Toward Soft Robots You Can Depend On

©PUNCHSTOCK

A Study of Antagonistic Actuation

BY ROBERTO FILIPPINI, SOUMEN SEN, AND ANTONIO BICCHI

Digital Object Identifier 10.1109/MRA.2008.927696

Physical human–robot interaction (pHRI) represents one of the most motivating, challenging, and ambitious research topics in robotics. Many of the future and emerging applications of robotics, be they in service [14], assistance and care [23], rehabilitation [34], or in more traditional working contexts [34], will indeed require robots to work in close vicinity if not in direct contact with humans.

A robot for pHRI applications must be regarded in all aspects as a safety-critical system, as it has been unfortunately proven several times in the past that conventional robots can be dangerous or even deadly machines [33]. Since the very beginning of industrial robotics, a great deal of attention has been paid to robot safety, the first line of defense having always been to take all measures to enforce segregation between robots and people [5], [40]. As market pressures together with ethical concerns are about to topple some of the barriers separating robots and people, safety standards are evolving. The 2006 revision of the ISO10218-1 standard [21], for instance, introduces more advanced concepts than in the past, such as the idea of a collaborative operation between humans and robots, and the replacement (albeit to a very limited, conservative extent) of fixed rules with risk assessment procedures. More generally, for applications involving pHRI, analysis tools are needed that are classical in the literature on critical systems [2], [38] but are still rather new in robotics [9], [10], [13], [42]. These tools focus on the attributes of 1) safety, i.e., the absence of damages and injuries; 2) reliability, the continuity of service; and 3) availability, the readiness of service; in a word, the comprehensive attribute of 4) dependability. The goal of this article is to begin an in-depth study of the dependability of robots for pHRI, starting with the analysis of an elementary, yet critical, robot component, i.e., the joint-level actuation subsystem.

As an answer to the need to build robots that can provide useful performance while guaranteeing safety against all odds, engineers have proposed several innovative solutions to overcome the classical paradigm "rigidity by design, safety by sensors and control," which is more suited for conventional industrial robotics, and are shifting toward a "safety by design, performance by control" philosophy [1], [14], [18]. In our own previous work [3], [4], variable stiffness actuation (VSA) and its generalization in variable impedance actuation (VIA) have been demonstrated to be effective in obtaining a safe yet performing robot motion by swiftly alternating stiff-and-slow and fast-and-soft motion modes. Indeed, in high-velocity impacts, low-joint impedance can effectively decouple the link's inertia from the actuator's reflected inertia, which is typically large due to the transmission gear ratio. Although the investigation of VIA, including variable damping [11], [25], [29], [31] and/or gear ratio, is a very promising research direction, as of today there are only very few examples of general VIA systems for robotics applications. On the contrary, a number of different prototypes exist that can vary the transmission stiffness [8], [22], [32], [43]. Among these, we focus on VSA mechanisms whereby joint stiffness values can be continuously varied as a function of joint velocities. This is

1070-9932/08/$25.00©2008 IEEE

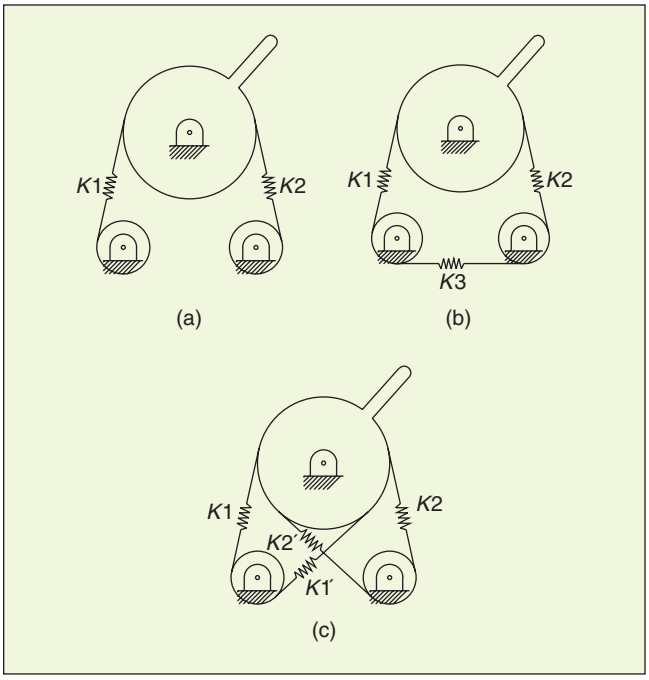

Figure 1. *Three possible arrangements for AA: (a) simple, (b) cross coupled, and (c) bidirectional.*

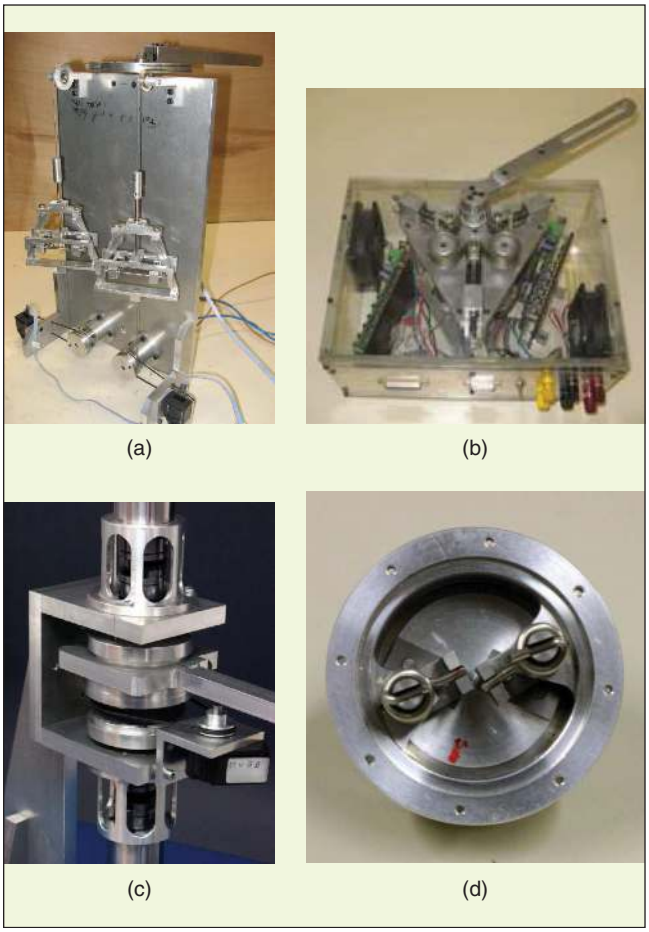

Figure 2. *Laboratory prototypes of three AA arrangements: (a) simple AA with exponential springs, (b) cross-coupled arrangement of the VSA-I, (c) bidirectional arrangement of the VSA-II, and (d) one half of the VSA-II opened up.*

contrasted to other methods that adapt compliance only once for each different task and implies that implementation of VSA requires hardware capable of changing stiffness with a time-constant comparable to that of the mechanics of the rigid robot (i.e., of the order of milliseconds). Furthermore, among several possible solutions to implement the VSA idea, we focus our attention here on the notable class of antagonistic actuation (AA) systems. Agonist-antagonist actuator pairs are commonly seen in nature and have been studied in biomechanics as well as robotics for a long time [15]. Artificial AA systems are more complex in design, construction, and operation when compared with conventional rigid robot joints. This increase in design complexity, while useful for achieving a safer system in nominal conditions, might affect the dependability attributes and the performance in the presence of faults.

This article describes possible implementations of the VSA concept via three different arrangements of the agonist-antagonist actuation scheme. A detailed comparative dependability analysis of possible specific failure modes is conducted, whose results provide insights on the design of the actuation mechanism and of fault management (FM) layers, including fault detection and identification (FDI), system reconfiguration, and fail-safe emergency stops, to provide the ability of tolerating faults and continuing safe operations.

