Phasor Measurement Unit Diagnosing

Mikhail Uspensky
•
Komi SC UD RAS, Syktyvkar, Russian Federation.
uspensky@energy.komisc.ru

Abstract

Based on the global navigation system timestamp an equipment is applied to synchronize the measurement moment in various power buses, which are remote from each other, to measure the current and voltage phasors for the power system control. It is named phasor measurement unit (PMU). This is complex device and it should support the necessary level of reliability for safe power system control. An enhancement of PMU functioning reliability can be obtained by redundancy of its assembled components. Aside from redundancy there is a failure identification task of components for ones from two devices and a concretization of this unit for its replacement. In the paper the failure identification issues are considered for redundancy, and the diagnosing algorithm, which solves these issues, is offered.

Key words: redundancy, diagnostics, reliability, phasor measurement unit.

1. Introduction

A reasonably exact simultaneity of measurements on time by means of Global Navigation Satellite System (GNSS), for example, GPS or GLONASS, allows to perform measurements of power system mode in the various its buses, which are remote from each other, by phasor measurement units (PMUs). They allow determining of the measurement phasor from simultaneous measurements of instant current or voltage values on the ends of the transmission line. Each measurement is marked by the timestamp. PMU is rather complex electronic device which it is possible to show in picture by seven integrated blocks [1], figure 1. Functions of such blocks are clear from their names, UTC is Coordinated Universal Time in which timestamps register from GNSS, SPS is a Synchronizing Pulse for measurement Sampling, simultaneity for instant measured values by all system PMUs.

The following Section is devoted to detection issues of PMU module unavailability. The PMU diagnosing algorithm taking into account detection features of its block unavailability is given in Section 3. Results of work are given in Section 4 – the conclusion.

2. Detection Issues of PMU Unavailability

An importance of failure identification for PMU elements is noted by many specialists, for example [2]-[4]. It is shown in work [5], PMU hardware reliability is estimated at occurred failure of any element or group of elements, which cause functioning failure of the device. Other words, it is PMU unavailability. However its functional reliability increases with channel PMU duplication, but also its partial unavailability increases too, if one from parallel elements is failed, since the number of elements of possible failure doubles. Besides, partial unavailability exists in two states. Firstly, when the device executes its functions correctly even with any failed elements, until the changing conditions do not lead to using of these failed elements. The device is revealed the down

