

Software and System Engineering to Ensure Patient Safety in Wireless Medical Device Networks

Vijay Gehlot (vijay.gehlot@villanova.edu) and Elliot B. Sloane (elliott.sloane@villanova.edu)

Villanova University

Abstract

The ability to deploy wireless patient monitors using industry-standard IEEE 802.x technologies allows patient mobility and clinical flexibility. However, interconnecting multiple life-critical medical devices from multiple vendors can introduce unintended life-threatening risks unless delivery of critical patient alarms to central monitoring systems and/or clinical personnel is assured. We discuss a formal methods based approach for modeling, simulating, and validating heterogeneous wireless patient care device networks and propose a multi-vendor verification and validation toolkit to improve a hospital's ability to properly implement and manage WMDNs to prevent patient injuries.

INTRODUCTION

The successful creation and adoption of internationally standardized wireless data network (WDN) components based on IEEE 802.11x (a.k.a. Wi-Fi) has been a boon for users of laptop and PDA computers. Large scale adoption and manufacturing has caused WDN prices to plummet, leading to ubiquitous deployment throughout academic, commercial, industrial, public, and home settings. This success has also fed rapid existing or emerging WDN innovations including Wi-Fi (IEEE 802.11a, b, and g), Wi-Max (IEEE 802.11n), Bluetooth (IEEE 802.15.1), and Zigbee (IEEE 802.15.4).^{1,2} Each of these WDNs involves trade-offs of many factors, including speed, interoperability, security, co-existence, battery life, and building/object penetration.

Diverse existing or emerging WDNs in healthcare are depicted in Figure 1, and they include both business and clinical applications. Business oriented examples include wireless bar-coded Supply Chain Management (SCM) in areas like the pharmacy and operating room, patient charge billing automation, and Voice over Internet Protocol (VoIP) communication. Many clinical Wireless Medical Device Network (WMDN) opportunities exist, too, including smart infusion pumps that leverage central pharmacy, drug and patient knowledge banks, Computerized Physician Order Entry (CPOE), mobile clinical monitoring, patient location, point-of-care clinical diagnostic testing, and patient charting.

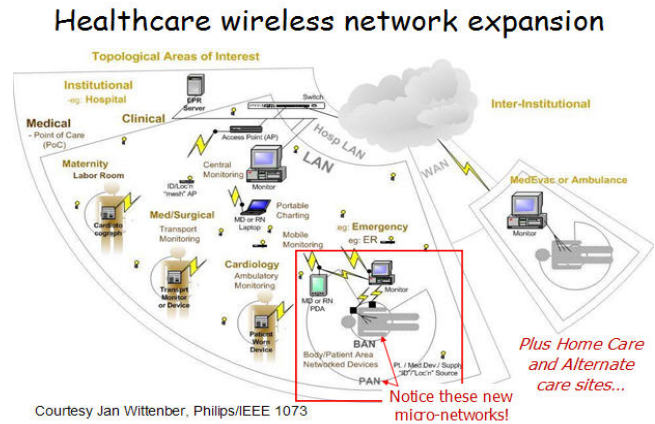


Figure 1. Ubiquity of wireless networks in healthcare

Important emerging innovations, such as the *Operating Room of the Future* project (Figure 2), are likely to deploy WMDN modalities as well (www.orfpnp.org).

Universal wireless interfaces replace hard wires and proprietary data link communications



Figure 2. Operating room of the future using WMDN

General business wireless applications (e.g., creating a purchase requisition) or archive-related WMDN applications that are not life-critical (e.g., retrieval of a mammogram) may coexist with the common and inexpensive WDN devices, especially as available bandwidth continues to increase. To accommodate these types of multi-user data demands, an elegantly simple Collision Sense Method (CSM) is used to handle multiple simultaneous wireless messages which employs random delays to re-sequence the messages. In brief, for many short-burst messages (e.g., a sentence of instant messenger text), this CSM strategy causes few visible delays, even for multiple simultaneous

users. If one or more users are sending large streams of data continuous – like 70 MByte DICOM images from radiology – other WDN users might experience noticeable erratic delays in system response. Although “mission critical” general business data is important, occasional delays can be tolerated. However, many alarms and related clinical information are “life critical,” as depicted in Figure 3. Life-critical data delays, distortions, loss, or other erratic delivery problems could cause serious injuries or death.^{1,3}