AA Arrangements

In its simplest implementation, an AA arrangement consists of two prime movers connected to the moving element (link) through two nonlinear elastic elements [see Figure 1(a)]. Rotation of the motors in the same sense generates a net torque to the joint, while rotations in the opposite sense set different levels of effective compliance at the joint. Depending on the implementation, prime movers can be regarded as either torque or position sources, and elastic transmissions can have different characteristics. We assume that motors have much higher reflected inertia at the joint axis than the link itself, due to the fact that in robotic applications high gear ratios are often used (gears are included in the prime-mover element in our analysis). We also consider unidirectional (tendon-like) transmission elements. A laboratory implementation of a simple AA arrangement is depicted in Figure 2(a).

A closer inspection of the musculoskeletal system in humans shows that not all articulations are actuated by an arrangement of agonistic–antagonistic muscles analogous to this simple case: indeed, more muscles are involved, and couplings exist between the actuation of different joints. From an engineering viewpoint, simple AA arrangements might not be optimal as well. For instance, if pull-only tendons are considered, the maximum torque available at the joint cannot be more than that of each single motor, and no net torque is available at the joint when stiffness is at the maximum. To overcome this limitation, a possible modification is to introduce a third elastic element (possibly different from the two antagonists) to cross couple the two prime movers [see Figure 1(b)]. Cross coupling allows setting preload forces in the system to tune it to nominal working conditions and using (a fraction of) each motor's torque in both directions. The VSA-I prototype introduced in [37] and depicted in Figure 2(b) is an implementation of this concept.

One further variation of the basic AA arrangement, which addresses the issues of unidirectional actuation not using cross coupling, consists of connecting each actuator to the link via two elastic elements (not necessarily symmetric) in the push-pull configuration [see Figure 1(c)]. The VSA-II prototype introduced in [35] and depicted in Figure 2(c) implements such a bidirectional AA arrangement. Figure 2(d) is a view of one half of the VSA-II mechanism. One motor is connected to the inner pulley (marked in red), while the link is fixed to the outer shells of the two halves. Two elastically preloaded four-bar mechanisms are visible, which are used to connect bidirectionally the motor to the outer shell.

Mechanics and Control Codesign

We chose to design the actuation arrangements considered in this article by the mechanical/control codesign approach that was illustrated in [3]. The basic idea is to select the mechanical elements (springs and motors) and design the nominal (open-loop) input functions so as to optimize performance while guaranteeing that a given risk threshold is never exceeded during the robot motion. This is a variational optimization problem (the so-called safe brachistochrone), which can be solved numerically. The evaluation of the safety threshold is done through extensive simulation runs of impacts of the moving link with a human, occurring at different velocities and for different values of joint stiffness. The impact effects were quantified using the head injury coefficient (HIC) [41]. It should be noted that the HIC criterion is not a completely satisfactory index for pHRI if the same metrics are used to measure the injury risk as in car crash tests, as discussed, e.g., in [12]. If HIC values evaluated for robotic impacts are mapped to risks by abbreviated injury scales developed for automotive applications, the results underestimate the consequences. Although other safety metrics are being actively investigated, we, in this study, use the HIC index, assuming that pHRI risks are proportional to HIC by a scaling factor still to be evaluated empirically. Confusion may occur about the units of measure for HIC. In SI units, HIC is measured in $m^{2.5}/s^4$. If acceleration is measured in $g = 9.81\ m/s^2$, instead, then HIC is measured in seconds. A factor of $g^{5/2} \approx 300$ applies between HIC values in different units. Automotive crash test literature typically uses the latter units. We use SI units in this article.

A substantial difference between the safe brachistochrone characterization in [3] and its application to the AA arrangements considered is that here the variation of stiffness cannot be achieved instantaneously (as it was in the ideal model in [31]), and its rate is limited by the available actuator torque and inertia. Furthermore, we take into account the dissipative effect of back electromotive force.

Interestingly enough, the basic result of the safe brachistochrone study remains valid in these more realistic conditions and for the different design configurations encountered in the AA implementations described here: the minimum-time control of a VSA under strict safety constraints consists of alternating stiff-and-slow and soft-and-fast motion modes. As an illustrative example, the numerical results for the safe brachistochrone optimization of the cross-coupled AA arrangement are shown in Figure 3.

Modeling for Dependability Assessment

The behavior of a system under unexpected conditions or failures is the main subject of dependability engineering. A system is said to be dependable when its service can be justifiably

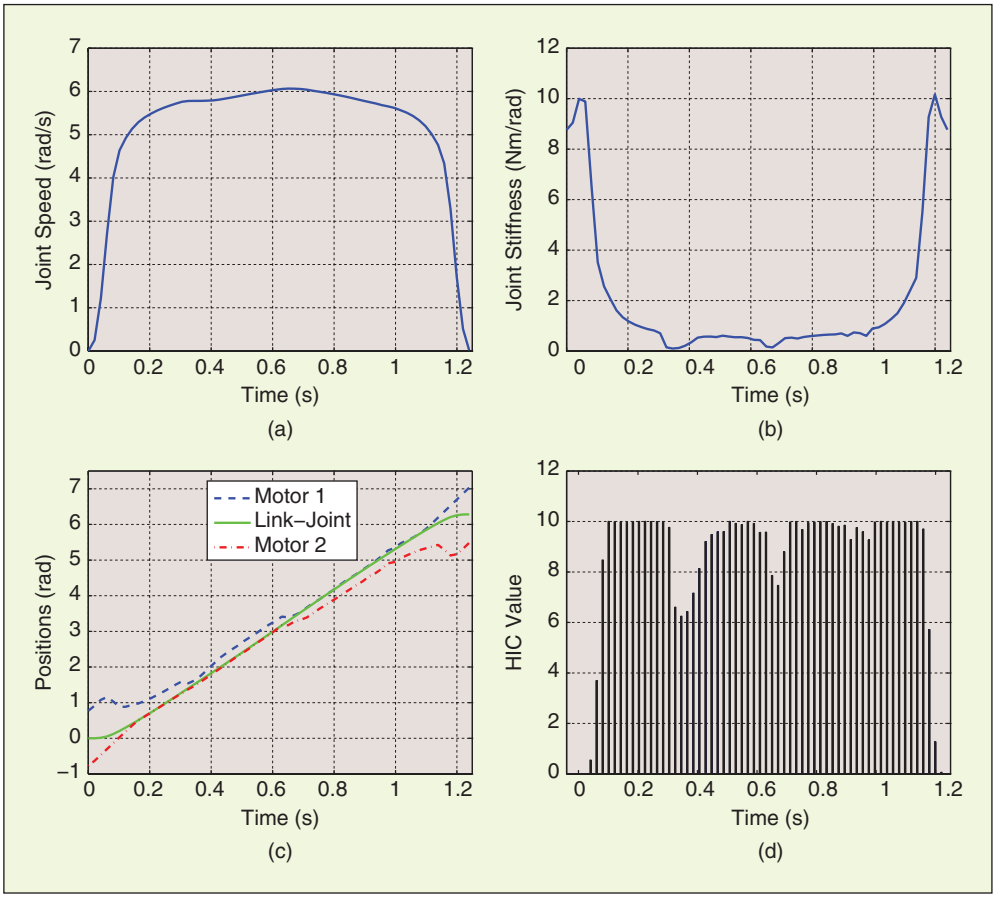

Figure 3. *Numerical optimization results for the codesign of a cross-coupled AA arrangement implementing joint variable stiffness. (a) The link goes through an approximately trapezoidal velocity profile. (b) Stiffness is correspondingly high in the initial and final phases of motion, and low in between. (c) Agonist and antagonist actuators are shown in action in the different phases. (d) The optimized HIC values during motion tend to the acceptable limit (here set to 10 $m^{2.5}/s^4$).*

trusted over well-stated operational conditions and a given time interval. This general definition specializes into several attributes [24]. The most important ones include

1) safety or the absence of catastrophic effects of failures
2) reliability or the continuity of service
3) availability or the readiness of service.

A dependability assessment study typically starts with the failure modes and effects analysis (FMEA) and returns a random variable for the dependability attribute, with its distribution and statistics (e.g., average and variance). For instance, the mean time to failure (MTTF) and the mean time between failure (MTBF) are often used as statistic indicators for reliability and availability, respectively.

