2007 IEEE International Conference on
Robotics and Automation
Roma, Italy, 10-14 April 2007

A Comparative Dependability Analysis of Antagonistic Actuation Arrangements for Enhanced Robotic Safety

Roberto Filippini, Soumen Sen, Giovanni Tonietti and Antonio Bicchi*

***Abstract*— In this paper we introduce an analysis of dependability of an elementary yet critical component of robotic systems designed to operate in environments shared with humans, i.e. the joint-level actuation system. We consider robot joints that implement the Variable Impedance Actuation (VIA) paradigm. The VIA has been demonstrated to be an effective mean to achieve high performance while constantly keeping injury risks to humans by accidental impacts below a given threshold. The paper describe possible implementations of the VIA concept which use the Antagonistic Actuation (AA) in three different arrangements. This study follows a previously reported paper dealing with safety. Here a detailed comparative dependability and performability analysis in front of possible specific failure modes is conducted, whose results provide additional and useful guidelines for design of safe and dependable actuation systems for physical human-robot interaction.**

I. Introduction

Need for a robotic assistant is becoming more and more relevant in present day society to elevate the quality of life in degrees varied from the assistance to a disabled person, to the comfort addition to an human being in general ([9]). For such applications involving intimate physical Human-Robot interaction (pHRI) ([4]), new analysis and design tools are clearly needed which go beyond traditional tools in robotics, and focus on attributes such as *safety*, the absence of damages and injuries, *reliability*, the continuity of service, and *availability*, the readiness of service, in a word the comprehensive attribute of *dependability* and *performability* ([1], [12]).

In this paper, we explore the application of such concepts to pHRI by analysing in some depth a critical component of a robotic system that must interact safely with humans. We consider robot joints designed to achieve high performance while constantly keeping injury risks to humans, due to accidental impacts, below a given threshold. To this aim, the **Variable Impedance Actuation** (VIA) approach was introduced in our previous works ([2], [3], [13]), where it has been demonstrated that, by suitably alternating "stiff and slow" and "fast and soft" motion modes, it is possible to obtain a safe yet performing motion for the robot. One notable class of actuations systems that naturally lend themselves to varying impedance are **Antagonistic Actuation** (AA) systems with nonlinear elements - a solution commonly seen in nature, and used in robotics in many instances. The AA systems are more complex in design, construction and operation, if compared to a conventional industrial type rigid robot joint. This increase in design complexity, while turning into a safer system, might affect the dependability attributes and the performance.

This paper aims at analysing and comparing the dependability and the performability of three AA arrangements, in front of possible specific failure modes. They are the simple, the cross-coupled, and the bi-directional AA, which all derive from a more general arrangement, see Fig. 1. This consists of two antagonistically posed prime movers with nonlinear elastic elements to transmit motions to the actuated joint/link. The derived variants differ in the transmission chain and the steering capability (single or bi-directional).

The dependability attributes of interest are the reliability, which is the probability that the system is functioning and ensures the full steering of the link, and the survivability, which is the probability that the system has the control of one steering direction at least. A performance index is identified in the maximum torque available at the link, which is indirectly related to the minimum time of operation (say pick to place task) introduced in related reports of [2], [3], and [13]. Safety is not addressed here. Previous studies [5] have demonstrated by numerical simulations that the system remains safe even with the occurrence of component failures.

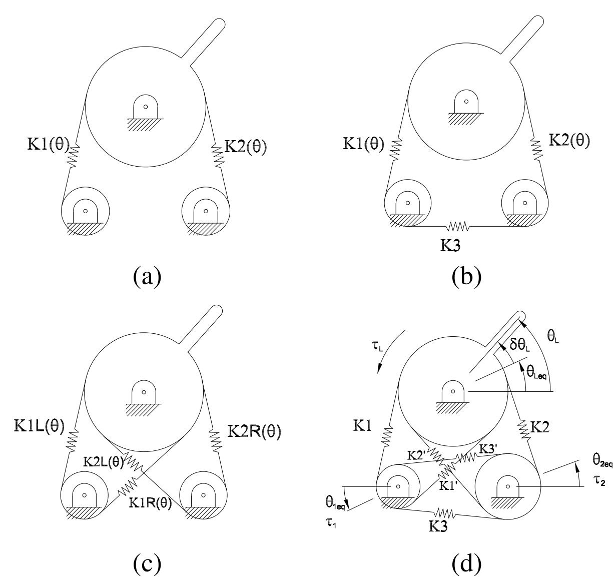

Fig. 1. (a) simple antagonistic arrangement , (b) simple arrangement with cross-coupling, (c) bi-directional without coupling between motors (d) and general arrangement.