Figure 3. Life critical vs. mission critical applications

For example, the unpredictable CSM delay can easily extend beyond the AAMI/ANSI-specified 10-second critical heart alarm period for central arrhythmia monitoring systems.⁴ Furthermore, the randomization of message transfers can completely invalidate intelligent alarm system management such as that specified in IEC/ISO 60601-1-8.⁵

In addition, erratic delay in real-time patient waveforms can interfere with computerized and human interpretation, risking misdiagnosis of illnesses and/or interfering with therapeutic interventions. Lastly, erratic WMDN-induced delays can cause intermittent spurious alarms such as lead-loss or “missing” patients, reducing system trust and greatly increasing “no problem found” complaints and investigations for the IS and BME departments and the manufacturers.

Regardless of the careful planning, procurement, installation, and management that goes into selecting and deploying WMDN systems, by nature there also will be many intentional and unintentional ad-hoc changes throughout the life cycle of these systems.

Clearly, serious patient safety risks can be caused by delayed or lost WMDN alarm and data streams, but, to date, non-proprietary WMDN Verification and Validation (V2) techniques do not exist. Single-vendor and heterogeneous multi-vendor deployment must be considered, as well as safe and reliable coexistence with other IS technologies sharing similar network components. V2 of even a homogeneous single vendor, single device WMDNS is very complex for several reasons including: absence of industry standards or regulations, unconstrained mobility of patients and devices,

and rapid changes in the underlying wireless network modalities.

Also, because the implementation of Decision Support System (DSS) capabilities for life-critical analyses like ECG arrhythmias or drug interactions varies by manufacturer, model, and user configuration, no single proprietary verification and validation strategy can, by itself, universally assure safe and reliable WMDN systems.

In this paper we explore a proposal of using a formal methods based approach as part of the verification and validation of heterogeneous wireless patient care device networks. In particular, we will address, via a suitable formal modeling approach and tool, the safety and performance issues in such networks. Furthermore, since the overall goal of this paper is also to propose development of a prototype Verification and Validation Toolkit (V2T) that will allow the Clinical/Biomedical Engineering and Information Systems departments to ensure safe and reliable operation of WMDN,^{1,3,6,7} this paper will conclude with a brief discussion about such a toolkit.

FORMAL METHODS, SOFTWARE ENGINEERING AND PETRI NETS

A *formal method* is a notation or technique, based on some mathematical theory, for modeling and analyzing systems. The advantage of formally modeling and analyzing a system is to ascertain that it behaves according to specifications and to identify potential problems or misunderstandings. Increasingly, formal methods are considered an integral part of software engineering and system development.^{8,9}

Over the years, several formalisms for modeling and analyzing systems have been proposed. One such formalism is Petri nets.¹⁰ Petri nets are useful for modeling concurrent, distributed and asynchronous behavior in a system. The attractive aspect of a Petri net is its graphical representation. An example Petri net model of a simple vending machine is depicted in Figure 4.

In the Petri net notation, circles (called *places*) represent possible states whereas the bars (called *transitions*) denote possible events. The black dots are called *tokens*. The current state of a system being analyzed is given by the distribution of black dots (called *marking*). In the example net above, a vending machine has two possible states: ready to accept coins (ready) and coins accepted (acc). The possible events are: insert coin (coin), push button to dispense soda (soda) and push button to dispense gum (gum). The current marking indicates that the machine is ready to accept coins. The label 2 on the edge connecting acc and soda imposes the requirement that soda costs two quarters.

Even in this simple scenario there are some interesting questions one may ask about the intended correct behavior. For example, we may want to establish that if soda costs 50 cents and we put 75 cents in, then we get back a soda and 25 cents; also we would not like the machine to dispense a soda if we put in just 25 cents.

