Study of different load dependencies among shared redundant systems

Jan Galdun, Jean-Marc Thiriet, Jan Ligus

STUDY OF DIFFERENT LOAD DEPENDENCIES AMONG SHARED REDUNDANT SYSTEMS *

JÀN GALDUN †, JEAN-MARC THIRIET ‡, AND JÀN LIGUŠ ‡

Abstract. The paper presents features and implementation of a shared redundant approach to increase the reliability of networked control systems. Common approaches based on redundant components in control system use passive or active redundancy. We deal with quasi-redundant subsystems (shared redundancy) whereas basic features are introduced in the paper. This type of redundancy offers several important advantages such as minimizing the number of components as well as increasing the reliability. The example of a four-rotor mini-helicopter is presented in order to show reliability improving without using any additional redundant components. The main aim of this paper is to show the influence of the load increasing following different scenarios. The results could help to determine the applications where quasi-redundant subsystems are a good solution to remain in a significant reliability level even if critical failure appears.

Key words. Shared redundancy, Dependability, Networked control systems

1. Introduction. To be able to obtain relevant results of reliability evaluations for complex systems, it is necessary to describe the maximum of specific dependencies within the studied system and their influences on the system reliability. Different methods or approaches for control systems' reliability improvement are developed in order to be applied to specific subsystems or to deal with dependencies among subsystems. A classical technique consists in designing a fault-tolerant control [1] where the main aim is to propose a robust control algorithm. Guenab and others in [2] deal with this approach and reconfiguration strategy in complex systems, too.

On the other side is the design of reliable control architectures. Probably the most used technique is to consider the redundant components which enlarge the system structure and its complexity too. Active and passive redundancy is the simplest way how to improve dependability attributes of the systems such as reliability, maintainability, availability, etc [3]. However, as it was mentioned the control structure turns to be more complex due to an increasing number of components as well as the number of possible dependencies among components, it is in particular the case for Networked Control Systems [4] [5].

The paper introduces complex networked control architecture based on cascade control structure. The cascade structure was chosen purposely due to its advantages. This structure is widely used in industrial applications thanks to positive results for quality of control which are already described and generally known [6]. On the other side it offers some possibilities of system reliability improvement. There are potentially redundant components such as controllers (primary, secondary). If more than one network is implemented we could consider them as potentially redundant subsystems too. Finally if the physical system allows it, it is possible to take profit from sensors. The cascade structure and other features are introduced in more details in the third part.

The paper is organised as follows. After bringing closer the research background, the shared redundancy is introduced. The controllers and networks are presented

[1] An earlier version of this paper was presented at the 3rd Real-Time Software Workshop, RTS2008, in Wisla, Poland, October 20, 2008.

[†] Laboratoire GIPSA-Lab (GIPSA-Lab UMR 5216 CNRS-INPG-UJF) BP 46, F-38402 Saint Martin d'Hères Cedex, France

[‡] Department of Cybernetics and Artificial Intelligence, Technical University of Košice, Letnà 9, 04012 Košice, Slovakia

in more details in order to show some dependencies which could be appeared when a shared redundancy approach is implemented. In the next part are presented networked topologies considered as cascade control (CC) structure of the 4-rotor mini-helicopter (drone) model [7]. Using Petri nets were prepared the models of the introduced quasi-redundant components as well as drone's control structure. A simple model of the two quasi-redundant subsystems is evaluated. Finally, are proposed the simulation results of the mentioned simple two components model as well as the model of the complex drone's structure with short conclusion.

2. Research Background. Control architecture design approach was taken into account by Wysocki, Debouk and Nouri [8]. They present shared redundancy as parts of systems (subsystems) which could replace another subsystem in case of its failure. This feature is conditioned with the same or similar function of the subsystem. Wysocki et al. introduce the shared redundant architecture in four different examples illustrated on "X-by-Wire" systems used in automotive applications. Presented results shown advantages of this approach in control architecture design.

The shared redundancy approach involves the problematic of a Load Sharing [9]. Thus, some of the components take part of the load of the failed components in order to let the system in functional mode. Consideration of the load sharing in mechanical components is presented by Pozsgai and others in [10]. Pozsgai and others analyze this type of systems and offer mathematical formalism for simple system 1-out-of-2 and 1-out-of-3. Also there are some mathematical studies [9] of several phenomena appeared on this field of research. Bebbington and others in [9] analyze several parameters of systems such as survival probability of load shared subsystems.

3. Shared Redundancy. Specific kind of redundant subsystems which have similar features such as active redundancy however gives us some additional advantages which will be introduced in further text. This kind of spares represents another type of redundant components which are not primary determined as redundant but they are able to replace some other subsystems if it is urgently required. This type of redundancy is referred as *shared redundancy* [8] or *quasi-redundancy* [11]. Due to its important advantages it is useful to describe this kind of spares in order to show several non-considered and non-evaluated dependencies which could have an influence to the system reliability. Identification and description of this influence should not be ignored in order to obtain relevant results of the reliability estimation of the systems which involve this kind of spares.