Methods for dependability assessment (modeling and analysis) are basically split into 1) combinatorial (e.g., fault trees, reliability block diagrams) and 2) state based (e.g., Markov chains, Petri nets). Combinatorial approaches typically return the probability of an event, e.g., the overall system failure, in a rather computationally efficient way, which is useful for the analysis of complex systems. State-based approaches instead return a richer description of the whole failure process, from the fault-free state to the system failure state, including the transitional states. When this description is required, state-based approaches prove to be more powerful and lend themselves to the evaluation of more detailed failure scenarios, including the effect of fault tolerant design and periodical inspections. In this article, we will adopt the state-based approach to analyze the dependability of rather simple joint actuation arrangements introduced previously.

Failure Modes and Fault Management

The FMEA is a tool for identifying the failure modes in a system and for reporting the causes on the basis of their occurrence and the general effects on the delivered function [16]. While FMEA analysis can be very detailed, we use it here only to establish a principled but reasonably simple failure model of the three AA arrangements under consideration (see Figure 1).

To this purpose, the following assumptions are made:

- Faults are statistically independent random processes.
- The occurrence of a fault in a component causes the sudden transition from a fully functional to a failed state.
- Faults are permanent. Slow performance drifts and transient and systematic failure modes are not considered.

To further limit the complexity of an FMEA for the three AA arrangements under consideration, we restrict our consideration to only two elementary components, i.e., motors and elastic transmission elements (referred to as springs, although they might not be realized as such in practice). The control and electronic power amplifier system is included in the motor FMEA model.

Motors are assumed to fail either by a controller fault (whereby in the worst case the shaft torque defaults to its maximum value) or by a mechanical gear breakdown, with the axis getting stuck at a fixed position or breaking loose. Springs breakage causes zero torque to be transmitted through the corresponding elastic element.

For a critical system such as a pHRI robot joint, some measures of FM should be taken to minimize the effects of faults. In our examples, we postulate a simple FM control layer, which consists of a series of three independent modules: sensors, internal logic, and recovery actions. Sensors pick up motor current and position signals, which are processed by the FDI logic, whose role is to track state changes in the joint actuation mechanism. Recovery actions are issued accordingly, either by system reconfiguration or fail-safe emergency stop.

Because we assume that VSA joints are controlled to track optimal safe velocity-stiffness references (planned, e.g., by the safe brachistochrone method), an FM action is necessary to restore the system to a functioning state or to stop it safely [27], [42]. For example, a spring failure in the bidirectional arrangement alters the mechanism stiffness and the effective impacting inertia at the link. To avoid risks in the subsequent operations, the system should be reconfigured to reset its internal stiffness value according to the optimal VSA solution in the new conditions.

Three types of reconfigurations are considered to restore the functioning of the system automatically, before repair intervention. A reconfiguration of the R1 type copes with the failure scenarios by which it is possible to recover control of both the link motion and stiffness, albeit at the cost of some performance loss (e.g., due to a reduced stiffness variation range). The breakage of the preloading spring in the cross-coupled AA and of one of the springs in the bidirectional AA are such scenarios. A second type of reconfiguration (R2) is applied when the steering of the link is not compromised, although stiffness cannot be controlled any longer. Controls are switched into the non-VSA mode in order that the system may continue to operate safely at a reduced velocity. Finally, a reconfiguration of the third type (R3) simply uses the residual functioning elements of the system to reduce the elastic energy stored in the system, before shutting down to a fail-safe stop. This fail-safe operation abort by emergency stop is issued if the detected failure is critical for safety or reconfiguration has failed.

The list of failure modes for the three arrangements illustrated in Figure 1 is shown in Table 1. Each component is assigned a failure mode, the effect is provoked at the system level, and the type of coverage action is provided by an FM system. The reported effects correspond to each fault occurring singularly.

State-Based Model

The last changes caused by the occurrence of single faults and sequences of faults with the respective recovery actions are accommodated in a state transition diagram, evolving as a discrete event system [6].

In total, the following five states are identified:

1) *Fault free*: The system functions normally.
2) *Recovered with VSA*: After successful reconfiguration, the system controls both the link motion and stiffness.
3) *Recovered without VSA*: After successful partial reconfiguration, the system controls the link position but not its stiffness.
4) *Fail-safe stop*: The system has been detected as failed and the operation stops.
5) *System failure*: The system has failed in operation.

The last state is reached in worst-case situations where a reconfiguration or fail-safe stop action may itself fail.

System dependability attributes are defined on subsets of the state space X. Thus, reliability is the probability of conserving the VSA function, namely of being in states $X_R =$

$\{$*fault free*, *recovered with VSA*$\}$. We introduce the term *steerability* to indicate a partial reliability attribute, for the system conserving the steering function possibly without stiffness (VSA) control. In other words, steerability is the probability of being in $X_{S_T} = X_R \cup \{$*Recovered without VSA*$\}$. The system is expected to be safe in the reliable states, in the *recovered without VSA* state and in the fail-safe stop state, namely $X_S = X_{S_T} \cup \{$*Fail-safe stop*$\}$ (compare later simulation results in the "Safety" section).

The state-based dependability models for the three AA arrangements are shown in Figure 4(a)–(c). The definitions of the states are described in Table 2. Cases where one motor axis gets stuck due to gear-box breakage lead immediately to failure (possibly through the R3 reconfiguration) and are not further discussed here. A 0 in a motor column, hence, indicates a loose joint, while 1 indicates correct functioning. Symmetric failure conditions in the considered systems are aggregated in a single state in the diagrams. A label with the names of the destination or source states is used in place of arcs to keep the description as compact as possible. For example, in Figure 4(c), the state X_3 has two labeled output transitions to states X_6 and X_7 and one labeled input transition from state X_0. Each state is also described by two entries spaced by the symbol || indicating for each motor whether it can apply bidirectional torques to the link (value 2), unidirectional (value 1), or no torque at all (value 0).

For all models, the actions issued by FM are successfully accomplished with a certain probability that depends on the correct execution of the fault-handling process, i.e., the sequence of detection, identification, and recovery [7], [20]. This probabilistic model is represented by a coverage factor C, which is a number that ranges between 1, in case the fault is certainly covered, and 0, if that fault is certainly not covered [39]. The noncoverage fraction $1 - C$ accounts for missed detections and/or improper reconfigurations, which lead to the *system failure* state.

Failures and recovery actions draw stochastic processes in X which, in our consideration, can be modeled by a continuous time Markov chain (CTMC) [39]. A CTMC is described by a state probability vector $p(t) = [p_0(t), \ldots \; p_{N-1}(t)]$, $p_i(t) \geq 0$, $\forall i = 0 \ldots \; N-1$, and $\sum p_i(t) = 1$. Here $p_k(t)$ is the probability that the system is in state X_k at time t. The probability distribution $p(t)$ evolves according to Kolmogorov's equation

$$\frac{d}{dt}p(t) = p(t)Q, \tag{1}$$

for $t \geq 0$, with initial conditions $p(0)$. The transition rate matrix Q, corresponding to the Laplacian of the transition graph, is specified for the three different models as follows.

1) Simple AA $Q_{\text{Simple}} =$

$$\begin{pmatrix} -\lambda_0 & \lambda_{01} & \lambda_{02} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \tag{2}$$

2) Cross-coupled AA $Q_{\text{CC}} =$

$$\begin{pmatrix} -\lambda_0 & \lambda_{01} & \lambda_{02} & \lambda_{03} & \lambda_{04} \\ 0 & -\lambda_1 & 0 & \lambda_{13} & \lambda_{14} \\ 0 & 0 & -\lambda_2 & \lambda_{23} & \lambda_{24} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{3}$$

3) Bidirectional AA $Q_{\text{Bid}} =$

$$\begin{pmatrix} -\lambda_0 & \lambda_{01} & 0 & \lambda_{03} & \lambda_{04} & 0 & 0 & \lambda_{07} \\ 0 & -\lambda_1 & \lambda_{12} & 0 & \lambda_{14} & 0 & \lambda_{16} & \lambda_{17} \\ 0 & 0 & -\lambda_2 & 0 & \lambda_{24} & 0 & \lambda_{26} & \lambda_{27} \\ 0 & 0 & 0 & -\lambda_3 & \lambda_{34} & \lambda_{35} & \lambda_{36} & \lambda_{37} \\ 0 & 0 & 0 & 0 & -\lambda_4 & 0 & \lambda_{46} & \lambda_{47} \\ 0 & 0 & 0 & 0 & 0 & -\lambda_5 & \lambda_{56} & \lambda_{57} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{4}$$

The diagonal elements of Q are the sum of the elements in the row, according to the balance of rates entering and leaving each state k, i.e., $\lambda_k = -\sum_{j=0,\neq k}^{N-1} \lambda_{kj}$.