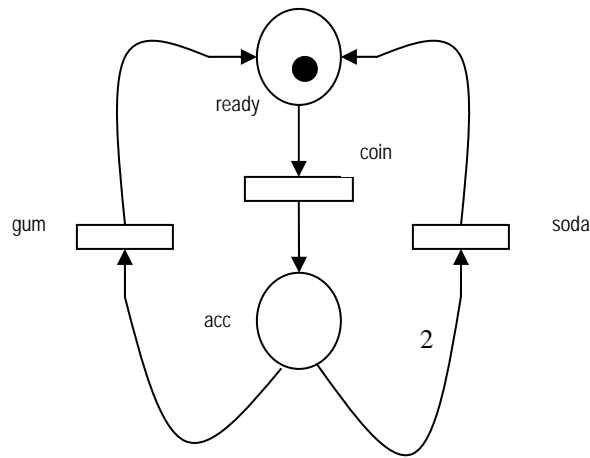


Figure 4. Petri net representation of a vending machine

Similar scenarios arise in healthcare settings. For example, suppose a heart alarm goes off and at the same time a large image file is being transmitted over the same wireless network, what will be the behavior of the network? Will the alarm signal reach the station in time? As mentioned, one way to analyze and answer such questions is to resort to a formal modeling and analysis technique.

AN EXAMPLE WMDN AND ITS CPN MODEL

We consider an example patient monitoring system consisting of various monitoring devices and a central work station connected via a wireless network as depicted in Figure 5. The specifics of the particular scenario we focus on include 10 patients with heart monitors and pulse oximeters and a nurse station with two nurses. In addition, the heart monitors may generate a low battery alarm too.

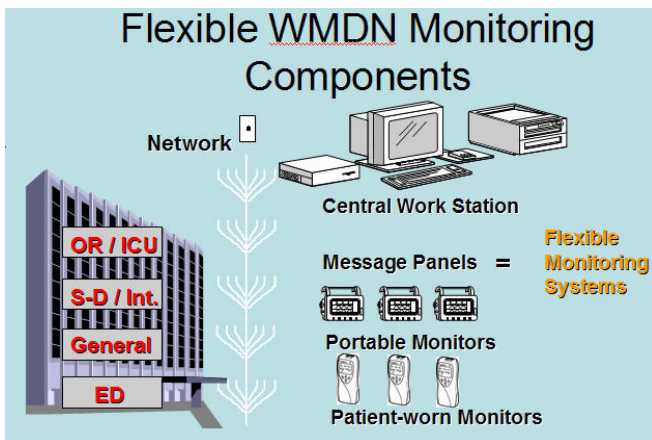


Figure 5. A patient monitoring system configuration

To model this patient monitoring system we chose to use Colored Petri Nets (CPNs).¹⁰ CPNs are an enhancement of Petri Nets in that the tokens have “colors” or types. CPN therefore allows one to trace and control the path and timing of each individual token in the net. We use colors to

distinguish, track, and control various types of alarms that may be generated. Furthermore, the CPN Tool, which is a computer tool for editing, modeling, simulating, and analyzing CPNs employs a powerful programming language called CPN ML (www.daimi.au.dk/CPNTools/). In our case, we define several functions using CPN ML to impose some quality of service requirements. The CPN Tool also includes the timed extension of CPNs which is useful in capturing and simulating temporal behavior of a system. The time concept is based on the notion of a global clock which represents model time (not actual physical time). A token may optionally be declared as a timed token. Such tokens carry a time stamp through simulation. We use the time stamped tokens to govern the availability, generation and handling of various alarms.

Figure 6 depicts this CPN model. In creating this model, we separated three categories (colors) of alarms: Red, Orange, and Yellow. The Red alarms are generated by heart monitors (transition labeled **HMAAlarm**). The Orange alarms are pulse oximetry alarms (transition labeled **POAAlarm**) and the Yellow alarms indicate low heart monitor battery situations that could signal the impending complete failure of a heart alarm monitor (transition labeled **LoBatAlarm**).

The CPN modeling tools handle time-dependent events quite differently than simple stochastic Petri net tools. Because of this, specific software was written to simulate realistic alarm events. The Red heart alarms fired infrequently, as one would expect for recovering patients. The Yellow battery alarms occurred least frequently because good hospital maintenance practices should ensure stable battery performance. The Orange pulse oximetry alarms occurred quite frequently, as they are prone to many false-positives due to patient movement sensitivity. In Figure 6, The oval shaped place labeled **802.11** represents a wireless LAN network access point. All alarms and reset request go through this network fabric. The packet queues are modeled using CPN ML’s list data structure. The central station is modeled as two nurses managing the monitors and alarms (transition labeled **HandleAlarm**).

