CONF-890555--19

CONF-890555--19

DE89 015692

DEVELOPMENT AND APPLICATION OF DIAGNOSTIC SYSTEMS TO ACHIEVE FAULT TOLERANCE*

by

Ronald W. King
Ralph M. Singer

EBR-II Division
Argonne National Laboratory
P. O. Box 2528
Idaho Falls, Idaho
83403-2528

The submitted manuscript has been authored by a contractor of the U. S. Government under contract No. W-31-109-ENG-38. Accordingly, the U. S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U. S. Government purposes.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Submitted for Presentation
at the
Seventh Power Plant Dynamics, Control
and Testing Symposium

May 15-17, 1989
Knoxville, Tennessee

Received by OSTI

JUL 26 1989

MASTER

* Work supported by the U. S. Department of Energy, Office of Nuclear Energy under Contract No. W-31-109-ENG-38.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

DEVELOPMENT AND APPLICATION OF DIAGNOSTIC SYSTEMS TO ACHIEVE FAULT TOLERANCE*

R. W. King
R. M. Singer
Argonne National Laboratory

ABSTRACT

Much work is currently being done to develop and apply diagnostic systems that are tolerant to faulted conditions in the process being monitored and in the sensors that measure the critical parameters associated with the process. A fault-tolerant diagnostic system based on state-determination, pattern-recognition techniques is currently undergoing testing and evaluation in certain applications at the EBR-II reactor. Testing and operational experience with the system to date has shown a high degree of tolerance to sensor failures, while being sensitive to very slight changes in the plant operational state. This paper briefly mentions related work being done by others, and describes in more detail the pattern-recognition system and the results of the testing and operational experience with the system at EBR-II.

Introduction

In order for a process operator or automatic control system to take appropriate control action or decide to take no action in response to an indicated abnormality in process operation, there must be assurance that the indication being received does, in fact, represent actual process or equipment conditions. This implies that a distinction must be made between readings from faulted and unfaulted instruments, and that an accurate determination of the value of a critical parameter must be provided even though the sensor measuring that parameter may have failed or degraded. In other words, the system must have a high degree of tolerance to faulted instrumentation including single and multiple faults. If the operator does not have a high degree of assurance that the indicated reading is correct, he has to make a decision on whether to take the action that is called for if the indication is correct, or assume the indication is incorrect. Since the action that may be called for in response to an indicated reading may be somewhat drastic, the operator may be hestitant to take that action until some other evidence is available regarding the validity of the indication. His decision about the validity of the indication, if incorrect, could have serious consequences.

---

* Work supported by the U. S. Department of Energy, Office of Nuclear Energy, under Contract No. W-31-109-ENG-38.

As a simple example that may occur to any of us, assume we are driving our expensive automobile on a very busy, fast turnpike that has no pull-off space on the side for several miles. Suddenly, the engine oil-pressure warning light comes on. There are tough choices to make. We either assume the indication is right or that it is wrong. All we know is that there is a fault; either the instrumentation is faulted or the process (the engine lubrication system) is faulted. The consequences of making a wrong decision about the validity of the indication are that if we keep going and the indication is correct, the engine would be ruined (very expensive), or risk life and limb by stopping on the turnpike, perhaps unnecessarily if the indication is wrong. This is a very simple situation compared to the situation that an operator of a large, complex process (such as a nuclear power plant) is in when he receives an indication of a serious plant abnormality. The potential impact of his decision on how to respond is several orders of magnitude greater.

The importance of providing a validated indication to the operator is extremely important to enable him to take immediate action without hesitation due to uncertainty about the validity of the indication. If the sensor providing the information has failed or degraded, an alternate means of providing the correct information to the operator must be provided in order to enable him to take appropriate action. Thus the system, in order to be tolerant of sensor/instrumentation faults, must be able not only to identify faulted instrumentation, but also provide a valid sensor value even under faulted conditions.