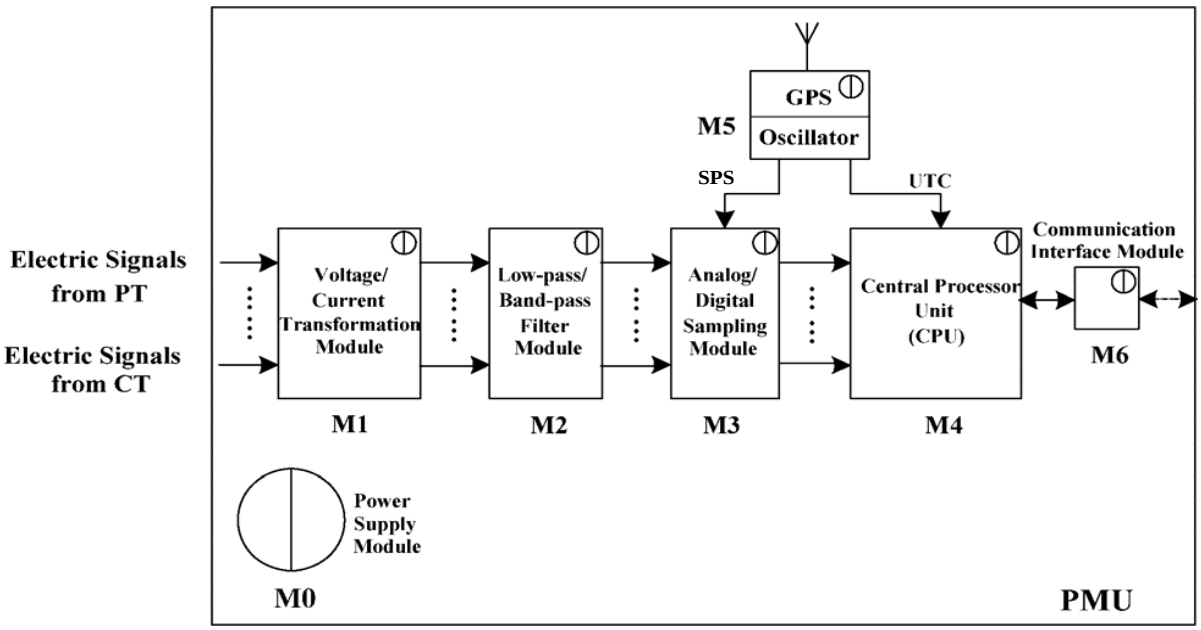

Figure 1: *Structure of PMU,* [1].

state only now (the system does not execute given functions). Secondly, when failed elements lead to the wrong solutions, for example, if information distortion is happened, because of failure takes place with any counters, registers or storage cells, but this element failure can't be detected. Such state types are related to the so-called hidden failures. One more failure cause can be connected with errors of the software.

The failure or error identification of the duplicated system usually is executed by diagnostics methods. The hidden hardware failure emergence is detected by comparison of results on an output of each channel by means of microprocessor of another channel. If the difference of output channel values is more than the accepted error ε

$$\left|x_{pmt1} - x_{pmt2}\right| = \Delta_{com} > \varepsilon ,$$

then it specifies that one of channels passed into an unavailable state. Here x_{pmt1} or x_{pmt2} is the output value measured by the first and second cards. Comparison of results of identical blocks of cards allows revealing a failed unit, and, therefore, PMU card. Card block testing should reveal the failed channel plate. Thus data receiving and processing does not interrupt because duplication. Since such comparison is executed by the device processors of both cards, processor failures and malfunction appear under control too. An important point of check is the order of the element testing which should be such that the following test makes the elements which passed testing on the previous step.

3. PMU Diagnosing Algorithm

It is possible to select four points for result comparison of each card work (arrows to CPU, fig. 2) at identification of a failure zone. The algorithm of such check is given in fig. 3. Since power sources are switched on parallel through a diode junction, providing power supply of both channels, their operation is tested simply, another module supplies both PMU channels at failure the one of two sources. Here it is enough to monitor, that levels of each source supply voltages is in tolerable limits with the selected period. Since output results $x_{pmt,i}$ of both cards coincide, then failure in measuring channels is absent; such testing is carried out by own plate processor. Otherwise own card source is determined as faulted by the CPU, which supplies from another card source.

The following point is comparison of output values of PMU cards. If their difference exceeds admissible value ε, i.e. one of cards works incorrectly, the process of failure card detecting is initiated. Such process is executed in parallel by each card. It begins with the built-in self-testing of the processor block, memory and the output interface. The result of testing is read by the parallel card processor. Self-examination in Sitara AM335x microprocessors with a Cortex-A8 kernel by the Texas Instrument company [6] can be an example of such testing. At negative result the faulted card is brought out of work with the message to the duty personnel. In case of positive result the third point is tested, it is communication block between PMU and GNSS and the card internal oscillator of time. GNSS receiver SN-4706 by the Russian «Design Bureau of Navigation Systems» Joint-stock Company Navis Inc. Design Bureau [7] or the PA6H module with the MT3329 crystal by the Adafruit Industries company [8], which both can work with the Russian GLONASS or with American GPS, for example. Simultaneous reading of time indications for some periods and calculation of the set period value Δt