As it was mentioned above, the *shared redundancy* (SR) mentioned by Wysocki and others in [8] is in further text taken into account in the same meaning as a *quasi-redundant* (QR) component. Thus, quasi-redundant components are the parts of the system which follow their primary mission when the entire system is in functional state. However, when some parts of the system fail then this function could be replaced by another part which follows the same or a similar mission, thus by quasi-redundant part. The quasi-redundant components are not primary determined as active redundant subsystem because each one has its own mission which must be accomplished. Only in case of failure it could be used. In NCS appears the question of logical reconfiguration of the system when the data flow must be changed in order to replace the functionality of a subsystem by another one. For example, some new nodes will lose the network connection and the system has to avoid the state when packets are sent to a node which does not exist. Thus, the main features of the shared redundancy could be summarized as follows:

"Quasi-redundant component is not considered as primary redundant component such

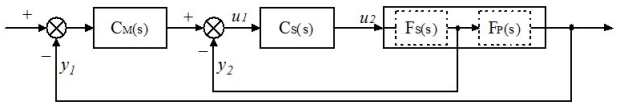

FIG. 3.1. *Main structure of the cascade control*

as the active or the passive redundant components."

Generally in networked control systems, three kinds of quasi-redundant components (subsystems) could be considered:

- QR controllers.
- QR networks.
- QR sensors.

Hence, a necessary but not sufficient condition is that a control structure where SR could be considered has to be composed at least of two abovementioned subsystems (controllers, networks, actuators). The subsystems should have similar functionality or construction in order to be able to replace the mission of another component. In case of quasi-redundant components there are several limitations. In order to take profit of quasi-redundant networks, it is necessary to connect all nodes in all considered QR networks. Thus, in case of different networks the components should have implemented all necessary communication interfaces. In case of QR controllers the hardware performance has to allow implementing more than one control task.

Third mentioned components are sensors. Consideration of the sensors as QR components has important physical limitations. In order to be able to replace a sensor for measuring a physical value X by another one for measuring Y it is necessary to use "multi-functional" smart sensors. *We can suppose that some combination of the physical values can not be measured by using one sensor due to the inability to implement the required functionality in one hardware component.*

Other limitation is the distance between failed sensor and its QR sensor which could have a significant influence to the possibility of its replacing. Generally, implementation of the QR sensors within control system structure could be more difficult than the application of the SR approach on controllers or networks.

There are several naturally suitable control structures which could implement the shared redundancy approach without other modifications such as cascade control structure (Fig. 3.1). This structure is often used in industrial applications thanks to its important features which improve the quality of control. With using cascade a control structure there are several constraints [8]. The main condition requires that the controlled system must contain a subsystem (secondary subsystem FS(s) - Fig. 3.1) that directly affect to the primary system FP(s). Thus, the cascade structure composes of two independent controllers which can be used in order to implement the shared redundant approach.

Usually for secondary subsystems there is a condition of faster dynamics than primary process. This condition must not be fulfilled [8]; in this case, some modifications of conventional cascade structure (Fig. 3.1) and control laws must be provided.

3.1. Quasi-redundant controllers. In the previous text, several suitable control structures were briefly introduced. As it was shown the controllers covered by these structures could be considered as quasi-redundant components by default. Thus,

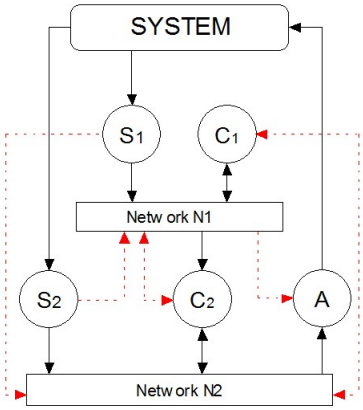

FIG. 3.2. *NCCS with two networks and alternative network connections*

the hardware of both components could be shared in order to implement a shared redundant approach.

Let's consider the networked cascade control system shown in figure 3.2. The system is composed of five main components (Sensor S_1, S_2, controllers C_1, C_2 and actuator A) and two networks. The communication flow among components is determined by its cascade control structure. Thus, sensor S_1 sends a measured value to controller C_1 (Master), the controller C_2 (Slave) receives the values from the sensor S_2 as well as the controller C_1 in order to compute an actuating value for the actuator A.

Each part of the system (components and networks) presents independent subsystem. However, when quasi-redundant components are studied, the system is not considered as composed of independent components. Depending on the performance parameters of the used hardware equipment in the control loop, a specific influence on the system reliability should be taken into account. Thus some dependencies should not be ignored in the dependability analysis. In the NCCS shown in Fig. 3.2 we could consider controllers C_1 and C_2 as the quasi redundant subsystems (components). Both QR controllers have a primary mission which should be followed. Thus, a controller C_1 controls outer control loop and controller C_2 stabilizes inner control loop. However in case of failure of one of them, we could consider the second one as a kind of spare.

As it was mentioned previously, the controllers follow their primary mission stabilization or performance optimization of the controlled system. Therefore, in regards to the similar hardware, it allows sharing the computing capacity and executing different tasks. Thus, in order to implement the SR approach, both controllers have to encapsulate both control tasks - for the outer and the inner control loop (see the cascade control structure in figure 3.1).

In non-failure mode the primary task is executed in both controllers. However, in case of controller's failure (primary or secondary) non-failed controller starts execute both tasks and computes actuating value for primary as well as secondary subsystems. In this case we can suppose two scenarios.