Much work is currently being performed to investigate ways to achieve fault-tolerance in diagnostic systems, particularly in the area of fault detection and sensor validation. Notable work being done in this area includes a signal validiation project at the University of Tennessee involving the integration of parallel diverse signal processing modules, each of which incorporates a different signal processing technique. These techniques include single and multiple variable consistency checking, process empirical modeling, signal anomaly detection and characterization, and other techniques [1,2]. Other work on sensor failure detection at the Univeristy of Tennessee has been directed toward the development of a non-linear model of a process that is used for prediction of the values of critical signals for comparison with the actual sensor readings [3].

An expert system for sensor validation and diagnostics has been developed at Ohio State University, that incorporates hardware and analytic redundancy, and expert knowledge of "normal expectations" of sensor data relationships under different conditions to identify questionable sensor values. It then employs the use of other sources of knowledge such as logical

diagnostic conclusions, analytic calculations, and relationships between unlike sensors to validate or reject the questionable sensor readings [4].

Some of the earlier work on fault isolation and signal validation has been performed at the Charles Stark Draper Laboratory [5,6]. Several other projects to develop fault-tolerant diagnostic systems are underway both in this country and in other countries. Additionally, intelligent display methods are being developed and tested which also provide a degree of sensor validation and fault detection [7].

One of the techniques currently in use and undergoing further development and testing at EBR-II in conjunction with E I International, is based on pattern-recognition, state determination methods. This system is called the System State Analyzer (SSA). In general terms, the SSA is somewhat related to many of the above mentioned techniques, and it has some characteristics that are similar to neural networks [8].

Pattern-Recognition, State-Determination-Based Diagnostics

The SSA, in different forms, is in various stages of development, testing, and application at EBR-II. The SSA has been developed specifically to be tolerant of instrumentation faults by being able to identify faulted instruments and provide a reasonably accurate estimated value for that instrument reading. This estimated value is based on previously learned pattern relationships with readings from other instruments that are similarly related to and define the process being monitored. The SSA has demonstrated a high degree of tolerance to sensor faults during plant tests and during normal plant operational surveillance. The SSA was also developed to be able to detect a change in the operational state of the process and provide information about the characteristics of the new state and what caused the state change. This can be a change to a different valid operational state or to a faulted state.

The SSA process begins with identification of system operational states over a learning period of system operation. Then the SSA compares new observed data with the learned state patterns. The SSA then establishes an estimated state based on the similarities with previously learned states. The estimated state is "built" using a weighted combination of learned states, the weighting value being determined by the degree of pattern overlap with each learned state. The estimated state contains a new estimated value for every parameter being monitored, including estimated values for sensors that have degraded or failed, assuming sensor data was available during the learning process. Because the estimated signal values are based on actual established relationships with the values of all the sensor signals in the signal group representing the process, the failure or degradation of any sensor has an insignificant effect on the SSA estimated value for that sensor signal.

SSA Methodology

In the SSA, the state of a system, whether a learned state or an observed state to be monitored, is represented by measured quantities instead of analytically derived parameters. The SSA methodology is based on using a collection of observations (learned states) of the measured quantities to create a data matrix. A state estimation is then made using only the current observation and the learned state data matrix. The SSA algorithm calculates a set of linear combination coefficients for all of the learned states based on the current observed state and uses all of these coefficients to create the estimated state. The estimated state includes an estimated value for each individual signal in the signal group being analyzed.

This methodology gives the SSA the property of essentially ignoring faults in individual signals during the system state estimation process. The estimation for the faulty signal is essentially unaffected because it is based primarily on the other signals in the signal group and the previously learned pattern relationships. The SSA methodology involves no fitting and no convergence criteria. The SSA uses a single-pass equation which is always solvable, thus making it fast and robust.