* Authors are at the Interdepartmental Research Centre "E.Piaggio", The University of Pisa, 56126 Pisa, Italy. bicchi@ing.unipi.it

II. System Description and Failure Modes

The functional block diagrams corresponding to the mechanical layouts (a), (b) and (c) of Fig. 1 are shown in Fig. 2. For the considered arrangements, it is assumed that all points are positively driven by transmissions (i.e. they are not friction driven) and motors are fully back-drivable. In rest of the text, elastic-transmission and stiffness-element or spring will be used synonymously.

All arrangements consist of a link joint, the actuation-transmission chain and the control module. The control module governs the motion of the link on the basis of the state information of the motors and the link, which are acquired by identical position sensors. In the **simple** AA (Fig. 2 (a)), each actuator transmits the motion to the link via a nonlinear spring K, toward a preferential direction (right or left). When these act together they are able to vary the impedance to make the link-joint either stiff or compliant, with the maximum torque (U) per direction corresponding to the maximum torque generated by one actuator. The **cross coupled** AA (Fig. 2(b)) adds a third spring between the two actuators ([13]) with a twofold role: it provides pre-loading and also permits the full steering of the link by each actuator. Thanks to that, the maximum generated torque per actuator can be set to U/2 to obtain an equivalent maximum torque U at the link-joint. The cross coupled AA has already been realized as reported in [13]. The **bi-directional** AA (Fig. 2(c)) has two springs (viz. K1R, K1L) per actuator instead of one, where each actuator can steer the link toward both directions. Again, it is possible to use smaller actuators of U/2 torque each to obtain an equivalent maximum torque U at the link.

A Failure Modes and Effects Analysis (FMEA) is conducted for the three AA arrangements separately. The FMEA is a standard procedure to obtain the systematic inventory of all failure modes in a system ([7]). The following assumptions define the scope of the analysis for the cases studied.

- The components of the three AA arrangements are assumed identical.
- Failures are assumed to be permanent[1], statistically independent and confined in the component where they develop.
- Failures related to the transmission/reception of the control signals are not considered.

The complete FMEA is omitted here, only a sample is given for the cross-coupled AA, see Table I. Each component is assigned the failure mode, the effect at system level, the coverage and the concerned attributes, reliability, survivability and performability. From the analysis it results that the controls and the link joint are single points of failure for the three arrangements and affect both reliability and survivability. All other faults affect the system performance, turning to be a reliability and survivability concern only if undetected (i.e. surveyed components) or accumulated beyond a certain threshold (i.e. redundant components). The faults masked by redundancy concern the components in the actuation chain (i.e. the actuator motors, the joints and the springs) of the bi-directional and the cross-coupled AA, while no redundancy exists for the simple AA. The detectable faults need continuous surveillance. Once detected, a reconfiguration is triggered to adjusts the controls with respect to the changed operational scenario. Two type of reconfigurations are considered:

- **Reconfiguration R1**: the system is reconfigured after the detected loss of one steering direction. This will avoid to plan motions in the lost steering direction.
- **Reconfiguration R2**: the system is reconfigured after a detected failure of one position sensor. The faulty measure is replaced by an estimate which is calculated from the state information acquired by the other two sensors. A further sensor fault is not tolerated

The reconfiguration facilities belong to a higher level of supervision and fault management. In dependability modeling they are usually represented with a coverage factor ([11], [10]). The coverage is a parameter C ($0 \le C \le 1$), non necessarily constant, which quantifies the ability of detecting the fault and recovering the system to a functioning state. Any unsuccessful reconfiguration, namely the residual $1-C$, is assumed to lead to the system failure.

