracking system to measure the actual rover position (accuracy less than 3mm) and orientation (accuracy less than 1º). The ExoMars rover is our main breadboard model used in dynamic tests in the testbed; this vehicle has three bogies equipped with angular position sensors, six wheels with independent driving and steering capabilities, force/torque sensors in each wheel, voltage and current measurements of all motors, and a real-time computer; see figure 4.

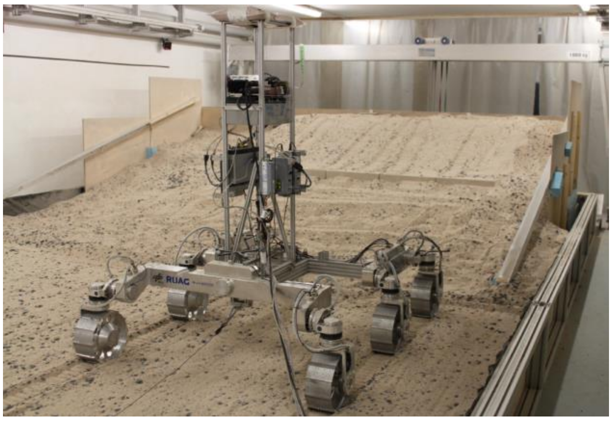


Figure 4. ExoMars Rover in the Planetary Exploration Laboratory of DLR

Hence, we consider a straight path Γ in the movement plane as illustrated in figure 5. Adopting the unicycle case, the Frénet frame representation in figure 5 is reduced to the following equations

$$\left\{\begin{array}{lcl} \dot{h} & = & v_0 \cos\theta_e \\ \dot{l}_e & = & v_0 \sin\theta_e \\ \dot{\theta}_e & = & \omega_0 \end{array}\right. \qquad (5)$$

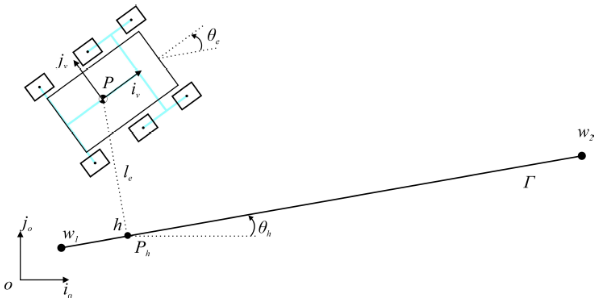


Figure 5. ExoMars Rover and path provided by Frénet representation

where v0 is the nonzero longitudinal velocity of the vehicle, $\theta_e = \theta_0 - \theta_h$ is the attitude of the vehicle with respect to the path, and ω_0 is the angular velocity of the vehicle. The straight line Γ is formed by the waypoints w1 and w2 to make the path where the inclined abscissa h at the point Ph is obtained by orthogonal projection of P on Γ. The objective of the path-following controller is to force le → 0 and $\theta_e \to 0$ driving and steering the wheels. But note that the kinematic model has just v0 and ω_0 as input variables. Thus, a higher level control system is designed to meet the path following objectives. This is possible by first constructing the Lyapunov function and determining ω_0 as control input dependant on three gains (k1, k2 and k3). The obtained control law is:

$$\omega_0 = -\left(k_1\,|v_0|\,\theta_e + k_2\,|v_0|\,\dot{\theta}_e + k_3 v_0 l_e \sin\theta_e \frac{1 + k_2\,|v_0|}{\theta_e}\right) \qquad (6)$$

These control law stabilizes the system considering k1 > 0, k2 > -1/|v0|, and k3 > 1. For each fault mode, the control system has the following block diagram as used in [3] .

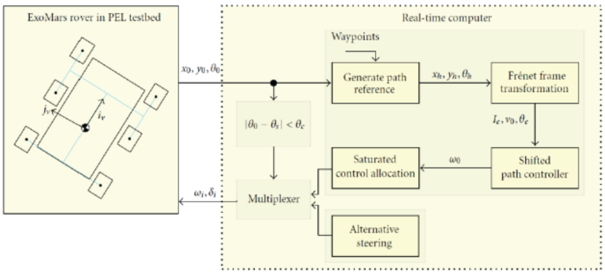


Figure 6. Block diagram of the path following controller in fault mode

The first experiment conducted was considering that steering motors may be blocked. Figure 7 shows the performance of the reconfigured controller compared to the faulty-free plant trying to follow the path.