WMDN SAFETY AND RELIABILITY SIMULATION

We had originally used simple stochastic Petri nets to model such a system.¹¹ Results of that analysis showed that serious overload situations can occur, and that handling of critical alarms may extend beyond several minutes. We further showed that dangerous delays can be reduced by intelligent alarm management at the nurses’ station. It was noticed that there were still situations where the pulse oximetry alarms began to queue up creating a bottleneck situation in the network. We then decided to explore incorporating IEEE 802.11e-style Quality of Service (QoS) techniques into the model. This decision precipitated our shift to CPN, since ordinary Petri nets do not support any

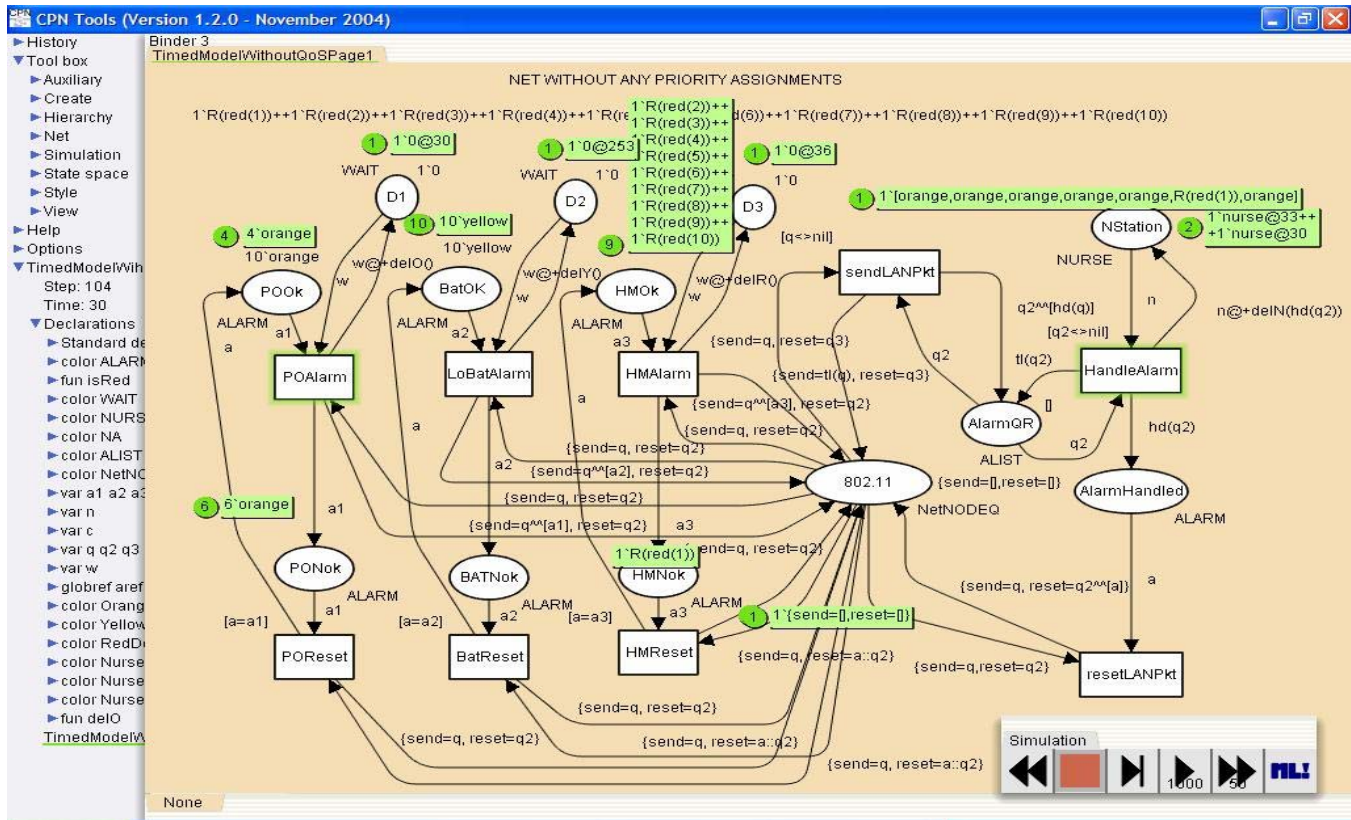


Figure 6. CPN model of a patient monitoring system

notion of priority, because individual or groups of tokens cannot be tracked or handled with unique rules.