As capable as the SSA methodology is in detecting system and instrument faults, it is only as good as the learned domain of system operation. The SSA, while being able to detect, flag, and characterize observed states that are outside of the learned domain, cannot provide reliable estimates for individual sensor readings when the system state has gone outside the domain. The boundaries of the learned domain are defined by the outlying or outermost learned states in the learned state collection. The learned domain can be narrow or broad depending upon the type of system diagnostics desired. The establishment of a valid learned domain is critical to proper SSA application and interpretation of the SSA analyses.

SSA Output Displays

An important feature of the SSA is the output display which provides to the operator or engineer the diagnostic information being generated by the SSA algorithm. Figure 1 is an example of an SSA output display called a signature plot which shows the distribution of actual system signals at a point in time, relative to the SSA estimated values which are represented by a horizontal line through the center of the plot. The vertical bars above the line to the left represent signals that are higher than the estimated values, and those below the horizontal line to the right represent signals that are lower than estimated. The signal deviations from estimated values are shown normalized to the average signal deviation for the entire group of signals, so that the height of a vertical bar indicates a multiple or a fraction of the average percent deviation for the group.

The average signal deviation from estimated values for the group at that point in time is shown at the top center of the graph. This value is very important for detecting process state changes, for differentiating between signal failures and process state changes, and for determining if the process is operating within the learned domain. The distribution of signals is shown as an ordered list from left to right showing in descending order those signals that deviate most in the positive direction on the far left, crossing over the horizontal line near the center indicating signals that are close to or right on estimated values, and continuing to the right with signals that are lower than estimated. The "X"s and the curve drawn through them are overlaid as an indication of an expected normal distribution of signal deviations as a multiple from 0 to 3 times the average deviation. Two vertical lists of numbers on the far left and far right sides of the plot indicate those signals that are three average deviations or more above or below the estimated values.

Another type of SSA output display is the individual signal plot as shown in Fig. 10. This type of plot is a time history plot that shows a DAS channel value plotted over time, the SSA estimated value for the same DAS channel plotted over the same time period, and an upper and lower "uncertainty boundary" above and below the SSA estimated signal trace representing relative uncertainty of the estimate based on how well the current data patterns are fitting into the learned domain.

SSA Test Experience at EBR-II

The SSA has been undergoing performance and operational testing in various forms at EBR-II for the past three years. The most significant results have been achieved using the "on-line" SSA software (in FORTRAN) that has been installed on the EBR-II Data Acquisition System (DAS) computer and runs in the background while the DAS performs its primary function of data collection, display, and storage. This version of the SSA uses one-minute signal averages from the DAS data log. The signal group being monitored consists of 115 signals representing the heat generation and transfer process from the reactor core to the primary, secondary, and steam systems. Many of the signals come from key plant parameter sensors measuring sodium flow rates, core inlet and outlet temperatures, and neutron flux.

The tests described below show first, the ability of the SSA to detect and characterize minor plant state changes simulating a faulted process, and then the ability to detect a faulted signal condition and provide a "correct" estimated value for the faulted signal.

The first two EBR-II plant tests discussed here were designed for characterization of the System State Analyzer. The purpose of the first test was to investigate the response and sensitivity of the SSA during a slow 1 MWt power decrease from normal full reactor power. The purpose of the second test was to

investigate the response of the SSA to a slow reduction in secondary sodium flow from normal full flow rate down to ~97 % of normal flow. The set up for these first two tests consisted of establishing a narrow learned domain from data recorded between 5:40 and 7:40 on the morning of the tests. Eleven equally spaced learned states were established during this time period. The choice of eleven learned states is somewhat arbitrary; experience has shown that this number works well, but no studies have been done yet to optimize the number of learned states for a particular application. The narrow learned domain established just before the test period provided assurance that the pre-test plant conditions would closely match the learned domain.