The first one supposes that the controller is able to execute all the necessary tasks within the required sample periods (Fig. 3.3a). Thus, no delays or other undesirable consequences are expected. In this case the behavior of the quasi-redundant com-

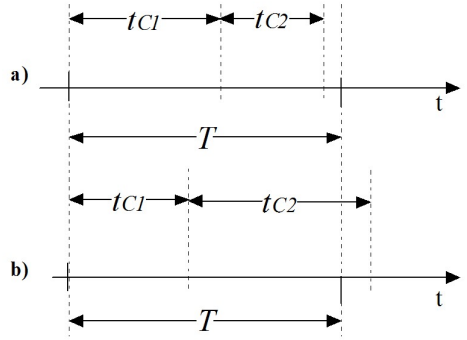

FIG. 3.3. *Possible scenarios for quasi-redundant controllers*

ponent is similar as in the case of active redundant components. Thus, in the case of failure of one of the components, the second takes care about its mission until its failure.

Figure 3.3b shows a second case when time to execute both necessary tasks is greater than the required sampling period. Thus, the controller will cause the delays which have significant influence to the system stability [12] [13]. Therefore, this delay could be known which allows its partially compensating by using several methods [14]. Thus, we can suppose that the system destabilization will not occur immediately after the first delay and we are able to compensate it for some time interval. Thus, quasi-redundant controller does not fail immediately but its reliability decreased.

There are several situations when this scenario could be considered. In critical systems where the failure of an important component could cause undesired damages or other dangerous consequences, the shared redundancy approach could help to allocate some time interval in order to maintain the system in a safe state. Thus, the SR approach can be a significant technique to secure the system before a damage risk.

3.2. Quasi-redundant networks. The second part of the NCS which could be taken into account as SR subsystems are networks. Let's suppose a system with two networks (Fig. 3.2) where all components could communicate (connect) on these networks (N_1 and N_2) if it is needed. In this case we can apply the SR approach on this system.

Considered functionality of the quasi redundant networks is as follows. Both networks transmit required data - network N_1 transmit data from S_1 to C_1 and from C_1 to C_2 such as network N_2 from S_2 to C_2 and from C_2 to A. Thus both networks are active and allocated during the system mission. The same as in the case of QR controllers: when a network failed, the second one can take its load after a system reconfiguration. Thus, all required data are sent through the second network. Hence, two similar scenarios as with the controller task execution could be described. The amount of transmitted data on the network with a specified bit rate has logically influence on the probability of failure of the network (of course this depends on the network type and other parameters mentioned). This influence could be ignored when the network performance parameters are sufficient. However, we can suppose that the probability of network failure is increasing simultaneously when the network load increases.

The characteristic between network loading and its bit rate depends on the net-

work type and have to be measured in real network conditions in order to determine the type of dependency - linear or nonlinear.

Not only the network bit rate can be important however other network limitations such as maximal number of nodes connected to the network, etc. All limits of the QR subsystems can create dependencies with direct influence on the system reliability. Primary, we could consider these dependencies as undesirable but in case of critical failures this SR approach gives some time to save the system.

When NCS with an SR approach are analyzed, this characteristic should be included in the prepared model and further evaluated in order to determine its influence to the reliability of the whole NCS.

3.3. Different scenarios in shared redundancy. When certain dependencies are ignored we could regard on the control system with QR components as a control structure with active redundant components. However, there are several important scenarios when the reliability of the system could be decreased in order to prevent dangerous consequences or other undesirable events.

These scenarios could appear when some conditions could not be fulfilled (insufficient execution time or network bit rate) but the system need some time in order to take a safe state. Hence, it is necessary to identify and describe the influence of these dependencies which leads to more relevant results. Thus, prevent from too pessimistic or too optimistic results of the reliability analysis of the considered systems. The dependencies could be distinguished as follows:

- active redundant dependency,
- single step change of the nominal failure rate $\lambda_n \in \langle 0; 1 \rangle$ increased once by a constant value - step load change,
- time depend change of the nominal failure rate λ_n -functional dependency- the load of the subsystem is changed with time passed from speared subsystem failure,
  1. linear,
  2. nonlinear.

Let's assume that the destabilization of the system does not occur immediately after the first delay on the network caused by insufficient controller's hardware or network's parameters. Thus, the quasi-redundant controller does not fail immediately but in this case its failure rate increases which correspond consequently to a decreased reliability.

Thus, in case of the active redundant dependency we suppose that a quasi-redundant subsystem has sufficient capacities in order to follow its primary mission as well as the mission of the failed subsystem (or subsystems).

A single step change of the nominal failure rate of the subsystem is considered in the case of subsystems where the failure rate of the quasi-redundant subsystem is changed (increased) once by a constant value (Fig. 3.4) during its life time. Thus, the new increased failure rate $\lambda^{'}$ remains constant during further life time of the subsystem. For example, let's suppose a NCS with two Ethernet networks where one of them has failed and consequently the system is reconfigured and all nodes (components) start to communicate through the non-failed network which has a sufficient bit rate capacity in order to transmit all the required data. However, the amount of data has been increased which consequently increases the probability of packets' collisions (under the assumption of a classical CSMA/CD protocol, for instance). Thus, the probability of failure (failure rate) has been increased up to the new value $\lambda^{'}$.