The illustrated fault tolerance features preserve the basic functionality, though they cannot prevent the degradation of the VIA optimal property. This degradation is quantified as a % reduction of the maximum torque at the link. For example, the failure of one of the two actuator motors (the motor joints must function to transmit the motion) or the failure of the K3 spring are both tolerated in the cross-coupled AA, though they cause a 50% reduction of the maximum torque. The bi-directional AA can withstand more combinations of faults, like the complete failure of one actuation chain (i.e. the motor or both springs) which is tolerated but causes a 50% reduction of the maximum torque. In a similar way, the failure of one of the four springs results in a 50% reduction of the maximum torque for one direction only (left or right), which makes 75% of the total. The failure of one spring (say, KL) in one actuation chain and the opposite spring (say, KR) in the other actuation chain transforms the bi-directional in the simple AA, with a 50% reduction of the maximum torque at the link. Any further accumulation of faults will imply the loss of one steering direction.

III. The Models for the Analysis of the System Dependability

The modeling and the analysis of the system dependability relies on the state based approach ([1], [8]). The failure process is described within a state transition diagram where the failure modes, identified in the previous section, are the random events that govern the state transitions. A general model for all AA arrangements is shown in Fig. 3. It consists of the states (i) ”fault-free”, the macro-states (ii) ”one steering direction” and (iii) ”two steering directions”, and the state (iv) ”failed”. The state ”fault-free” is the initial one. The macro-state ”one steering direction” is reached

[1]Transient and systematic failures are not taken into consideration [1]

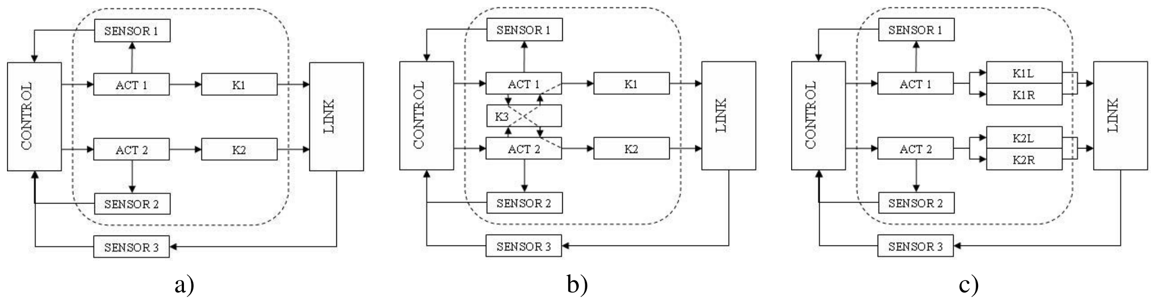

Fig. 2. Functional block diagrams of the simple AA (a), the cross-coupled AA (b) and the bi-directional AA (c).

TABLE I

FMEA OF THE CROSS-COUPLED AA

Component	Failure mode	Effect	Coverage	Attribute
Controls	HW/SW failure	System failure	-	Reliability/Survivability
Link-joint	Breakage	System failure	-	Reliability/Survivability
Sensors	Breakdown or wrong value	Decreased accuracy	Reconfiguration R2	Performance
Actuator motor	Motor breakdown	Reduction of the applied torque	Redundancy	Performance
Actuator joint	Joint-coupling failure	One steering direction lost	Reconfiguration R1	Reliability
Springs K1,K2	Breakage	One steering direction lost	Reconfiguration R1	Reliability
Spring K3	Breakage	Compliant in the rest position	-	Performance

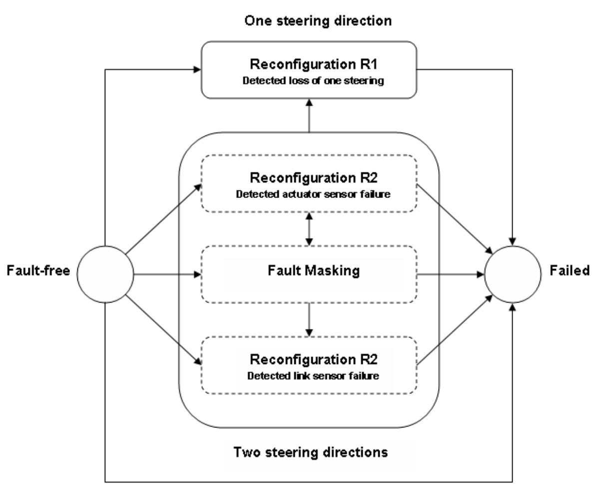

Fig. 3. The general state transition diagram for the AA arrangements.

after the successful reconfiguration R1. The macro-state ”two steering directions” groups the states in which the system has suffered from faults that have not compromised the full steering of the link. Within this state, the system may undergo a reconfiguration R2 due to a detected sensor failure. The ”failed” state acts as a sink for the failure process. Once in it, the system cannot be restored to operation any more.