The first test was initiated at 9:41 a.m. with slight movement of the controlling rod intended to slowly drop power about one-third to one-half of the 1 MWt total power reduction planned. No adjustments were made to any other plant parameters during this test. The SSA signature plot of the plant taken just before initiation of rod movement indicated an average signal deviation of 0.03 % from estimated values which is very good steady state agreement as expected (Fig. 1). The next update of the SSA one minute after initial rod movement (Fig. 2) indicated that the average signal deviation had doubled to 0.06 %, and six nuclear-power-related DAS channels were being flagged abnormally low by the SSA. The next one-minute update (Fig. 3) indicated a 0.09 % average deviation and indicated two thermal-power-related channels being low in addition to the nuclear channels. This trend continued as the power level was reduced to the targeted value at about 9:52. The maximum average deviation value reached shortly after that time was 0.35 % as indicated on the signature plot show in Fig. 4. This demonstrated the capability to detect and diagnose what could be a process fault simulated by reactor control rod movement.

After completion of the power reduction, the controlling rod was slowly returned to near its starting position (a slight adjustment was made to allow for fuel burnup) at 10:21 a.m. A slight overshoot in power level was experienced as the reactivity feedback effects came into play. This can easily be seen in the signature plot recorded at -110 minutes (Fig. 5) showing the signal shift to the high end of the plot, compared with the signature plot shown in Fig. 4.

After the plant was returned to and stabilized near the pre-test conditions, the second test was initiated at 10:35 by reducing secondary flow by about 1 %. The pre-test signature plot is shown in Fig. 6, indicating an average deviation of 0.04 % and showing a well balanced plot. The first update after the start of the test one minute later indicates an average deviation of 0.06 % and flags three secondary-flow-related signals as "leading" the transient (Fig. 7). Secondary flow was reduced one more 1 % step, and then two 0.5 % steps for a total flow reduction of about 3 % from normal full power conditions.

The final flow reduction was completed at 10:53. The maximum average signal deviation reached was 0.58 % at 11:05 (Fig. 8). Secondary flow was returned to initial conditions at 11:38. The plant was allowed to stabilize at pre-test conditions; the SSA average signal deviation returned to 0.04 % by 11:50 (Fig. 9), and the test was terminated at 11:54.

The next test was performed to investigate the ability of the SSA to provide an accurately estimated value for an important plant parameter when the sensor that provides the parameter measurement has degraded and no longer provides a valid signal. Also, as part of this test, multiple signal failures were introduced into the system on a sequential basis to determine the effect of multiple signal failures on the SSA estimated values for key parameters. The test was performed during normal full power operation of the plant. The "signal failures" were introduced on-line by changing conversion units in the DAS computer software to provide output values that represented different sensor/signal failure modes. No actual plant changes were made during the test, the plant remained at steady-state full power operation for the duration of the test.

During the test, a reactor core DT channel (DAS No. 97) was monitored as the reactor parameter of interest. Both the DAS-indicated value and the SSA estimated value were monitored throughout the test. The same signal map containing 115 DAS channels was employed for this test as for the two tests described above. The test started with a simulated partial and then complete failure of the monitored core DT channel (No. 97) resulting in the a drop from the pre-test value of ~180 deg. F to an indicated 170 deg. F, and then to 0 deg. F. This can be seen on the DAS/SSA plot (Fig. 10) where the change in DAS reading occurs at -172 and -164 minutes. There is no observable change in the SSA estimated value for DT even though the simulated failure has caused significant changes in the "measured" value.

The DAS DT channel was returned to normal at -156 minutes. Beginning at -145 minutes, several more simulated signal failures were introduced. All of the failures introduced directly affected one or more signals in the SSA signal map. Some of these failures directly affected the core DT channel value on DAS, as can again be seen in Fig. 10 beginning at -145 minutes. Again, the SSA estimated value for core DT was essentially unaffected throughout the test. A total of 14 signals (12 %) out of the total of 115, were degraded significantly or failed completely. The SSA responded with an increasing uncertainty band on the estimated value as more signals were failed. The test was terminated at -66 minutes by restoring all DAS channel readings to their correct values.

