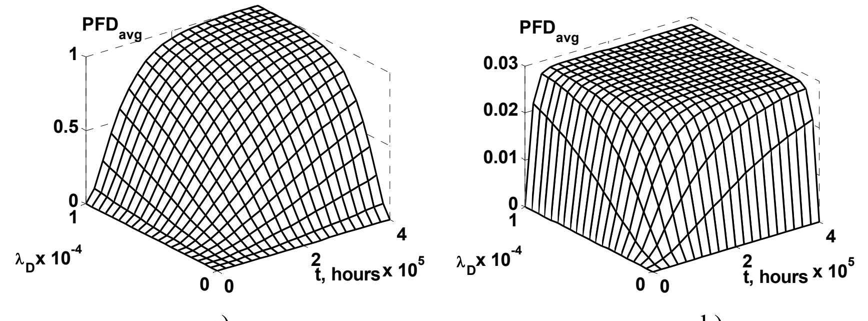
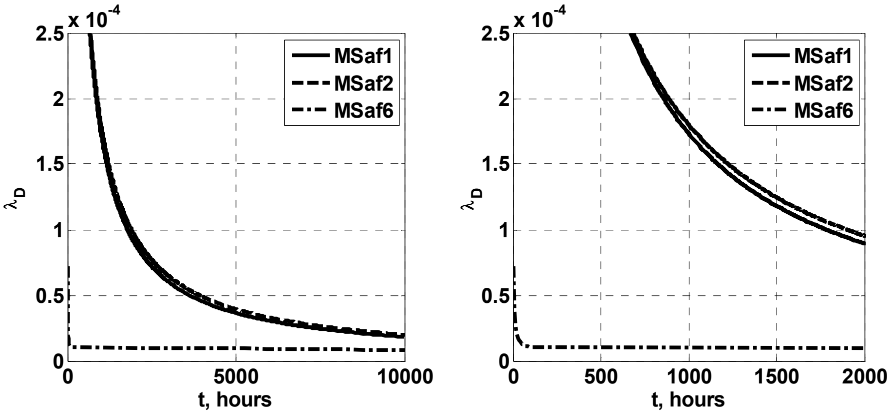


a) b)

**Fig. 9.** Dependence of $PFD_{avg}(t)$ function behavior from the input parameter $\lambda_D$ for MSaf1 (a) and MSaf2 (b)



a) b)

**Fig. 10.** Projections of function $PFD_{avg}$ to the plane $[t,\lambda_D]$ on the $PFD_{avg}$=1e-3 level on the scale of $t\in[0\ldots10000]$ (a) and $t\in[0\ldots2000]$ (b)

For the MSaf6 model for basic values of input parameters (in particular DC=0.5) the requirements of SIL3 are fulfilled in case of $\lambda_D$< 1e-5 1/hr.

## 8 Conclusions

The analysis of ICS functional safety simulation received results showed that:

a) in case of the accounting of secondary manifestation of dangerous failures and detections their diagnostic system (model MSaf2) for base-line values of input parameters reaches the settled $PFD_{avg}$ value = 0.028 that it isn't enough for safety arrangements of the SIL3 level;

b) in case of value of dangerous failures rate $\lambda_D$ = 2.5e-5 (1/hour) the considered system meets requirements of SIL3 during the first 8000 operation hours; for extension of this period till 10000 hours it is necessary to increase spanning by diagnostics to the DC=0.92 level (models MSaf1 and MSaf2);

c) if it is impossible to increase the spanning by diagnostics, then it is necessary to reduce failure density of each channel to $\lambda = 2^*\lambda_D = 4e\text{-}5$ 1/hour for the extension of the temporal period of SIL3 requirements support till 10000 hours (models MSaf1 and MSaf2);

d) for the system with majority device which initiates additional diagnostics of the hardware channels (model MSaf6) a sufficient condition of support of requirements of SIL3 is the spanning by diagnostics DC>0.65.

The developed Matlab-programs which can be used in engineering practice are a subject of practical interest.

The essential lack of the developed models is the absence of taking note of software failures in ICS channels. The accounting of manifestation of software defects and their elimination during rescue and recovery operations as it is described in [8], is the direction of further researches and improvement of the developed models. Also, further researches and improvement of the developed models is to analyze software features and interactions with hardware failures in instrumentation and control system channels.

## References

1. IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements (2010)
2. Sklyar, V.V. Elements of the information and control systems functional safety analysis methodology. Radioelectronic and computer systems 6(40), 75--79 (2009)
3. IEC 61508-6:2010. Functional safety of electrical/electronic/programmable electronic safetyrelated systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (2010)
4. Bahmach, E.S. Siora, A.A. Sklyar, V.V. Tokarev, V.I. Kharchenko, V.S. FPGA-based NPP information and control systems safety accession and provision Radioelectronic and computer systems 7, 75--82 (2007)
5. Langeron, Y. Barros, A. Grall, A. Berenguer, C. Combination of safety integrity levels (SILs): A study of IEC61508 merging rules. Journal of Loss Prevention in the Process Industries 21(4), 437--449 (2008)
6. Al-Kuwaiti, M., Kyriakopoulos, N., Hussein, S.: A comparative analysis of network dependability, fault-tolerance, reliability, safety, and survivability. IEEE Communications Surveys & Tutorials 11(2), 106--124 (2009)
7. Trivedi, K.S., Dong Seong Kim, Roy, A., Medhi, D.: Dependability and safety models. In: Proceedings 7th International Workshop on the Design of Reliable Communication Networks (DRCN 2009), pp. 11-20, IEEE Press, Washington, DC (2009)
8. Ponochovny, Y.L., Siora, A.A., Kharchenko. V.S. Models of dual-channel information management system readiness considering the software updating. Radioelectronic and computer systems 6(70), 135--139 (2014)