The dependability attributes of interest are defined on this state space. The *reliability* $R(t)$ is the probability that the system is in ”fault-free” or in the macro-state ”two steering directions” at time t. The *survivability* $SV(t)$ accounts for the probability the system has not failed at time t. The *performability* $\Pi(t)$ quantifies the average maximum torque delivered by the system at time t.

The model of Fig. 4 is a specialization of the general model of Fig. 3 for the cross-coupled AA arrangement. Within the macro-state ”two steering directions”, the states X1 and X5 represent the system that suffered from a detected fault of the link sensor. The states X2 and X6 represent the system that suffered from a detected fault of one actuator sensor. In order to avoid a messy crossing of state transitions, a label with the names of the destination/source states is used, like for the state X3 that has four output transitions to X5, X6, X7 and X8, or for the state X7 that has five input transitions from X0, X2, X3, X4 and X6. Each state is also given a pair of variables that corresponds to the number of actuation chains available per steering direction. This is going to be used for the performability calculation. For example, 2+2 in X0, X1 and X2 means that both actuators have full steering of the link, 2+0 in the state X4 means that one actuator (it does not matter which one) can apply its contribution toward both directions with the other actuator being failed, 1+1 in the state X3, X5 and X6 means that there is one actuator per steering direction. For both cases the maximum torque drops to 50% the nominal value. The simple AA is modeled in the same state transition diagram by assuming X3 as the initial state. The bi-directional AA is a bit more complex but conceptually identical to the model of Fig. 4 [6].

The state transitions are governed by the occurrence of faults in the system, which are concurring random events. The resulting stochastic process is a Continuous Time Markov Chain (CTMC) [11]. This draws a probability distribution $\mathbf{p}(t)$ in the finite space X of N states, calculated with the following Kolmogorov equations:

$$\frac{d}{dt}\mathbf{p}(t) = \mathbf{p}(t)\,(Q_1 + Q_2) \quad (1)$$

where $\mathbf{p}(t) = [p_0(t), p_1(t), \ldots, p_N(t)]$, with $\sum p_i(t) = 1$ and $p_i(t) \geq 0$, $\forall i = 0 \ldots N$, $t \geq 0$. Q_1 is the transition rates matrix of the actuation chain. Q_2 is the transition rates matrix

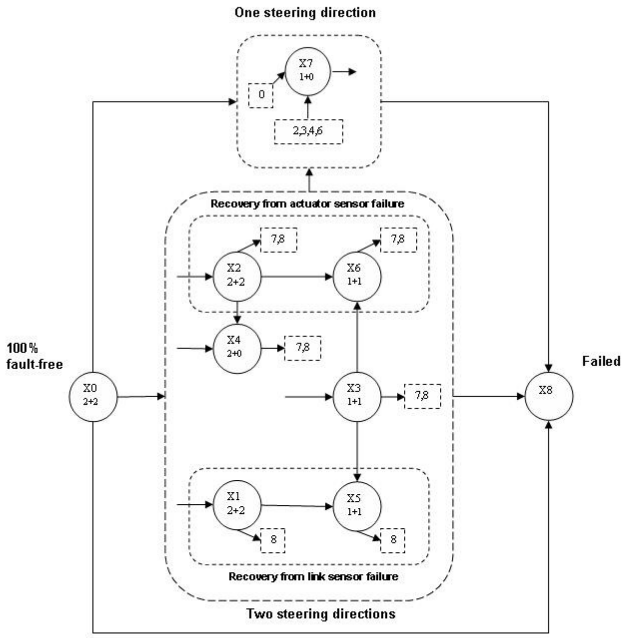

Fig. 4. State transition diagram of the cross-coupled AA.