The transition rates of Q are expressions of the component failure rates and of the reconfiguration coverage factors.

Let $\lambda_{M_i^+}$ and $\lambda_{M_i^0}$ denote the number of failures per hour of motor M_i defaulting to maximum torque and to zero torque, respectively, and $\lambda_{M_i} = \lambda_{M_i^+} + \lambda_{M_i^0}$. Let also λ_{K_i} be the failure rate of the nonlinear spring K_i, and $\lambda_{K_i'}$ be the failure rate of the linear spring K_i'.

In the analysis, we have assumed identical motors and symmetrical springs, so that $\lambda_{M_i^+} = \lambda_{M^+}$, $\lambda_{M_i^0} = \lambda_{M^0}$, $\lambda_{M_i} = \lambda_M$, $\lambda_{K_i} = \lambda_K$, and $\lambda_{K_i'} = \lambda_{K'}$. When only one motor or spring among the symmetrical ones is valid, the subscript is omitted.

For example, transition $X1 \longrightarrow X3$ from *recovered with VSA* to *fail-safe stop* for the cross-coupled arrangement is:

$$\lambda_{13} = C_3(\lambda_{K_1} + \lambda_{K_2} + \lambda_{M_1} + \lambda_{M_2}), \tag{5}$$

Table 1. FMEA of the three AA arrangements.

Component	Failure Mode	Effect	Action
Simple AA			
Motor 1 $\wedge$ 2	Maximum torque	Uncontrolled motion	Fail-safe stop
Motor 1 $\wedge$ 2	No torque	Uncontrolled motion	Fail-safe stop
Motor 1 $\wedge$ 2	Stuck	Uncontrolled stiffness	R3
Springs $K1 \wedge K2$	Breakage	Uncontrolled motion	Fail-safe stop
Cross-coupled AA			
Motor 1 $\wedge$ 2	Maximum torque	Uncontrolled motion	Fail-safe stop
Motor 1 $\wedge$ 2	No torque	Uncontrolled motion	R2
Motor 1 $\wedge$ 2	Stuck	Link stuck	R3
Springs $K1 \wedge K2$	Breakage	Uncontrolled motion	Fail-safe stop
Spring $K3$	Breakage	Uncontrolled motion	R2
Bidirectional AA			
Motor 1 $\wedge$ 2	Maximum torque	Uncontrolled motion	R3
Motor 1 $\wedge$ 2	No torque	Uncontrolled motion	R2
Motor 1 $\wedge$ 2	Stuck	Link stuck	R3
Springs $K1 \wedge K2$	Breakage	Uncontrolled stiffness	R1
Springs $K1' \wedge K2'$	Breakage	Uncontrolled stiffness	R1

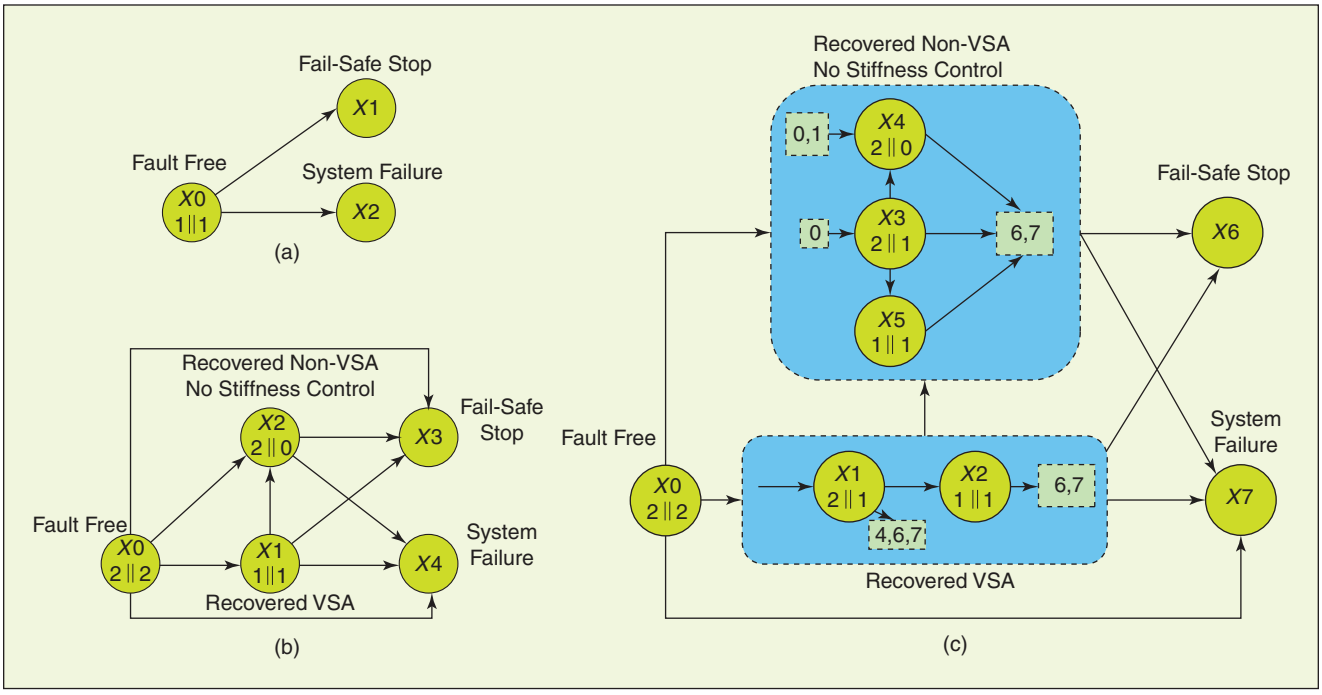

Figure 4. *State-based dependability models of the (a) simple, (b) cross-coupled, and (c) bidirectional AA arrangements.*

Table 2. Description of the functional states.

State	M1	K1	K1′	M2	K2	K2′	K3
Simple AA							
X0	1	1	N/A	1	1	N/A	N/A
X1 and X2	Failure of any further component from state X0						
Cross-coupled AA							
X0	1	1	N/A	1	1	N/A	1
X1	1	1	N/A	1	1	N/A	0
X2	1	1	N/A	0	1	N/A	1
X2(sym.)	0	1	N/A	1	1	N/A	1
X3 and X4	Failure of any further component from states X1 and X2						
Bidirectional AA							
X0	1	1	1	1	1	1	N/A
X1	1	1	1	1	1	0	N/A
X1(sym.)	1	1	0	1	1	1	N/A
X2	1	1	0	1	1	0	N/A
X3	1	1	1	1	0	1	N/A
X3(sym.)	1	0	1	1	1	1	N/A
X4	1	1	1	1	0	0	N/A
X4(sym.)	1	0	0	1	1	1	N/A
X4	1	1	1	0	1/0	1/0	N/A
X4(sym.)	0	1/0	1/0	1	1	1	N/A
X5	1	0	1	1	0	1	N/A
X6 and X7	Failure of any further component from states X2, X3, X4, and X5						

where the coverage factor C_3 accounts for reconfiguration R3 in case of failure of one component among two nonlinear springs and two motors, given spring $K3$ has already failed. Transition $X0 \longrightarrow X1$ from *fault free* to *recovered with VSA* for the bidirectional arrangement is:

$$\lambda_{01} = C_1(\lambda_{K_1'} + \lambda_{K_2'}), \tag{6}$$

where the coverage factor C_1 accounts for reconfiguration R1 in case of failure of one of the two linear springs. An example is also given for transitions that lead to the *system failure* state. Transition $X0 \longrightarrow X2$ from *fault free* to *system failure* for the simple arrangement is:

$$\lambda_{02} = (1 - C_3)(\lambda_{M_1} + \lambda_{M_2} + \lambda_{K_1} + \lambda_{K_2}), \tag{7}$$

where $1 - C_3$ accounts for the missed coverage in case of failure of one component among two motors and two springs.