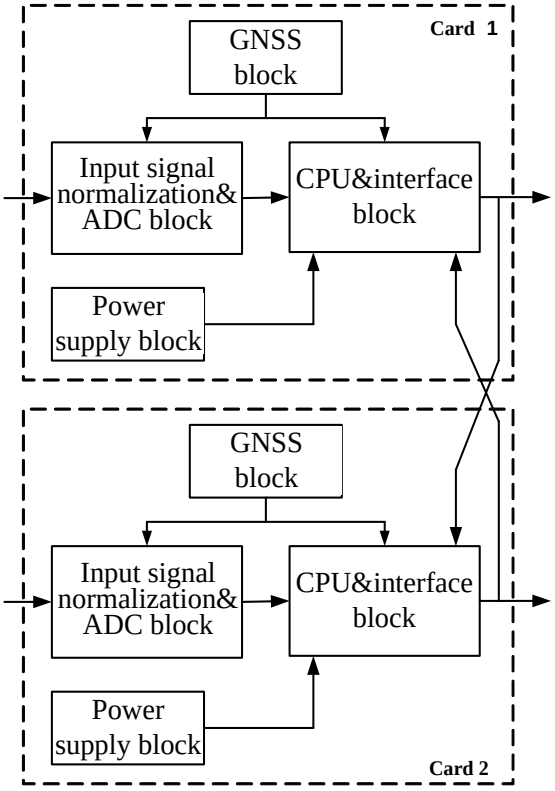

Figure 2: *PMU card combining at duplication*

$$t_{n+2} - t_{n+1} \neq t_{n+1} - t_n \neq \Delta t$$

points incorrectly working block, where t_{n+i} $i = 0, 1, 2, \ldots$ is the timestamps accompanying the corresponding measurements.

Otherwise transition to the following point of comparison takes place. Output registers of the analog-to-digital converter (ADC) are tested. Here operability of the card analog part is detected: the signal normalization block of current and voltage, the block of low-frequency bandpass filters, ADC and communication block with GNSS, in a certain degree. Simultaneous ADC values of cards differ, if time signal fault takes place for one of channels. But it become clear in the previous test. Here it is necessary to get test signals through ADC, i.e. zero and reference voltage. The zero signal allows to reveal deviations in channel analog part and bits of channel digital part, which are faulty being in unit status. The reference voltage input corresponding to a unit status of all bits for a channel bit grid allows to reveal changes of gain ratio in channel analog part and changes of bits in channel digital part, which are faulty being in zero status. The modern ADC equipment usually has self-examination means which can be caused if necessary, for example, in SPC56EL60 system by the ST Microelectronics Company [9].

If both cards did not reveal the listed deviations, it is obvious that technical part of PMU cards is workable, and failure is not connected with element fault of these cards. Let's remind that it is important to reveal not so the failed block, as a failed card, and the approach described above provides such action.

It is more difficult to test the software. Simple duplication of programs will not lead to error identification as operations are identical. Therefore except careful software testing at its developing it is possible to offer use of different algorithms for receiving identical indexes. Such approach allow to reveal a software errors and failures as in the debugging course, so in PMU work that significantly improves software reliability.