for the control module and the link and it is conceptually identical for the three cases studied. The two matrices for the model of Fig. 4 are defined below:

$$Q_1 = \begin{pmatrix} -\lambda_0 & \lambda_{01} & \lambda_{02} & \lambda_{03} & \lambda_{04} & 0 & 0 & \lambda_{07} & \lambda_{08} \\ 0 & -\lambda_1 & 0 & 0 & 0 & \lambda_{15} & 0 & 0 & \lambda_{18} \\ 0 & 0 & -\lambda_2 & 0 & \lambda_{24} & 0 & \lambda_{26} & \lambda_{27} & \lambda_{28} \\ 0 & 0 & 0 & -\lambda_3 & 0 & \lambda_{35} & \lambda_{36} & \lambda_{37} & \lambda_{38} \\ 0 & 0 & 0 & 0 & -\lambda_4 & 0 & 0 & \lambda_{47} & \lambda_{48} \\ 0 & 0 & 0 & 0 & 0 & -\lambda_5 & 0 & 0 & \lambda_{58} \\ 0 & 0 & 0 & 0 & 0 & 0 & -\lambda_6 & \lambda_{67} & \lambda_{68} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda_7 & \lambda_{78} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (2)$$

$$Q_2 = (\lambda_{CONTROL} + \lambda_{LINK}) \times$$
$$(-I + [1,1,1,1,1,1,1,1,1]^T \times [0,0,0,0,0,0,0,0,1]) \quad (3)$$

where I is the 9×9 identity matrix, $\lambda_{CONTROL}$ and λ_{LINK} are the failure rates of the control module and the link respectively. The diagonal elements of Q_1 are:

$$\begin{cases} \lambda_0 = \lambda_{01} + \lambda_{02} + \lambda_{03} + \lambda_{04} + \lambda_{07} + \lambda_{08} \\ \lambda_1 = \lambda_{15} + \lambda_{18} \\ \lambda_2 = \lambda_{24} + \lambda_{26} + \lambda_{27} + \lambda_{28} \\ \lambda_3 = \lambda_{35} + \lambda_{36} + \lambda_{37} + \lambda_{38} \\ \lambda_4 = \lambda_{47} + \lambda_{48} \\ \lambda_5 = \lambda_{58} \\ \lambda_6 = \lambda_{67} + \lambda_{68} \\ \lambda_7 = \lambda_{78} \end{cases} \quad (4)$$

Each λ_k is the output rate of state Xk, which is the sum of all rates in the row k, according to the balance equation of the Markov chain. All states are transient (i.e. $p_i(t) = 0$ for $t \to \infty$, $i = 0 \ldots 7$) with the exception of X8 that is absorbing (i.e. $p_8(t) = 1$ for $t \to \infty$). The equation (1) is solved for the initial condition of $\mathbf{p}(t)$ at t = 0.

Reliability, survivability and performability for the model of Fig. 4 are defined as follows:

1) The system is reliable if $x(t) \in \{X0,\ldots,X6\}$.

$$R(t) = 1 - p_7(t) - p_8(t) \quad (5)$$

2) The system has survived in all states with the exception of the state X8.

$$SV(t) = 1 - p_8(t) \quad (6)$$

3) The performance $\Pi(t)$ returns the average maximum torque in X.

$$\Pi(t) = p(t)\pi^T = \sum_{i=0\ldots8} p_i(t)\pi_i \quad (7)$$

where $\pi = [\pi_0, \ldots, \pi_8]$ is the reward vector and π_k is the % of the maximum torque available at the link in the state k. Further details on the model building can be found in [6].

IV. Dependability Analysis

A. The Default Case Study

The analysis has been conducted for the three AA arrangements under the following assumptions:

- (A1): the failure rates are assumed to be constant;
- (A2): the coverages $C1$ and $C2$ for the reconfigurations R1 and R2 are assumed to be constant;
- (A3): the failure of the control module and the link joint are not included in the analysis, that is $Q_2 = 0$.

The assumed values for the failure rates and the coverage for the three models are listed in Table II. These figures are not related to any experimental evidence and only serve as dataset for the comparison. For the cross-coupled AA only, the failure rate of the actuator is equally apportioned to the motor failure (λ_{MOT}) and the joint coupling failure (λ_{JC}), the former affecting performance, the latter reliability.