A third case considers the change of the nominal failure rate λ_n which depends on

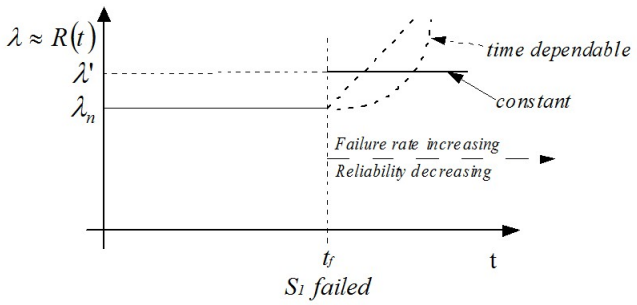

FIG. 3.4. *Possible failure rate curves for the subsystem S_2 during its mission*

the time passed from the moment of the failure until current time of the working of the quasi-redundant subsystem which encapsulates the executing necessary tasks (own tasks as well as tasks of the failed subsystem). Thus, a functional dependency has to be considered. This dependency of the change of the failure rate λ_n could be described by a linear or nonlinear dependency / function. We could study the previous example of the system with two networks. However, in this case the bit rate of the second (non-failed) network is not sufficient. Consequently delays in data transmission as well as other consequential undesirable problems such as system destabilization might be caused. We can suppose that the non-failed network will fail in some time. Thus, the nominal failure rate λ_n of the second network is now time dependent and is linearly or nonlinearly increased until the system failure. Mentioned examples with related equations are further discussed in more details.

Let's suppose that the reliability of the system $R(t)$, probability of the failure during time interval $\langle 0; t\rangle$, is characterized by a nominal failure rate $\lambda_n \in \langle 0; 1\rangle$. Let's suppose a system with two subsystems S_1 and S_2 (such as the networks in the previous examples) whereas the subsystem S_1 will fail at first and then the quasi-redundant subsystem S_2 will follow both missions (S_1 and S_2). In figure 3.4 are shown two above mentioned scenarios when the nominal failure rate λ_n of the subsystem is increased by a constant value or by a value which could be described as a linear or nonlinear function (functional dependencies).

At first increasing the failure rate λ_n one time by a constant value (see Fig. 3.4) will be dealt. It corresponds to the reliability reduction of the quasi-redundant subsystem S_2 by increasing the failure rate, during its mission, from its nominal value λ_n up to new $\lambda^{'}$. Consequently, the system will follow its primary mission thanks to the QR subsystem S_2 but its failure rate is already increased and consequently the probability of failure of S_2 is higher. The difference between nominal λ_n and increased $\lambda^{'}$ failure rate will be called decrease factor d_R. Thus, the mentioned constant value is characterized by the decrease factor d_R of the QR subsystem and a new changed failure rate $\lambda^{'}$ at the fail time t_f is given by the followed simple formula:

$$\lambda^{'} = \lambda_n + d_R \tag{3.1}$$

The failure rate increases only one time by the specified value and the QR subsystem S_2 with a new constant failure rate $\lambda^{'}$ will follow both missions of its own mission and mission of the failed subsystem S_1.

The second case shown in figure 3.3 considers the reliability reduction where the failure rate λ_n is increased during the working of the subsystem S_2 by a specified

decrease factor. This change of the nominal failure rate depends on time whereas with time extending the failure rate of the S_2 is got near to 1 (system failed). Thus, a decrease function $f_{d_R}(t)$ is represented by a linear or nonlinear characteristic and depends on the real subsystem which is considered as quasi-redundant. Thus, an increased failure rate $\lambda^{'}$ of the subsystem S_2 depends on time t and is given by the following formula:

$$\lambda^{'}(t) = \lambda_n + f_{d_R}(t) \tag{3.2}$$

As it was mentioned, the decrease function $f_{d_R}(t)$ can be represented by a simple linear function, for example,

$$\lambda^{'}(t) = \lambda_n + d_R 10^{-3}(t + 1 - t_f) \tag{3.3}$$

where $t + 1$ allows changing the nominal failure rate λ_n at the moment of the failure at time t_f.

On the other side a nonlinear exponential function can be considered as follows:

$$\lambda^{'}(t) = \lambda_n + e^{d_R(t-t_f)} \tag{3.4}$$

where $\lambda^{'}$ is the value of the increased failure rate, λ_n is the nominal failure rate of the component, t_f is the time of the failure of the component, d_R is the decrease factor which has a direct influence on the increased failure rate.

3.4. Application to a mini-drone helicopter. The NCC structure is applied for the control of a four rotors mini-helicopter (Drone, Fig. 3.5). The proposed control structure for this real model is as follows. The NCC architecture is composed of one primary controller (Master) and one secondary controller (Slave), thirteen sensors, four actuators and two communication networks.

The Master is designed for attitude stabilization (control) through Slave controller for angular velocity control for each propeller. The aim of the control is to stabilize coordinates of the helicopter [10].

The controllers are used as quasi-redundant components within the presented networked cascade control system (further only NCCS). They use the same control algorithm (propeller's angular velocity control) but with different input data (set point, system output, etc.)

Hence, in case of failure, one of them could retransmit all the required data to another one, whereas pre-programmed control algorithm should compute the actuating value. Thus, the failed controller is replaced by a second one which starts to compute the actuating value.

Other quasi-redundant parts of this control structure are networks (Fig. 3.6). As in the case of controllers, one of the networks can compensate another one after a system reconfiguration. Usually, two networks are primary designed due to reduction amount of transmitted data. However, in case of network failure all data could be retransmitted through the second one.