Failure rates in the expressions are added up because of their assumed statistical independence.

Results

Dependability Analysis Results

The dependability attributes of interest, reliability R, and steerability S_T are defined for the three AA mechanisms as the stochastic variables $R(t)$ and $S_T(t)$, where

- simple: $R(t) = S_T(t) = p_0(t)$
- cross coupled: $R(t) = p_0(t) + p_1(t)$; $S_T(t) = R(t) + p_2(t)$
- bidirectional: $R(t) = p_0(t) + p_1(t) + p_2(t)$; $S_T(t) = R(t) + p_3(t) + p_4(t) + p_5(t)$.

A numerical evaluation of reliability and steerability is conducted under the following assumptions for all models:

1) The component failure rates are constant and equal to 10^{-5} failures per hour.
2) Systems are assumed to be working correctly at the start. Hence, the initial probability vector is $p(0) = [1, 0, \ldots, 0]$.
3) An indefinitely long mission time is specified so that operations only end when the system fails.

In these conditions, the transient analysis of $p(t)$ can be replaced by average statistics [39], in particular MTTF for reliability and mean time to steering failure (MTTSF) for steerability. These quantities can be calculated by applying the final value theorem of the Laplace transform, i.e.,

$$\mathrm{MTTF} = \lim_{t\to\infty} \int_0^t R(\tau)d\tau = \lim_{s\to 0} R(s) \tag{8}$$

$$\mathrm{MTTSF} = \lim_{t\to\infty} \int_0^t S_T(\tau)d\tau = \lim_{s\to 0} S_T(s) \tag{9}$$

where

$$\begin{aligned} R(s) &= p(0)(sI - Q)^{-1}\nu_r \\ S_T(s) &= p(0)(sI - Q)^{-1}\nu_s \end{aligned}$$

with ν_r and ν_s suitably defined according to the above discussion: for instance, for the cross-coupled AA, one has

$$\begin{aligned} \nu_r^T &= [1 \quad 1 \quad 0 \quad 0 \quad 0] \\ \nu_s^T &= [1 \quad 1 \quad 1 \quad 0 \quad 0]. \end{aligned}$$

Three operational scenarios are considered, namely, OP I, OP II, and OP III, which correspond to three different settings of coverage factors $C1$, $C2$, and $C3$. In the first scenario, recovery actions R1, R2, and fail-safe stop always occur when needed ($C1 = C2 = C3 = 1$). In the second scenario, reconfiguration R2 is not available ($C2 = 0$, $C1 = C3 = 1$), while in the third case no reconfiguration is operational, and only the fail-safe stop action is available ($C1 = C2 = 0$, $C3 = 1$). Numerical results for MTTF and MTTSF are reported in Table 3 and illustrated in Figure 5. With the only fail-safe emergency stop and no reconfiguration (OP III), the simple AA is the most reliable arrangement with MTTF = 2.8 years, while the bidirectional AA and the cross-coupled AA are 1.9 and 2.3 years, respectively. The result can be explained by considering that without reconfigurations, the complexity in the design of the bidirectional and cross-coupled arrangements turns out to be a source of unreliability for the system. For example, the breakage of a linear spring affects the trajectory of the link and lowers the reliability. If reconfiguration R1 is performed (OP II), MTTF (as well as MTTSF) becomes 2.8 years for the three AA arrangements. Reconfiguration R2 in scenario OP I ensures an MTTSF of six years for the bidirectional, against four years for the cross-coupled and 2.8 years for the simple arrangement.

Safety

As mentioned earlier, the design of the three VSA actuators has been conducted so that an impact occurring in any phase of their motion would not exceed a given injury risk. However, this guarantee only holds in case the systems are fully functioning. To assess the safety of the mechanism in case of possible faults, the effects of impacts occurring in coincidence with some of the possible mechanical faults must be considered.

As reasonable coverage of all possible cases by actual impact experiments is not feasible, a rather extensive simulation campaign has been conducted. In each simulation run, faults are injected in the system according to the model described in the sections discussing FMEA and reliability analysis. We consider faults consisting of the failure of a single component, occurring at an arbitrary time instant in the course of task execution by the VSA system. Representative fault timing is considered to be in the acceleration, intermediate, and deceleration phases. No FM strategy is used in the simulations. For comparison purposes, the dynamical models of three AA arrangements for VSA are considered. The model parameters (inertias, spring constants, and actuator torques) are chosen so that they would perform equally well under nominal fault-free conditions. Specifically, they accomplish the reference task (a rest-to-rest motion of 2π rad) under equal safety bounds in the same time.

An example simulation with a fault injected in the acceleration phase for the three different arrangements is reported in Figure 6, showing that this type of fault can actually become

Table 3. MTTF and MTTSF (in years) for the actuation arrangements versus different settings of the FM system (three OP scenarios).

	OP III		OP II		OP I	
	MTTF	MTTSF	MTTF	MTTSF	MTTF	MTTSF
Simple	2.8	2.8	2.8	2.8	2.8	2.8
Cross coupled	2.3	2.3	2.8	2.8	2.8	4.0
Bidirectional	1.9	1.9	2.8	2.8	2.8	6.0

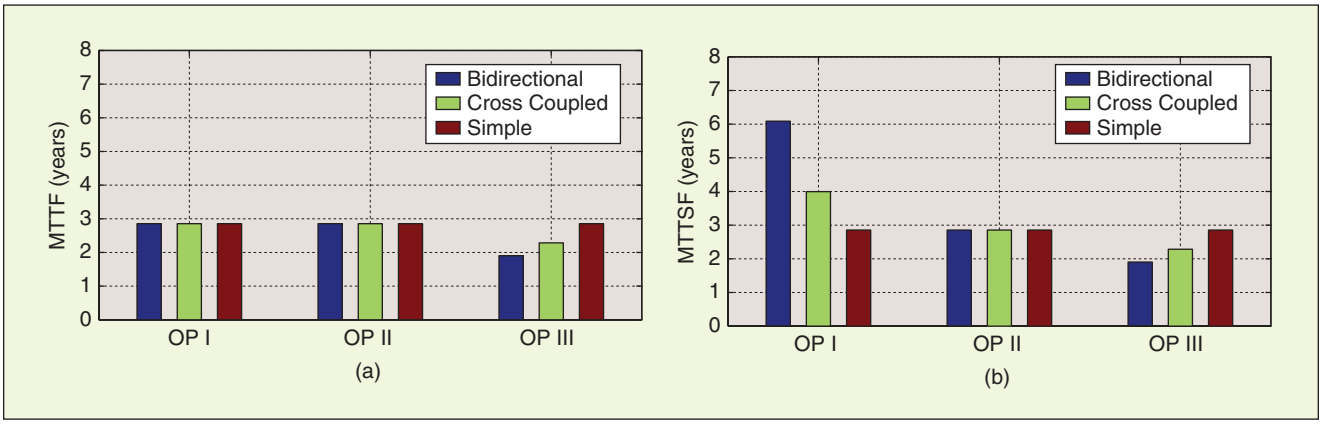

Figure 5. *(a) Reliability (MTTF) and (b) steerability (MTTSF) of the actuation systems versus the FM coverage (three OP scenarios).*

dangerous. As another representative example, the effects of failure of the coupling elastic element in a cross-coupled actuator is shown in Figure 7. It can be observed that the system maintains the ability of adapting stiffness in this case. Accordingly, safety margin violations are only marginal. Similar results are found for the bidirectional arrangement, thus confirming the expectation (discussed in the "State-Based Model" section) that reliable states are safe.