The transition rates of Q_1 are function of the components failure rates. As an example, the transition rate λ_{37}, which links X3 to X7, is defined as $\lambda_{37} = C_1(2\lambda_K + 2\lambda_{MOT} + 2\lambda_{JC})$. The rates of failure modes leading to the loss of one steering direction are added up because mutually independent and multiplied by the reconfiguration coverage. The other transition rates are derived in a similar way [6]. The initial state probabilities and the reward vectors are defined for each model separately. For example, the initial state probability vector for the model of Fig. 4 is $\mathbf{p}(0) = [1,0,0,0,0,0,0,0,0]$ and the reward vector is $\pi = [100,100,100,50,50,50,50,0,0]$. The simple AA is analysed on the same model by assuming $\mathbf{p}(0) = [0,0,0,1,0,0,0,0,0]$ and $\pi = [0,0,0,100,0,100,100,0,0]$.

Results for reliability, survivability and performability are shown in Fig. 5, 6 and 7 for a time interval of 10000 h. As reasonably expected, the bi-directional is the most reliable of the three AA arrangements. This is also attested by the calculation of the mean time to failure, which is defined as $MTTF = \lim_{t\to\infty} \int_0^t R(\tau)d\tau$ [7]. The MTTF is 4.1 years for the bi-directional AA, 2.7 years for the cross-coupled and 2.4 years for the simple AA. The bi-directional AA has also resulted in a larger probability of surviving and a larger performance than the other two arrangements.

TABLE II

PARAMETERS SETTING FOR THE ANALYSIS.

Failure rate	Failures per hour
$\lambda_{ACT} = \lambda_{MOT} + \lambda_{JC}$	$10^{-5} = \frac{1}{2}10^{-5} + \frac{1}{2}10^{-5}$
λ_K	10^{-5}
λ_{SENSOR}	10^{-5}
Coverage	**Value**
C_1	1
C_2	1

The simple AA is slightly more performing than the cross-coupled, though it is less reliable. This can be explained by the fact that the cross-coupled AA applies half the torque per actuator, i.e. U/2 instead of U. For a larger capacity of the actuator motors, the cross-coupled would turn to be better in performance too than the simple AA.

B. Sensitivity Analysis

The sensitivity analysis is conducted with respect to the coverages C1 and C2. Four scenarios are analysed, which are obtained for C1 and C2 either 1 or 0, where 1 means that the reconfiguration is included and 0 means that is not. The results are calculated for t = 10000 h and plotted in Fig. 5, 6 and 7. For the three AA arrangements, reliability and performability are sensitive to C2 as shown in Fig. 5 (right) and Fig. 7 (right). On the contrary, for the cross-coupled and the simple AA arrangements the survivability is less sensitive to C2 than to C1, see Fig. 6 (right). The lines joining the four points are just to make the plots more readable and they do not correspond to any intermediate value.

V. CONCLUSIONS

This paper has presented the study of dependability and performability of an actuation mechanism for safe cooperating human-robot applications. As case studies, three antagonistic actuation arrangements (simple, cross-coupled and bi-directional) of an intrinsically safe robot link have been considered. The failure modes of the various components have been identified through FMEA and arranged into a state transition diagram for the description of the system failure processes. Two dependability attributes have been considered: the reliability, which is the probability of steering the link in both directions, and the survivability, namely the probability of keeping the control of the link in one direction at least. The maximum torque available at the link has been taken as a performance index. The model has been analysed for a given operational scenario, assuming that the system is continuously working and no repair is possible. The bi-directional AA has resulted the most dependable and performing architecture, followed by the cross-coupled AA. An additional sensitivity analysis has demonstrated that the calculated dependability attributes and performance strongly depend on the fault detection and reconfiguration facilities, which are the basic constituents of a fault management strategy.

Some extensions of this study are envisaged in order to get further evidence on benefits and drawbacks of the various design alternatives. In particular, the design should take into consideration the costs associated to each solution. In this respect, the cross-coupled AA could represent a better compromise between dependability and costs than the more complex bi-directional AA. The results also depend on the functioning of the control system and the link, which have not been considered in the study. The inclusion of other parts of the system will likely complicate the model and its analysis. Nevertheless, under certain assumptions and reasonable approximations, the modeling approach can be scaled up and applied to more complex robotic structures. To this end, an important requirement is to verify that the various parts develop independently their failure process thus enabling separate modeling and analysis.