The described approach for subsystem's failure compensation by using the shared redundancy requires a logical reconfiguration of the NCCS. Thus, in case of failure the hardware configuration is non-touched but communication ways must be changed in order to transmit the data to a non-failed component or through a non-failed network.

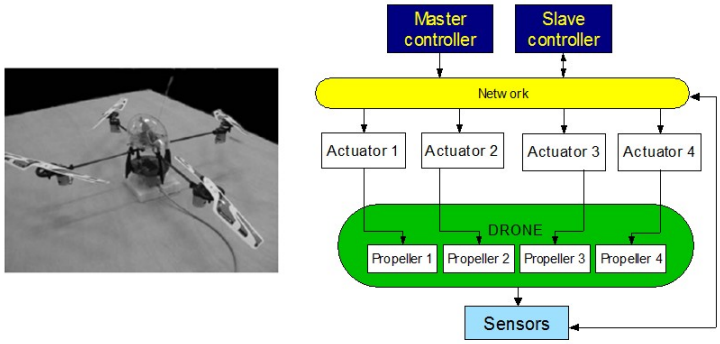

FIG. 3.5. *Cascade control structure of a mini-helicopter with one network*

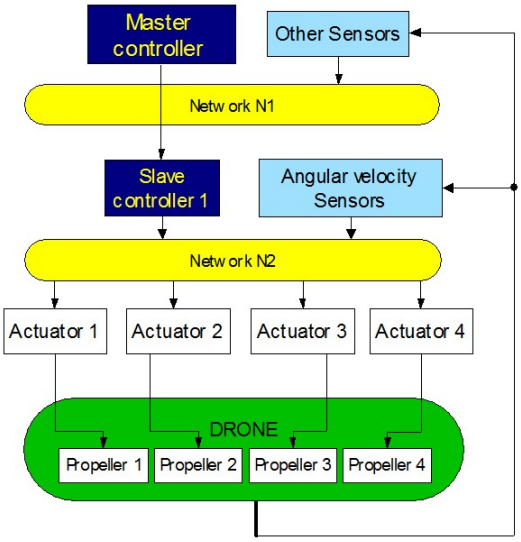

FIG. 3.6. *Cascade control structure of a mini-helicopter with two networks*

4. Simulation and results. All the presented networked control architectures (Fig. 3.5, 3.6) were modelled by using Petri nets. This tool was chosen thanks to its ability to model different types of complex systems and dependencies within them. To provide the reliability analysis, the Monte Carlo simulation (further only MCS) method was used. The multiple simulations of the modelled architecture [1] are provided to obtain the reliability behavior of the basic two quasi-redundant components (for example two controllers in CCS structure).

Model of the system covers the simulation of the random events of the basic components of the system such as sensors, controllers and actuators as well as the network's random failures. Software used for model preparation is CPN Tools which allow multiple simulation of the model in order to obtain statistically representative sample of the necessary data to determine the reliability behavior of the studied model.

As it was mentioned, the simulation of the simple two quasi-redundant compo-

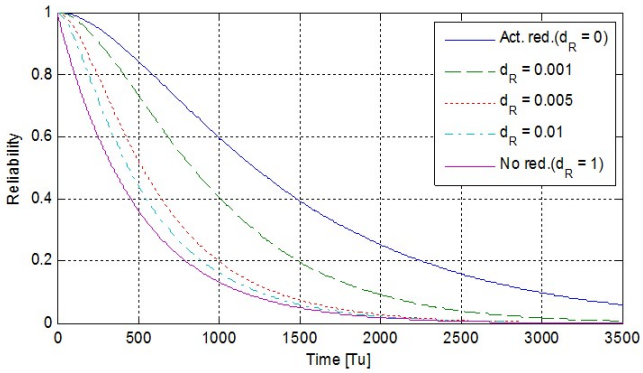

FIG. 4.1. *Influence of the increased failure rate of the component by a constant decrease factor d_R to the reliability of the system composed of two quasi-redundant components*

nents with all considered changes of the failure rate (single, linear, nonlinear) was provided. Thus, new failure rate $\lambda^{'}$ of the non-failed component is computed by using equation (3.1), (3.3) and (3.4).

This change could be called as single change because the component's failure rate is changed only once during the QR component's life time. Both components have equal nominal failure rate $\lambda_n = 0.001$.

Few examples of the influence of the single step change of the failure rate by the specified decrease factor d_R to the reliability behavior are shown in figure 4.1. We can see there are five curves. Two non-dashed curves show the studied system as a system with two active redundant components (thus, d_R is equal to zero - first curve from the top) and as system without redundant components (thus, the system composes of two independent components without redundant relation - first curve from the bottom). These two curves determine borders where the reliability of the studied system can be changed depending on the value of the decrease factor d_R.

As we can see from figure 4.1, a single increasing of the nominal failure rate λ_n of the non-failed components by the same value as was nominal failure rate λ_n up to $\lambda^{'} = 0.002$ ($d_R = 0.001$) cause a significant reduction of the reliability.

Table 4.1 show several values of the life time (parameter MTTFF) for the studied system. Each table (Table 4.1, 4.2, 4.3) shows the life time of the studied components as active redundant subsystems ($d_R = 0$) and as independent subsystems ($d_R = 0.999$). From the value of the decrease factor $d_R = 0.01$ the life time of the system significantly improves (18% and more). The results of the linear and nonlinear failure rate increasing are shown in tables 4.2 and 4.3. In all tables are noted the percentual value of the increased life time corresponding to the decrease factor.