Table 4 describes a summary of the consequences of the various failures in the three arrangements as obtained through simulations. Note that simulations evaluate the worst-case consequence of an impact occurring at any time between the start and end of motion, in the presence of a given type of failure occurring in one of the three phases. Thus, for instance, the first line in Table 4 means that, if in a simple AA arrangement, motor 1 fails defaulting to maximum torque in the acceleration phase, then at some subsequent time an impact will overcome the safety limits.

It should be further noted that a conventional joint, rigidly connected to the motor, and dimensioned to achieve the same performance in the reference task, would result to be unsafe for impacts even in the fault-free case (the only countermeasure

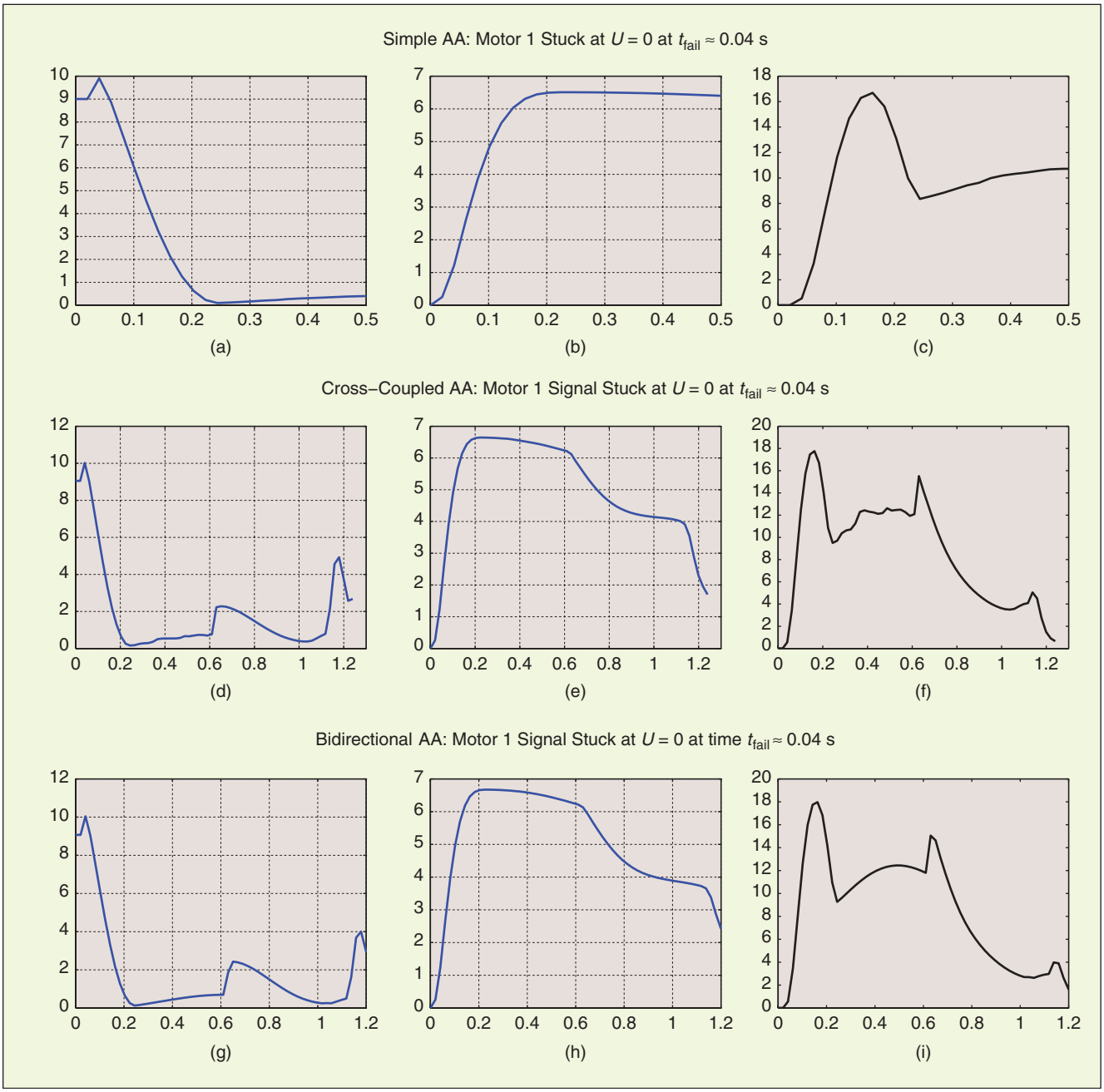

Figure 6. *An example of a safety-verification simulation test, showing runs for each of the three arrangements with a failure of motor 1, defaulting to zero torque in the acceleration phase. The effects of the fault are shown on the (a), (d), and (g) joint stiffness (in Nm/rad); (b), (e), and (h) velocity (in rad/s); and (c), (f), and (i) resulting HIC for impacts potentially occurring thereafter (in $m^{2.5}/s^4$). Time is reported in seconds on the abscissae.*

here would be to lower the velocity and hence the performance).

Conclusions

In this article, we performed an analysis of the dependability of an elementary yet critical robot component, i.e., the joint-level actuation subsystem. We consider robot actuators that implement the VSA paradigm, i.e., ability to change the effective transmission stiffness during motion to achieve high performance while constantly keeping injury risks by accidental impacts with humans below a given threshold.

Without attempting a comprehensive review of different existing design approaches to VSA, we focused on the analysis of three different arrangements of agonistic/antagonistic actuation mechanisms for pHRI applications. Several aspects of their performance, safety, and dependability have been considered to get an indicative, though certainly not exhaustive, comparison of these alternatives.

According to our results, the simple AA arrangement is more reliable (due to the simplicity of its mechanical implementation) if FM is not used. Proper FM actions can make other designs perform equally well as the simple AA concerning reliability and can perform better for steerability. Simulations of impacts in failed states (where FM is not used by a worst-case assumption) also show that the different designs have comparable safety properties.

Although overall results for the bidirectional arrangements are somewhat superior, especially in terms of steerability (if FM is applied), we do not extrapolate any general claim in this regard. Indeed, many factors influence the results of similar studies, and each case should be considered in detail and very carefully.

The scope of the study can become quite broad, and many of the theoretical and technical issues presented here (e.g., fault detection, supervisory control, and safety-related systems) will require further separated investigations. One of the purposes of this work was to explore and further promote dependability studies in robotics, as a means of addressing concerns in safety-critical robotic systems for physical interactions with humans. In this sense, a robot for pHRI applications is a

Table 4. Single component failures during acceleration, intermediate, and deceleration phases for the particular nominal task execution.

Component	Failure Mode	Consequence
Simple AA		
Motor 1	Maximum torque	Acceleration → Unsafe Intermediate → Unsafe Deceleration → Safe
Motor 1	No torque	Acceleration → Unsafe Intermediate → Safe Deceleration → Safe
Motor 2	Maximum torque	Acceleration → Safe Intermediate → Safe Deceleration → Safe
Motor 2	No torque	Acceleration → Unsafe Intermediate → Unsafe Deceleration → Safe
Spring $K1$	Breakage	Acceleration → Safe Intermediate → Safe Deceleration → Safe
Spring $K2$	Breakage	Acceleration → Marginally unsafe Intermediate → Safe Deceleration → Safe
Cross-coupled AA		
Motor 1	Maximum torque	Acceleration → Unsafe Intermediate → Unsafe Deceleration → Safe
Motor 1	No torque	Acceleration → Unsafe Intermediate → Safe Deceleration → Safe
Motor 2	Maximum torque	Acceleration → Safe Intermediate → Safe Deceleration → Safe
Motor 2	No torque	Acceleration → Unsafe Intermediate → Unsafe Deceleration → Safe
Spring $K1$	Breakage	Acceleration → Safe Intermediate → Safe Deceleration → Safe
Spring $K2$	Breakage	Acceleration → Marginally unsafe Intermediate → Safe Deceleration → Safe
Spring $K3$	Breakage	Acceleration → Marginally unsafe Intermediate → Marginally unsafe Deceleration → Safe
Bidirectional AA		
Motor 1	Maximum torque	Acceleration → Unsafe Intermediate → Unsafe Deceleration → Safe
Motor 1	No torque	Acceleration → Unsafe Intermediate → Safe Deceleration → Safe
Motor 2	Maximum torque	Acceleration → Safe Intermediate → Safe Deceleration → Safe
Motor 2	No torque	Acceleration → Unsafe Intermediate → Unsafe Deceleration → Safe
Spring $K1$	Breakage	Acceleration → Safe Intermediate → Safe Deceleration → Safe
Spring $K2$	Breakage	Acceleration → Marginally unsafe Intermediate → Safe Deceleration → Safe
Spring $K1' \wedge K2'$ (preloading linear springs)	Breakage	Acceleration → Safe Intermediate → Safe Deceleration → Safe