We used CPN Tool to create two versions of the model. One without priority management (Figure 6) and one with priority (QoS) management. The modification entailed a priority based queuing policy implemented as CPN ML functions. In essence, these programs were designed to prioritize the passage of Red tokens ahead of Yellow ones, and Yellow ones ahead of Orange ones to ensure that critical heart alarms or heart monitor battery failure alarms propagate ahead of the less critical pulse oximetry alarms. Our simulations runs using these CPN models show a relative improvement of handling of heart alarms when QoS was included. In fact, in many cases the heart alarms were handled almost immediately, and serious delays decreased.

These series of evolving Petri net simulations suggest several practical conclusions:

1. Design and deployment of a wireless patient monitoring network may not be a simple process;
2. Use of common, industry standard 802.11x (Wi-Fi) network components may create an artificial sense of security, as their successful use for less risky network applications is not at all like life-critical medical signals;

3. QoS-compliant network equipment, such as IEEE 802.11e or other proprietary solution, appear to be necessary for life-critical applications;
4. CPN tools, with further refinement, can be programmed to simulate wireless medical device networks with, and without, QoS; and
5. Simulation of network performance with a tool such as CPN Tool may be essential to predict and avoid life-threatening data delays.

CPN Tool also has a graphical interface which allows modules to be copied and/or customized as needed. Because of this, we believe it can be used to quickly represent almost any patient monitoring configuration as part of a toolkit (i.e., almost any number and configuration of patient monitors, wireless network hubs, and central stations, along with accurate priority and decision rules). Unlike most existing tools, this CPN model can allow pre-planning of WMDN by including appropriate components and network element, and rules, and then running simulations to detect problems like insufficient bandwidth, inadequate priority management, deadlock conditions, and unreachable states.

Of course, transceiver interference, physical problems like shielded walls, or conflicting internal device intelligence or rules are not addressed by this model. Therefore, other steps are still needed for complete V2 for WMDNs. The important contribution that this CPN model CAN assure is that when the RF and other issues are properly addressed, the WMDN itself will introduce patient safety risks. Further, as future changes to the WMDN occur, the existing CPN model can

be updated and retested as part of the v2 process for the revised system.

V2T: VERIFICATION AND VALIDATION TOOLKIT

A usable V2T will have to provide a way to validate the safe and reliable initial and ongoing performance of any proposed WMDN system, and to do so, it must document and test all alarm functions, clinical data management, and any other operational data that is included.

Three general verification and validation techniques exist,¹² often referred to as:

1. Black box testing – unknown internal system components or configuration that requires through external testing of all functions and potential failure modes to determine reliability.
2. White box testing – complete internal system details fully known and transparent for testing and observation, which allows complete systemic performance testing.
3. Gray box testing – hybrid situation of Black and White box systems, in which only some internal detail and access is available.

It is expected that the prototype V2T will have to include all three approaches, as some portion of both heterogeneous (mixed vendors and/or models) and homogeneous systems will have hidden (unknown) interactions that must be validated regardless of the situation.

In the case of a completely new system design and installation, a formal, independent validation process is important. This will allow proper specification, valid installation acceptance testing, and periodic systemic revalidation following major system repairs or changes. In keeping with IEEE Software Engineering practices, a validation process such as this can be performed incrementally: first validating individual pieces or modules and then validating subsystems by careful testing of all interface modes and functions. Ultimately, the entire system is validated by testing the combination all subsystems. Manufacturer testing or verification procedures must be considered during this process, but they are rarely site- or situation-specific, and they are often out of date.

Once a complete WMDN system is successfully validated, safe and reliable system performance following individual changes, such as repairing a device or upgrading a piece of hardware or software should be verified and documented by testing critical performance parameters and/or anticipated critical failure modes such as power interruptions. Again, if available, manufacturer documentation may be helpful for portions of this work.