Table 4.1 shows the MTTFF parameters of both complex mini-helicopter structures. In the first drone structure (Fig. 3.5) two quasi-redundant controllers are considered. In the second structure (Fig. 3.6) two groups of quasi-redundant subsystems are considered and simulated - the controllers and the networks.

In all simulated systems was observed the influence of the single step of the failure rate by a value specified by the decrease factor d_R. The same as in tables 4.1 - 4.3,

TABLE 4.1
MTTFF OF SIMULATED CONTROL STRUCTURES WITH DIFFERENT DECREASE FACTORS

Decrease factor - d_R	MTTFF - Drone (Fig. 3.5)	MTTFF -Drone (Fig. 3.6)
0	55(+11%)	58(+22%)
$2 * 10^{-3}$	54(+9%)	56(+17%)
10^{-2}	53(+7%)	54(+13%)
$59 * 10^{-2}$	50.5(+2%)	49(+3%)
0.999	49.6	47.6

TABLE 4.2
MTTFF OF THE TWO QUASI-REDUNDANT WITH SINGLE STEP CHANGE OF THE FAILURE RATE

$\lambda_n = 10^-3$	Act. red. $d_R = 0$ ($\lambda' = 10^-3$)	$d_R = 0.001$ ($\lambda' = 0.002$)	$d_R = 0.005$ ($\lambda' = 0.006$)	$d_R = 0.01$ ($\lambda' = 0.011$)	$d_R = 0.1$ ($\lambda' = 0.101$)
MTTFF[Tu]	1503 (+ 300%)	1002 (+200%)	667(+34%)	589(+18%)	509(+2%)
$\lambda_n = 10^-3$	No red. $d_R = 0.999$ ($\lambda' = 1$)				
MTTFF[Tu]	499				

there are shown the life time of system corresponding to different decrease factors 2.10^{-3}, 10^{-2}, 59.10^{-3}. We can see that increasing the component's nominal failure rate λ_n by a decrease factor equal to 59.10^{-3}, which represents approximately 59 times higher the failure rate, has a significant influence to decreasing the life time of the system. The results are a little bit better than in the case of the system without redundant components ($d_R = 0.999$), but we could see that they are almost the same.

The drone's structure composes of twenty (twenty-one - structure with two networks) components - thirteen sensors (3 gyro-meters, 3 magneto-meters, 3 accelerometers, 4 rotors' angular velocity sensors), two controllers, four actuators and one (two) networks. Due to the high ratio of independent components and shared redundant components within the drone's structure (18 independent and 2 quasi-redundant - Fig. 3.5) there is a difference between life times for minimal and maximal d_R is significantly smaller (about 11% and 22%) than in the case of a basic two components subsystem (Table 4.1, 4.2, 4.3).

The Mean Time Before First system's Failure is significantly longer in the case of a basic two component subsystem than in the drone's case. As it was mentioned above this is caused by the difference in complexity between basic and drone's NCC architecture. In case of comparison between two drones structures (Fig. 3.5, 3.6) the results are better for architecture with two networks which is composed of two quasi-redundant subsystems - controllers (Master, Slave) and networks when the decrease factor is smaller than 59.10^{-3}. The increasing of the nominal failure rate by the decrease factor greater than 59.10^{-3} significantly decreases the life time of the drone. On the other side, even if the controller loading will change its failure rate approximately ten times ($d_R = 10^{-2}$) the system's life time is about 7% longer than in the case of the system without a shared redundant approach implementation.

4.1. Reliability approximation. In previous article states we focused on the description of the dependencies among QR components and their influence to the final reliability of the systems. The aim of this research is to propose a simple analytical method which describes the reliability behavior of the shared redundant subsystems with dynamically changed failure rate. Hence, in next states we introduce an an-

TABLE 4.3
MTTFF OF THE TWO QUASI-REDUNDANT WITH LINEAR INCREASING OF THE FAILURE RATE

$\lambda_n = 10^-3$	Act. red. ($d_R = 0$	$d_R = 10^-3$	$d_R = 10^-2$	$d_R = 10^-1$	No redundancy
MTTFF[Tu]	1503 (+ 300%)	1153 (+231%)	812(+63%)	611(+22%)	499

TABLE 4.4
MTTFF OF THE TWO QUASI-REDUNDANT WITH EXPONENTIAL INCREASING OF THE FAILURE RATE

$\lambda_n = 10^-3$	Act. red. ($d_R = 0$	$d_R = 10^-3$	$d_R = 10^-2$	$d_R = 10^-1$	No redundancy
MTTFF[Tu]	1503 (+ 300%)	902 (+80%)	676(+35%)	537(+8%)	499

alytical equation which allows approximating the reliability of the two component system. Of course, a quasi-redundant approach is considered. Thus, a finally simple method for the dependability analysis is proposed as an extension of the common known methods for the dependability analysis. The proposed method for reliability behavior approximation supposes that both quasi-redundant components have the same or similar nominal failure rate where differences are small and could be ignored. As it was mentioned above, the system composed of two QR components is considered. In this case study, we introduce only the results for reliability approximation where a single step change of the failure rate (further only FR) is considered. This FR behavior is described in the previous part of the article (3.3) by equation 3.1. Thus, let's suppose two QR components with the nominal failure rate λ_n and define the decrease factor d_R, then the reliability $R_{2qr}(t)$ behavior of the QR subsystem composed of both components can be described as follows:

$$R_{2qr}(t) = 1 - \prod_{i=1}^{2}(1 - e^{-(\lambda_n + k_i d_R)t}) \tag{4.1}$$

where k_i is the approximated coefficient.