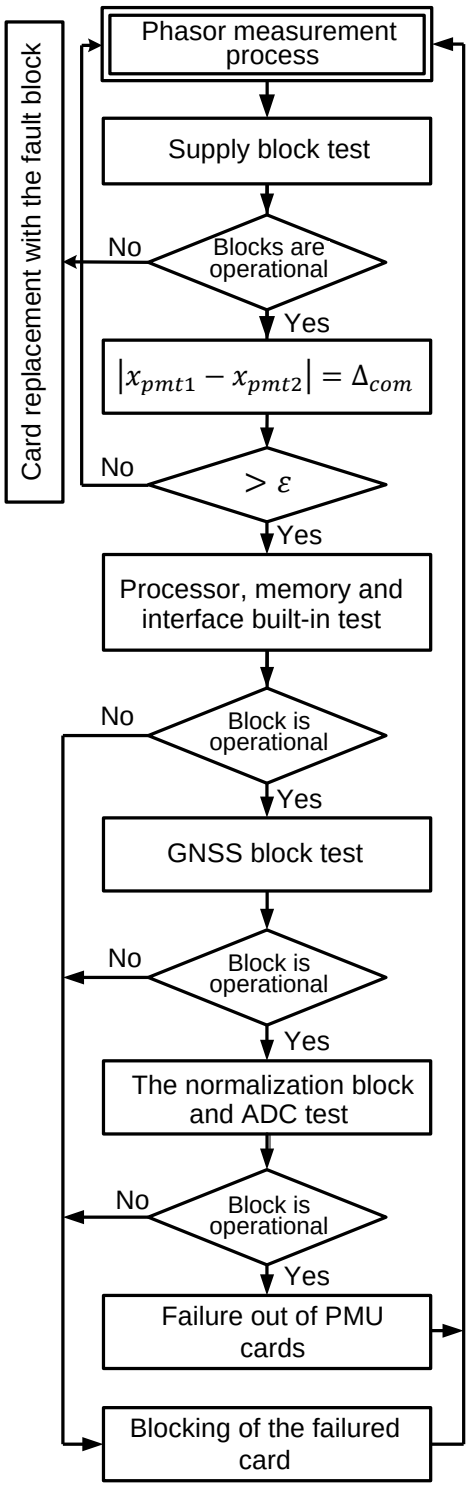

Figure 3: *Identification algorithm of the failure card.*

By considering of PMU functioning reliability, it is worth to remember about reliability of used GNSS system which depends not only on reliability of own elements, but also a number of external influences [10].

4. Conclusion

Since phasor measurement units are used to monitor power system modes, high requirements for their reliability of hardware are imposed to them. Such reliability can be provided with PMU duplication. Here it is important to reveal the event of PMU technical failure in real time. Then it is necessary to detect namely failed card with the purpose of its blocking and the subsequent replacement.

Such check algorithm, in which the step sequence provides testing of the element in the following step with use of the elements that are checked on the previous step, is offered. Failure Δ_{com}identification is performed by comparison of results from card output values for the same moment in time. The test results of the microprocessor, memory and the output interface are detected by the processor of another card. Monitoring specifics of the power supply units are determined by the period check of supply voltage levels.

The given diagnosing system of the duplicated PMU provides the values of hardware availability for such device $A = 0.99974$ [5].

References

[1] Wang Y., Li W., Zhang P., Wang Bi., Lu J. Reliability Analysis of Phasor Measurement Unit Considering Data Uncertainty // IEEE Transactions on power systems, Vol. 27, No. 3, August 2012. – Pp. 1503-1510.

[2] Shneerson E.M. *Digital relay protection* / M.: Energoatomizdat, 2007. - 549 p. (In Russian).

[3] Gurevich V. I. *Microprocessor protection relays. Device, issues, perspectives* / M.: Infra- Inzheneriya, 2011. - 336 p. (In Russian).

[4] Gipkina A.P., Pevtsova L.S. Program reliability estimation of microprocessor relay protection // Naukovedeniye Inter-Log, Vol.7, No. 2, 2015. – Pp. 1-10. *Available*: http://naukovedenie.ru/ (In Russian).

[5] Uspensky M. I. Functioning reliability estimation of the phasor measurement unit //Relay protection and automation. 2017, No. 3. – Pp. 33-38. (In Russian).

[6] Samarin A. Sitara AM335x - a new microprocessor line for industrial applications with the Cortex-A8 kernel // Components and technologies, 2012, No. 3. – Pp. 57-64. *Available*: http:// www.kit-e.ru/ (In Russian).

[7] Morozovsky Yu. The domestic navigation GLONASS/GPS receiver is approved // Wireless technologies, No. 1, 2009. – Pp. 26-28. *Available*: http://elibrary.ru/ (In Russian).

[8] Adafruit Ultimate GPS / Last updated on 2017-02-20 01:12:52 AM UTC – 38 p. *Available on*: https://learn.adafruit.com/adafruit-ultimate-gps/

[9] AN3324 Application note. Implementing power-on self tests for SPC56EL60 in locked step / Doc ID 18311 Rev.2, September 2013. – 37 p. *Available on*: www.st.com/

[10] Uspensky M. I. Natural issues of time synchronization in WAMS system // Methodical questions of research of reliability of big systems of power. Iss. 67. Syktyvkar, 2016. – Pp. 396-402. (In Russian).