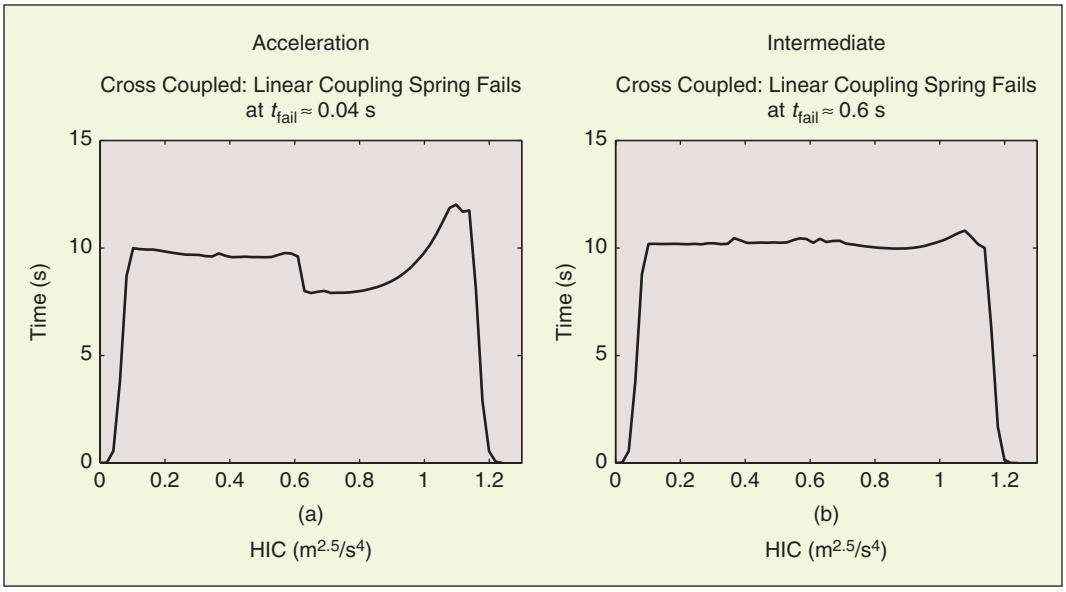

Figure 7. *Simulation results corresponding to failures of the coupling elements in a cross-coupled AA arrangement. HIC values developed with faults injected during (a) acceleration and (b) intermediate phases are shown, indicating a marginal violation of the set value (10 $m^{2.5}/s^4$), which can be tolerated if a suitable safety margin is used.*

unique benchmark for improving the state of art of fault tolerant design as well as in developing tools to master performance, dependability, and safety issues of a robotic structure.

Acknowledgments

We thank Riccardo Schiavi, Giorgio Grioli, Gianluca Boccadamo, Marco Piccigallo, and Giovanni Tonietti for their work on different aspects of the development of VSA actuators. This work was supported by the PHRIENDS Specific Targeted Research Project, funded under the Sixth Framework Programme of the European Community under Contract IST-045359. We are solely responsible for its content. It does not represent the opinion of the European Community and the community is not responsible for any use that might be made of the information contained therein.

Keywords

pHRI, safety, VSA, AA, mechanism, control, FMEA, dependability, reliability, steerability.

References

[1] A. Albu-Schäffer, A. Bicchi, G. Boccadamo, R. Chatila, A. D. Luca, A. D. Santis, G. Giralt, G. Hirzinger, V. Lippiello, R. Mattone, R. Schiavi, B. Siciliano, G. Tonietti, and L. Villani, "Physical human-robot interaction in anthropic domains: Safety and dependability," presented at the 4th IARP/IEEE-EURON Workshop on Technical Challenges for Dependable Robots in Human Environments, Nagoya, Japan, 2005.

[2] A. Avizienis, J. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Depend. Secure Comput.*, vol. 1, no. 1, pp. 11–33, Jan./Mar. 2004.

[3] A. Bicchi and G. Tonietti, "Fast and soft arm tactics: Dealing with the safety–performance tradeoff in robot arms design and control," *IEEE Robot. Automat. Mag.*, vol. 11, no. 2, pp. 22–33, June 2004.

[4] A. Bicchi, S. L. Rizzini, and G. Tonietti, "Compliant design for intrinsic safety: General issues and preliminary design," in *Proc. Int. Conf. Robotic Systems (IROS 2001)*, Maui, HI, 2001, pp. 1864–1869.

[5] A. Bicchi, E. Colgate, and M. Peshkin, "Physical human-robot interaction," in *Springer Handbook of Robotics*, O. Khatib and B. Siciliano, Eds. New York: Springer-Verlag, 2008, ch. 57, pp. 1335–1348.

[6] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Events Systems*. Norwell, MA: Kluwer, 1999.

[7] J. B. Dugan and K. S. Trivedi, "Coverage modeling for dependability analysis of fault tolerant systems," *IEEE Trans. Comput.*, vol. 38, no. 6, pp. 775–787, June 1989.

[8] C. English and D. Russell, "Implementation of variable joint stiffness through antagonistic actuation using rolamite springs," in *Mechanism and Machine Theory*, vol. 34. New York: Pergamon, 1999, pp. 27–40.

[9] R. Filippini, S. Sen, G. Tonietti, and A. Bicchi, "A comparative dependability analysis of antagonistic actuation arrangements for enhanced robotic safety," in *Proc. Int. Conf. Robotics and Automation (ICRA 2007)*, Rome, 2007, pp. 4349–4354.

[10] G. Giralt and P. Corke, Eds., "Technical challenge for dependable robots in human environments," presented at the IARP/IEEE Workshop, Seoul, Korea, 2001.

[11] A. H. C. Goslin and V. Hayward, "Time-domain passivity control of haptic interfaces with tunable damping hardware," in *Proc. World Haptics Conf. 2007*, pp. 164–169.

[12] S. Haddadin, A. Albu-Schäffer, and G. Hirzinger, "Safety evaluation of physical human-robot interaction via crash-testing," presented at the Robotics: Science and Systems Conf. (RSS 2007), Atlanta, 2007.

[13] D. L. Hamilton, I. D. Walker, and J. K. Bennett, "Fault tolerance versus performance metrics for robot systems," in *Proc. IEEE Int. Conf. Robotics and Automation*, 1996, pp. 3073–3080.

[14] J. Heinzmann and A. Zelinsky, "The safe control of human friendly robots," in *Proc. IEEE/RSJ Int. Conf. Intelligent Robots and Systems (IROS'99)*, pp. 1020–1025.

[15] N. Hogan, "Adaptive control of mechanical impedance by coactivation of antagonist muscles," *IEEE Trans. Automat. Control*, vol. 29, no. 8, pp. 681–690, 1984.

[16] A. Hoyland and M. Rausand, *System Reliability Theory: Models and Statistical Methods*, 2nd ed. New York: Wiley, 2005.

[17] J. W. Hurst, J. E. Chestnutt, and A. A. Rizzi, "An actuator with physically variable stiffness for highly dynamic legged locomotion," in *Proc. IEEE Int. Conf. Robotics and Automation*, New Orleans, 2004, pp. 4662–4667.

[18] K. Ikuta, H. Ishii, and M. Nokata, "Safety evaluation method of design and control for human-care robots," *Int. J. Robot. Res.*, vol. 22, no. 5, pp. 281–297, May 2003.