The parameter decrease factor d_R and approximated coefficients of equation 4.1 are shown in table 4.5. In each row of the table is shown the decrease factor with the corresponding value of the coefficients k_1 and k_2. The table shows several different values of the decrease factor whereas non-mentioned values can be easily approximated by using an appropriate method.

The maximal error of the approximation given by the parameters of the equation 4.2 is less than 1

$$R_{2\lambda_n}(t) = 1 - \prod_{i=1}^{2}(1 - e^{-(\lambda_n + \frac{d_R}{2})t}) \tag{4.2}$$

where d_R is the decrease factor and λ_n the nominal failure rate of the QR components. It is necessary to explain that the error of all the approximations converge to the highest mentioned limits (1% for table's coefficients) in the bottom part of the reliability curves where the reliability of the system is smaller than 0.4. Thus, in live period when a component replacement could be already too delayed.

TABLE 4.5
PARAMETERS OF EQUATION 4.1 FOR A SINGLE STEP FR CHANGE

Decrease factor - d_R	k_1	k_2
λ_n	0.44	0.52
$2\lambda_n$	0.39	0.395
$3\lambda_n$	0.28	0.393
$4\lambda_n$	0.198	0.434
$5\lambda_n$	0.154	0.46
$6\lambda_n$	0.13	0.4653
$7\lambda_n$	0.11	0.46
$8\lambda_n$	0.099	0.471
$9\lambda_n$	0.09	0.46
$10\lambda_n$	0.081	0.463
$20\lambda_n$	0.0445	0.38
$30\lambda_n$	0.0296	0.377
$40\lambda_n$	0.0225	0.385
$50\lambda_n$	0.0182	0.3518
$70\lambda_n$	0.0133	0.3284
$80\lambda_n$	0.011625	0.32475
$100\lambda_n$	0.0094	0.3332

4.2. MTTF parameter approximation. Each quasi-redundant subsystem does not exceed the limits of the bound of the minimal ($MTTF_{min}$) and maximal time life ($MTTF_{max}$) of the quasi-redundant subsystem. The parameter $MTTF_{max}$ represents the maximal time life of the QR subsystem which could be obtained when the conditions are equal to the conditions of the subsystem with active redundant components. Thus, the nominal failure rate of the non-failed component is not changed when its load has been increased - the case when the decrease factor is equal to zero. The lowest life time limit could be defined by the parameter $MTTF_{min}$ which characterizes the subsystem composed of the independent components. Thus, when one of the components fails the system is considered as failed. In term of the decrease factor, it is equal to 1 or (1-λ_n) for a single step FR change. Let's suppose the system life time limited by the bound defined by the MTTF parameter such as $\langle MTTF_{min}; MTTF_{max}\rangle$. These two parameters could be found by solving the simple following equations [15]:

$$MTTF_{min} = \int_0^\infty \prod_{i=1}^{n} R_i(t)dt \tag{4.3}$$

and

$$MTTF_{max} = \int_0^\infty (1 - \prod_{i=1}^{n}(1 - R_i(t)))dt \tag{4.4}$$

where R_i(t) is the reliability of each component.

In the final part of the results presentation we described the life time increasing of the two component QR subsystem with regard to the life time parameter $MTTF_{min}$ whereas various values of the decrease factor d_R are considered. We consider it as a simple and fast method for life time approximation. The results are shown in table 4.5. As in the previous part of this case study, we consider only the influence of the single step increasing of the nominal failure rate to the final life time of the two components QR system characterized by its MTTF parameter. In the first line, the failure rate of

TABLE 4.6
APPROXIMATED VALUES OF THE MTTF REDUCTION OF THE TWO-COMPONENT QR SUBSYSTEM WITH DIFFERENT SINGLE STEP CHANGE OF THE NOMINAL FAILURE RATE λ_n

Single step change of λ_n	2 λ_n ($d_R = \lambda_n$)	3 λ_n ($d_R = 2\lambda_n$)	4 λ_n	5 λ_n	7 λ_n	10 λ_n	20 λ_n	40 λ_n	100 λ_n
Extended $MTTF_{min}$	50%	35%	25%	20%	15%	10%	5%	2%	1%

the non-failed QR component characterized by the multiple of the nominal failure rate λ_n. The second line shows the corresponding MTTF parameter percentage reduction within the limits defined by the abovementioned interval of the maximal and minimal life times (MTTF). The MTTF values introduced in table 4.5 are rounded, hence the method error is about +/-2 for the multiple of the nominal failure rate smaller or equal to $40.\lambda_n$ (decrease factor $d_R < 40$). For higher value of the decrease factor, the approximated error is about +/-1 of values shown in the table. Thus, in the case of very similar analysis result of considered complex structures it is necessary to prepare the exact model in order to obtain a more exact MTTF parameter reduction. This method could be used for the QR subsystems with the same failure rate or for the system when difference among the nominal failure rate λ_n of the components is very small and can be ignored. In the case of a nominal FR smaller than 10^{-2}, the increased value $100.\lambda_n$ should represent approximately 0.1 whereas the error could be higher. Then, it could be useful that the value of nominal FR determined for a time interval T transforms to the greater value for a shorter time interval (unit).