In conclusion, as a perspective direction of research, the dependability and safety issues, addressed here and in [5] respectively, could be reformulated in a larger comprehensive framework. The new study will make it possible to calculate the minimum time of the VIA as a function of maximum torque available at joint, which is one of the results of this paper. Furthermore, the optimal performance for the VIA will depend on the system failure process and, importantly, on the inherent fault tolerance for a more effective evolution of the design alternatives.

VI. ACKNOWLEDGEMENTS

This work is supported by the Prospective Research Project PHRIDOM as part of the FP6-2002-IST507728 Network of Excellence EURON, and by the FP6-2006-IST045359 Specific Targeted Research or Innovation Project PHRIENDS.

REFERENCES

[1] A. Avizienis, J. Laprie, B. Randell and C. Landwehr, *Basic Concepts and Taxonomy of Dependable and Secure Computing*, IEEE Transactions on Dependable and Secure Computing, vol. 1, No. 1, pp. 11-33, January/March 2004.

[2] A. Bicchi and G. Tonietti, *Fast and Soft Arm Tactics: Dealing with the Safety–Performance Tradeoff in Robot Arms Design and Control*, IEEE Robotics and Automation Magazine, Special Issue on "Safety Among Us", Vol.11, No.2, June, 2004.

[3] A. Bicchi and S. Lodi Rizzini and G. Tonietti, *Compliant Design for Intrinsic Safety: General Issues and Preliminary Design*, Proc. Int. Conf. on Rob. Sys., IROS 2001, Maui, Hawaii.

[4] A. Bicchi, E. Colgate, M. Peshkin, *Physical Human-Robot Interaction*, to appear in the "Handbook of Robotics", O. Khatib, B. Siciliano (eds.), Springer Verlag, 2006.

[5] G. Boccadamo, R. Schiavi, S. Sen, G. Tonietti and A. Bicchi, *Optimization and Fail-Safety Analysis of Antagonistic Actuation for pHRI*, In Henrik I. Christensen, editor, European Robotics Symposium 2006, volume 22 of Springer Tracts in Advanced Robotics, pages 109 - 118. Springer Berlin / Heidelberg, 2006.

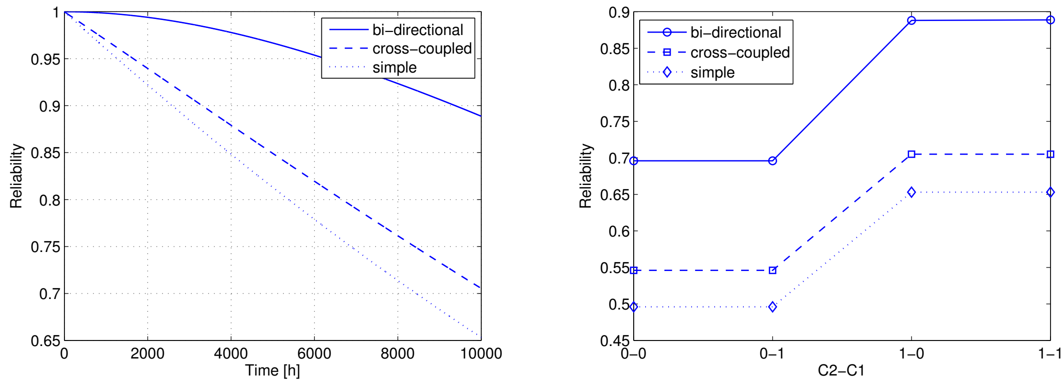

Fig. 5. Reliability (left), and related sensitivity (right) at t = 10000 h with respect to C1 and C2, for the different arrangements.