[19] *Functional Safety of Electrical-Electronic-Programmable Electronic Safety Related Systems*, IEC Standard 61508, 1998.
[20] R. Iserman, *Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance*. Berlin, Germany: Springer-Verlag, 2006.
[21] *Robots for Industrial Environments—Safety Requirements. Part 1: Robot*, ISO10218-1, 2006.
[22] K. Koganezawa, T. Nakazawa, and T. Inaba, "Antagonistic control of multi-DOF joint by using the actuator with non-linear elasticity," in *Proc. IEEE Int. Conf. Robotics and Automation*, Orlando, May 2006, pp. 2201–2207.
[23] Y. Hirata, A. Hara, and K. Kosuge, "Motion control of passive intelligent walker using servo brakes," *IEEE Trans. Robot.*, vol. 23, no. 5, pp. 981–990, Oct. 2007.
[24] J. Laprie, "Dependability: Its attributes, impairments and means," in *Predictably Dependable Computing Systems*, B. Randell et al. Eds. New York: Springer Verlag, 1995, pp. 3–24.
[25] K. F. Laurin-Kovitz, J. E. Colgate, and S. D. R. Carnes, "Design of components for programmable passive impedance," in *Proc. IEEE Int. Conf. Robotics and Automation*, Sacramento, Apr. 1991, pp. 1476–1481.
[26] D. Logothesis, A. Puliafito, and K. S. Trivedi, "Markov regenerative models," in *Proc. Int. Computer Performance and Dependability Symp.*, Erlangen, Germany, 1995, pp. 134–143.
[27] B. Lussier, R. Chatila, F. Ingrand, M. O Killijian, and D. Powell, "On fault tolerance and robustness in autonomous systems," presented at the 3rd IARP-IEEE/RAS-EURON Joint Workshop on Technical Challenges for Dependable Robots in Human Environments, Manchester, U.K., Sept. 7-9, 2004.
[28] J. McDermid, "Issues in the development of safety critical systems," *Safety-Critical Systems: Current Issues, Techniques and Standards*, F. Redmill and T. Anderson, Eds. London, U.K.: Chapman Hall, 1990, pp. 16–42.
[29] J. S. Mehling, J. E. Colgate, and M. A. Peshkin, "Increasing the impedance range of a haptic display by adding electrical damping," in *Proc. 1st Joint Eurohaptics Conf. Symp. Haptic Interfaces for Virtual Environment and Teleoperator Systems*, 2005, pp. 257–262.
[30] H. J. Merly, P. Prasad, and G. Nusholtz, "Head injury risk assessment for forehead impacts," *SAE Trans.*, vol. 15, no. 6, pp. 26–46, 1996.
[31] T. Morita and S. Sugano, "Robot arm equipped with mechanical impedance adjuster," in *Proc. IEEE/RSJ Int. Conf. Intelligent Robots and Systems*, 1995, vol. 1. pp. 407–412.
[32] M. Okada, Y. Nakamura, and S. Ban, "Design of programmable passive compliance shoulder mechanism," in *Proc. IEEE Int. Conf. Robotics and Automation*, Seoul, Korea, 2001, pp. 348–353.
[33] OSHA Technical Manual. *Industrial Robots and Robot System Safety* [Online]. Available: http://www.osha.gov/dts/osta/otm/otm_iv/otm_iv_4.html
[34] *Draft Standard for Trial Use for Intelligent Assist Devices—Personnel Safety Requirements*, Robotic Industries Association, T15.1, 2002.
[35] R. Schiavi, G. Grioli, S. Sen, and A. Bicchi, "VSA-II: A novel prototype of variable stiffness actuator for safe and performing robots interacting with humans," presented at the IEEE Int. Conf. on Robotics and Automation, Pasadena, CA, May 2008.
[36] K. W. Hollander and T. G. Sugar, "Design of lightweight lead screw actuators for wearable robotic applications," *ASME J. Mech. Des.*, vol. 128, no. 5, pp. 644–648, 2006.
[37] G. Tonietti, R. Schiavi, and A. Bicchi, "Design and control of a variable stiffness actuator for safe and fast physical human/robot interaction," in *Proc. IEEE Int. Conf. Robotics and Automation (ICRA 2005)*, pp. 528–533.
[38] K. S. Trivedi, G. Ciardo, M. Malhotra, and R. Sahner, "Dependability and performability analysis," in *Performance Evaluation of Computer and Communication Systems* (Lecture Notes in Computer Science), L. Donatiella and R. Nelson, Eds. New York: Springer-Verlag, 1993, pp. 587–612.
[39] K. S. Trivedi, *Probability and Statistics with Reliability, Queuing and Computer Science Applications*, 2nd ed. New York: Wiley, 2002.
[40] K. T. Ulrich, T. T. Tuttle, J. P. Donoghue, and W. T. Townsend, "Intrinsically safer robots," Barrett Technology Inc., Final Report NASA Contract NAS10-12178, 1995.
[41] J. Versace, "A review of the severity index," presented at the Stapp Car Crash Conf., 1971, Paper SAE 710881.
[42] M. L. Visinsky, J. R Cavallaro, and I. D. Walker, "A dynamic fault tolerance framework for remote robots," *IEEE Trans. Robot. Automat.*, vol. 11, no. 4, pp. 477–490, Aug. 1995.
[43] J. Yamaguchi, S. Inoue, D. Nishino, and A. Takanishi, "Development of a bipedal humanoid robot having antagonistic driven joints and 3-DOF trunk," in *Proc. IEEE/RSJ Int. Conf. Intelligent Robots and Systems*, Victoria, Canada, 1998, pp. 96–101.

Roberto Filippini received the Laurea degree in computer engineering in 2000 and his Ph.D. degree in automatics, robotics, and bioengineering from the University of Pisa in 2006. He worked in the Centro Interdipartimentale di Ricerca E. Piaggio, Pisa, and CERN, Geneva, where he contributed to the dependability analysis of the Large Hadron Collider machine protection system. Currently, he is at the Paul Scherrer Institut in Switzerland. His research interests include dependability modeling and probabilistic safety assessment of safety-critical systems.

Soumen Sen received his bachelor's degree in mechanical engineering from the National Institute of Technology, Durgapur, India, in 1992 and his master's degree in production technology and robotics from Jadavpur University, Kolkata, India, in 1994. He worked with the Department of Atomic Energy, Government of India, for more than nine years. He served in the Centre for Advanced Technology, Indore, where he was involved in the design activities for development of a large particle accelerator, and, subsequently, in Bhabha Atomic Research Centre, Mumbai, where he worked on robotics for nuclear applications and multifingered grasping and manipulation. In August 2005, he joined the Centro Interdipartimentale di Ricerca E. Piaggio, Pisa, Italy. Currently, he is pursuing a Ph.D. program in automation, robotics, and bioengineering at the University of Pisa. His research activity concerns pHRI and its associated design and the development of robots and robot components.

Antonio Bicchi is a professor of automatic control and robotics at the University of Pisa. He graduated from the University of Bologna in 1988 and was a postdoctoral scholar at the Artificial Intelligence Lab, Massachusetts Institute of Technology, from 1988–1990. His main areas of research include dynamics, kinematics, and control of complex mechanical systems including robots, autonomous vehicles, and automotive systems; haptics and dexterous manipulation; theory and control of nonlinear systems, in particular, hybrid (logic-dynamic, symbol-signal) systems. He has edited and published more than 200 papers in international journals, books, and refereed conferences. Currently, he serves as the director of the Interdepartmental Research Center E. Piaggio of the University of Pisa. He is a Fellow of the IEEE and chair of the conference editorial board for the IEEE Robotics and Automation Society (RAS). He has served as past vice-president for Member Activities, IEEE RAS, Distinguished Lecturer, and editor for several scientific journals including *IEEE Transactions on Robotics and Automation*. He chaired the First World Haptics Conference in 2005 and the Hybrid Systems: Computation and Control Conference in 2007.

Address for Correspondence: Antonio Bicchi, Interdepartmental Research Centre E. Piaggio, University of Pisa, 56126 Pisa, Italy. E-mail: bicchi@ing.unipi.it.