5. Conclusion. The paper shows the influence of additional reliability decreasing of the quasi-redundant component to entire reliability of the studied system. The description of this dependency is getting closer to show the behavior of the system reliability when a shared redundancy approach is implemented. The results shown in tables 4.1 - 4.3 could be very helpful in order to approximate the life time of the quasi-redundant subsystems under different conditions of the failure rate increasing. The presented cascade control architecture is suitable for a shared redundancy approach implementation and could be applied to similar systems. For example, Steer-by-Wire control [16] of two front wheels in a car, etc. In addition the paper has shown the conventional cascade control structure within conditions of networked control systems as naturally suitable to profit from quasi-redundant subsystems as networks, controllers and potentially sensors if the physical process allows it. Despite of some constraints for using this type of control, the cascade architecture is widely used in industrial control applications. Hence, only the reconfiguration algorithm should be implemented to take profit from quasi-redundant subsystems.

The case study presented in parts 4.1 and 4.2 (results section) extends the field of common methods for reliability approximation. Equations (4.1, 4.2) are considered as simple and fast analytical method in order to evaluate the reliability of the systems which covers two-component QR subsystems with single step FR change.

The main advantages of the quasi-redundant components could be summarized as follows:

- The system is composed only of necessary components (parts) for following the primary mission of the system whereas higher system reliability is ensured without using any additional active redundant components.

- Following the first point we could suppose less number of components used for saving the control mission. Thus, the economic aspect could be significant.
- Prevention of the system's critical failure when a QR subsystem has no sufficient hardware capacities.

REFERENCES

[1] J. T. Spooner, K., M. Passino, *Fault-Tolerant Control for Automated Highway Systems*, in IEEE Transactions on vehicular technology, vol. 46, no. 3, 1997, pp. 770-785.

[2] F. Guenab, D. Theilliol, P. Weber, Y.M. Zhang, D. Sauter, *Fault-tolerant control system design: A reconfiguration strategy based on reliability analysis under dynamic behaviour constraints*, in 6th IFAC Symposium on Fault Detection, 2006, pp. 1387-1392.

[3] J. C. Laprie, H. Kopetz, A. Avižienis, *Dependability: Basic Concepts and Terminology*, Chapter 1, Springer-Verlag / Wien, ISBN: 3-211-82296-8, 1992.

[4] A. Mechraoui, Z. H. Khan, J.-M. Thiriet, S. Gentil, *Co-design for wireless networked control of an intelligent mobile robot*, in ICINCO09 - International Conference on Informatics in Control, Automation and Robotics (ICINCO), Italie (2-5 July 2009), pp. 318-324 ISBN: 978-989-674-000-9.

[5] R. Ghostine, J.-M. Thiriet, J.-F. Aubry, M. Robert, *A Framework for the Reliability Evaluation of Networked Control Systems*, in 17th IFAC World Congress, July 6-11, 2008 - pp. 6833-6838.

[6] C. Brosilow, J. Babu, *Techniques of Model-Based Control*, Prentice Hall, 2002, ch. 10.

[7] P. Castillo, A. Dzul, R. Lozano, *Real-Time Stabilisation and Tracking of a Four Rotor Mini-Rotorcraft*, in IEEE Transaction on control systems technology, Vol. 12, No. 4, 2004, pp. 510 - 516.

[8] J. Wysocki, R. Debouk, K. Nouri, *Shared redundancy as a means of producing reliable mission critical systems*, in 2004 Annual Symposium - RAMS - Reliability and Maintainability, 2004, pp.: 376-381.

[9] M. Bebbington, C-D. Lai, R. Zitikis, *Reliability of Modules with Load Sharing Components*, in Journal of Aplied Mathematics and Decision Sciences, 2007.

[10] P. Pozsgai, W. Neher, B. Bertsche, *Models to Consider Load-Sharing in reliability Calculation and Simulation of Systems Consisting of Mechanical Components*, in IEEE - Proceedings annual reliability and maintainability symposium, 2003, pp.: 493 - 499.

[11] J. Galdun, J. Ligus, J-M. Thiriet, J. Sarnovsky, *Reliability increasing through networked cascade control structure - consideration of quasi-redundant subsystems*, in World IFAC Congress, Seoul, South Korea, 2008.

[12] J. Galdun, R. Ghostine, J. M. Thiriet, J. Ligus, J. Sarnovsky, *Definition and modelling of the communication architecture for the control of a helicopter-drone*, in 8th IFAC Symposium on Cost Oriented Automation, 2007.

[13] J. Ligusova, J.M. Thiriet, J. Ligus, P. Barger, *Effect of Element's Initialization in Synchronous Network Control System to Control Quality*, in RAMS/IEEE conference Annual Reliability and Maintainability Symposium, 2004.

[14] S.I. Nicolescu, *Stabilité systèmes à retard - Aspects qualitatifs sur la stabilité et la stabilisation*, Diderot multimedia, 1997.

[15] I. Stary, *Spolehlivost systmu*, (in Czech), CVUT, Prague, ISBN 80-01-01756-7, 1998.

[16] G. Leen, D. Heffernan, *Expanding Automotive Electronic Systems*, in Computer IEEE, Vol. 35, 2002, pp. 88-93.