The prototype V2T methodology that we are suggesting should include the following processes and related documentation:

1. Detailed inventory of each device, subsystem, and interface;

2. Identification and selection of appropriate detailed white-, black-, or gray-box testing technique for each device, subsystem, and interface;
3. Simulation of safe and reliable WMDN system performance using CPN;
4. Respecification and/or reconfiguration of WMDN components to address any deficiencies identified in the CPN model in step 3 above;
5. Simulation or site-testing to assure avoidance of RF conflicts;
6. Verification of reliable interoperability of imbedded medical device DSS and intelligent alarm systems, which might also be done with CPN or another formal method tool;
7. Creation of a verification process and documentation package that specifies all tests and results;
8. Determination and documentation of verification intervals and/or criteria;
9. Creation of preliminary verification process and documentation for future repairs, upgrades, and changes;
10. Periodic review of verification and validation procedures and documentation; and
11. Update of the CPN model to support V2 and problem analysis of future modifications.

CONCLUSIONS

This proposed V2T will serve the following critical risk mitigation functions following any WMDN component or system change:

1. Assure patient safety
2. Assure reliable system operation
3. Facilitate pre- and post-installation detection of problem states
4. Assist in diagnosis of problems
5. Assure HIPAA compliance
6. Meet JCAHO alarm management requirements

The risks inherent in creating such a toolkit lie in development and deployment of an inadequate or grossly inefficient V2T. If the V2T is incomplete or inaccurate, it could lead to a false sense of security and, potentially, to selection, installation, and acceptance of expensive WMDN systems that have unacceptable failure or safety characteristics. Further, if the V2T is too complex or grossly inefficient, it may not be practical for any but the most complex and/or expensive projects.

At present, however, no suitable general alternative exists in the market. Vendor-specific validation and verification procedures are rarely fully documented as a matter of proprietary protection. In addition, the vendor will rarely accept any responsibility for customization or mixing other vendor's products with theirs, creating an unacceptable sole-vendor deadlock.

ACKNOWLEDGEMENTS

Special thanks are offered to Rick Schrenker and Ricky Hampton of Partners Healthcare, the Operating Room of the Future project, the National Institute of Standards and Technology, the Welch-Allyn Corporation, and the IEEE 1073 RF Wireless Medical Device Taskforce. Their collective insight and the excellent pictures included in this paper are invaluable to our research.

REFERENCES

1. R. Hampton., "CE Challenges," AAMI Annual Clinical Engineering and Productivity Subcommittee Meeting. June 4, Boston, MA, 2004.
2. J. Wittenber, "Wireless network standard overview for IEEE 1073 Wireless Medical Device working group," as cited in Hampton, 2004, above.
3. D. Cypher, "802.11x and 802.15x Incompatibility Analysis for the IEEE 1073 Wireless Medical Device Taskforce," National Institute of Standards (NIST) February 2005.
4. AAMI/ANSI EC13:2002 Standard for Cardiac Monitors, Heart Rate Meters, and Alarms.
5. IEC/ISO/DIS 60601-1-. 2003 Medical equipment – Part 1-8. General Requirements for safety – Collateral standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems.
6. R. Hampton, Report at IEEE 1073 Wireless Medical Device Working Group at the FDA. March, Gaithersburg, MD, 2005.
7. V. Gehlot and E.B. Sloane, "Colored Petri Net Simulation for Design of Heterogeneous, Multi-Vendor, Integrated, Life-Critical Wireless (802.x) Patient Care Device Networks," Abstract in Americas Computer and Information Society (AMCIS) 2005 Annual Conference, Omaha, NB, July 2005.
8. C.M. Holloway, "Why Engineers Should Consider Formal Methods," In *Proc. 16th Annual Digital Avionics Systems Conference*, October 1997.
9. J.P. Bowen and M.G. Hinchey, Ten Commandments Revisited: A Ten-Year Perspective on the Industrial Application of Formal Methods, In *FMICS '05: Proceedings of the 10th international workshop on Formal methods for industrial critical systems*, September 2005.
10. C. Girault and R. Valk, *Petri Nets for Systems Engineering*, Springer-Verlag, 2003.
11. E.B. Sloane and V. Gehlot, "Applications of the Petri Net to Simulate, Test, and Validate the Performance and Safety of Complex, Heterogeneous, Multi-modality Patient Monitoring Alarm Systems," In *Proceedings of the IEEE Engineering in Medicine and Biology Annual Conference*, September, San Francisco, CA, 2004.
12. National Institute of Standards and Technology (NIST). 1996. Reference Information for the Software Verification and Validation Process (<http://hissa.ncsl.nist.gov/HHRFdata/Artifacts/ITLdoc/234/val-proc.html>)