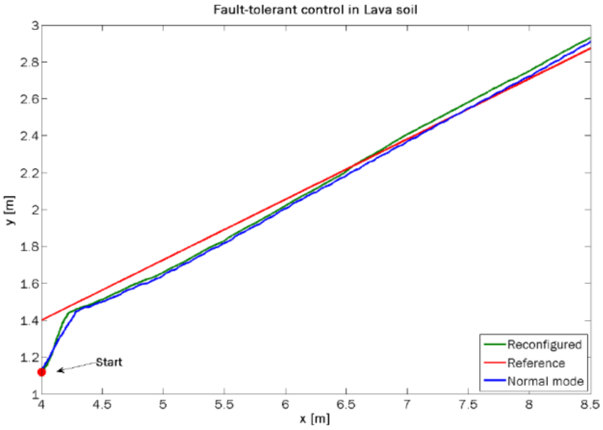


Figure 7. Performance of the fault-tolerant control in the ExoMars Rover under fault in three steering motors driving on lava sand

Even in the presence of three blocked wheels the fault tolerant control system is able to follow the path suitably with negligible performance deterioration. In order to test the control system under a more difficult situation, the same fault was injected during driving on Kalk sand. This is an adverse situation and makes nonlinearities more apparent. Figure 8 shows the comparison between reconfigured (with three steering motors blocked) and normal mode again.

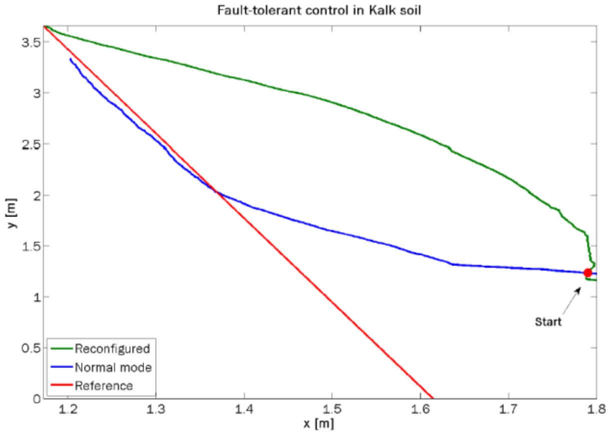


Figure 8. Performance of the fault-tolerant control in the ExoMars Rover under fault in three steering motors driving on kalk sand

5. CONCLUSION AND OUTLOOK

The Dilemma Diagnoser was introduced. The modelling of the problem based on subspace of wrong decisions is not common and treats a subtle question which arises during implementation of fault tolerant controllers. The question is the transition from one operating mode to another. The diagnosis statement has its own transitory effects and does not allow a smooth transition (switching in the case of control reconfiguration) from one controller to another. Considering all uncertainties involved in the decision process a dilemma is identified, no solution seems to be safe enough to assume the risk of immediate switching. A solution is proposed and tested in the case of the ExoMars rover in the testbed of the German Aerospace Center (DLR). A subsequent work is the application of the Dilemma Diagnoser to other vehicles considering a comprehensive fault repertoire and critical situations to apply a fully autonomous fault tolerant control. The current application to wheeled rovers is very useful when a rover drives around craters and has to follow trajectories autonomously with just small deviations from the desired path. This can be extrapolated for contexts of other vehicles and is precisely the idea of future work, integrating detection and coupled diagnosis-reconfiguration.

6. ACKNOWLEDGEMENTS

Parts of the work on rover modelling were performed in conjunction with the HGF alliance project Planetary Evolution and Life (HGF-Helmholtz-Gemeinschaft der Großforschungsanstalten). And parts of the work leading to the development of the rover path-following control have received funding from the European Community’s Seventh Framework Programme (FP7/2007-2013) under Grant Agreement nº 262744. The authors wish to gratefully acknowledge the support by HGF and EC.

7. REFERENCES

1.Nyberg, M., (1999). Model based fault diagnosis: Methods, theory, and automotive engine applications, Ph.D. thesis, Linköpings Universitet.

2. Basar, T. & Olsder, G.J., (1982). Dynamic noncooperative game theory, Academic Press.

3. Leite, A.C., Schäfer, B., Souza, M.L.O., (2012). Fault-Tolerant Control Strategy for Steering Failures in Wheeled Planetary Rovers, Journal of Robotics, vol. 2012, Article ID 694673, 15 pages, 2012. doi:10.1155/2012/694673