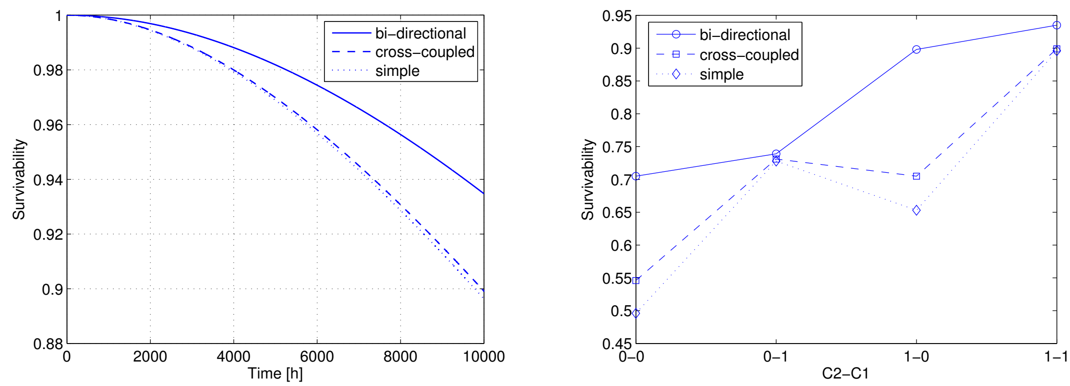

Fig. 6. Survivability (left) and related sensitivity (right) at t = 10000 h with respect to C1 and C2, for the different arrangements.

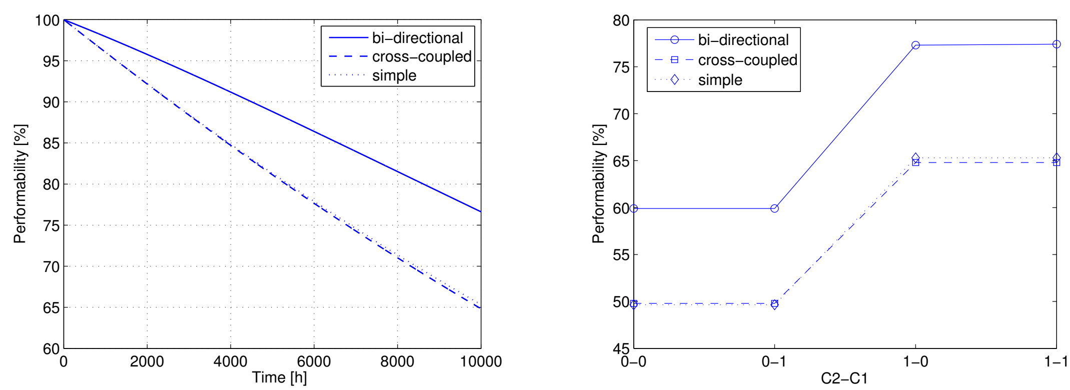

Fig. 7. Performability (left) and related sensitivity (right) at t = 10000 h with respect to C1 and C2, for the different arrangements.

[6] R. Filippini, *A dependability study for safe co-operating robot applications*, Technical Report, Interdepartmental Research Center E. Piaggio, Pisa, 2006.

[7] A. Hoyland and M. Rausand, *System Reliability Theory: Models and Statistical methods*, 2^{nd} edition, Wiley, New York, 2005.

[8] J. Muppala, R. Fricks, and K. S. Trivedi, *Techniques for System Dependability Evaluation*, in Computational Probability, W. Grassman (ed.), pp. 445-480, Kluwer Academic Publishers, The Netherlands, 2000.

[9] M. Peshkin et al., *T15.1 Draft Standard for Trial Use for Intelligent Assist Devices - Personnel Safety Requirements*, Robotic Industries Association, 2002

[10] D. Powell, *Failure Mode Assumptions and Assumption Coverage*, Proceeding of the 22th Annual International Symposium on Fault Tolerant Computing FTCS 22, pp. 386-395, IEEE, Boston, MA, USA, July 1992.

[11] K.S. Trivedi, *Probability and Statistics with Reliability, Queuing and Computer Science applications*, 2^{nd} edition, Wiley, New Jork, 2002.

[12] K.S. Trivedi, G. Ciardo, M. Malhotra, R. Sahner, *Dependability and Performability Analysis, Performance Evaluation of Computer and Communication Systems*, Lecture Notes in Computer Science, L. Donatiella, R. Nelson (eds.), pp. 587-612, Springer-Verlag, 1993.

[13] G. Tonietti and R. Schiavi and A. Bicchi, *Design and Control of a Variable Stiffness Actuator for Safe and Fast Physical Human/Robot Interaction*,In Proc. Int. Conf. on Rob. and Auto., 2005, pp.528-533.