SSA Operational Experience at EBR-II

Use of the SSA as an engineering surveillance tool for periodic monitoring of EBR-II plant conditions has resulted in some interesting observations during normal plant operations. In several instances, the SSA has detected signal problems. These have ranged from instrument drift to sensor failures. The most notable of these occurrences was observed in 1988 with the degradation of a thermocouple (TC) measuring mixed-mean reactor coolant temperature in the reactor outlet pipe. This measurement provides the basis for the reactor core DT determination and is used by the reactor operator as a control parameter. The TC degradation mode resulted in a drop in the indicated temperature, resulting in a drop in indicated core DT of about seven degrees over a period of about 40 minutes beginning with a one degree drop, then continuing down on a jagged decline. Over this same time period, the SSA estimated value for this core DT channel came up about one-half degree shortly after the drop in indicated DT, and then held steady. Later analysis indicated that the reactor operator, observing an indicated drop in core DT, raised reactor power very slightly to compensate. He then observed that the indicated core DT was not responding to his action and switched to other core DT indicators for plant control and held the plant steady. The SSA estimated value continued to provide an accurate estimate of the DT value during the TC failure and responded properly to the slight power increase [9].

The SSA is currently being used for pattern comparisons of EBR-II plant states at different times during a reactor run and from run to run. Specific applications are to assist in plant power level determinations, and to search for system abnormalities that may be indicative of short or long-term system or component degradation. It has also been used for plant transient test monitoring, and for comparison of initial pre-test plant conditions with pre- and post-test conditions from a previous test. Other developments ongoing include the development (by EI International) of a digital feedwater controller that includes on-board signal validation using the SSA pattern-recognition technology, and the development of an SSA version in "C" that runs in near real time, and provides the basis for a real-time hierarchical diagnostic and signal validation system that is being integrated into the model-based display system under development by the EBR-II Division of Argonne National Laboratory.

Conclusions

The development of fault-tolerant diagnostic systems is progressing along several paths. The development and use of a pattern-recognition, state-determination methodology as the basis for fault-tolerant diagnostic systems has been very successful in tests and initial applications at the EBR-II reactor facility. The SSA algorithm is inherently fast and can therefore be incorporated into systems requiring near real-time diagnosis, and it is robust in the sense that it will always provide an answer

and an indication of the degree of uncertainty of the answer, even when multiple input failures have occurred. It is these features that are important to the development and application of fault-tolerant diagnostic systems. The SSA technology is generic to the extent that many different types of applications are being developed with little or no change required in the basic SSA algorithm.

Combining the SSA technology with other technologies, particularly in the artificial intelligence/expert system area, is beginning to show potential particularly for the development of powerful and fast diagnostic and automatic control systems.

References:

1. B. R. Upadhyaya et al., "An Integrated Approach For Signal Validation in Nuclear Power Plants," Proceedings of the ANS Topical Meeting on Artificial Intelligence and Other Innovative Computer Applications in the Nuclear Industry, Snowbird, Utah, August 31-September 2, 1987, pp. 167-174.

2. B. R. Upadhyaya et al., "An Integrated Architecture for Signal Validation in Power Plants," Third IEEE International Symposium on Intelligent Control, Arlington, Virginia, August 24-26, 1988.

3. Z. Frei and B. R. Upadhyaya, "Automated Generation of Nonlinear System Characterization for Sensor Failure Detection," 27th IEEE Conference on Decision and Control, Austin, Texas, December 7-9, 1988.

4. S. Hashemi, B. K. Hajek, and D. W. Miller, "An Expert System for Sensor Data Validation and Malfunction Detection," Proceedings of the ANS Topical Meeting on Artificial Intelligence and Other Innovative Computer Applications in the Nuclear Industry, Snowbird, Utah, August 31-September 2, 1987, pp. 149-156.

5. A. Ray, M. Desai, and J. Deyst, "Fault Detection and Isolation in a Nuclear Reactor," J. of Energy, Vol. 7, Jan-Feb 1983, pp. 79-85.

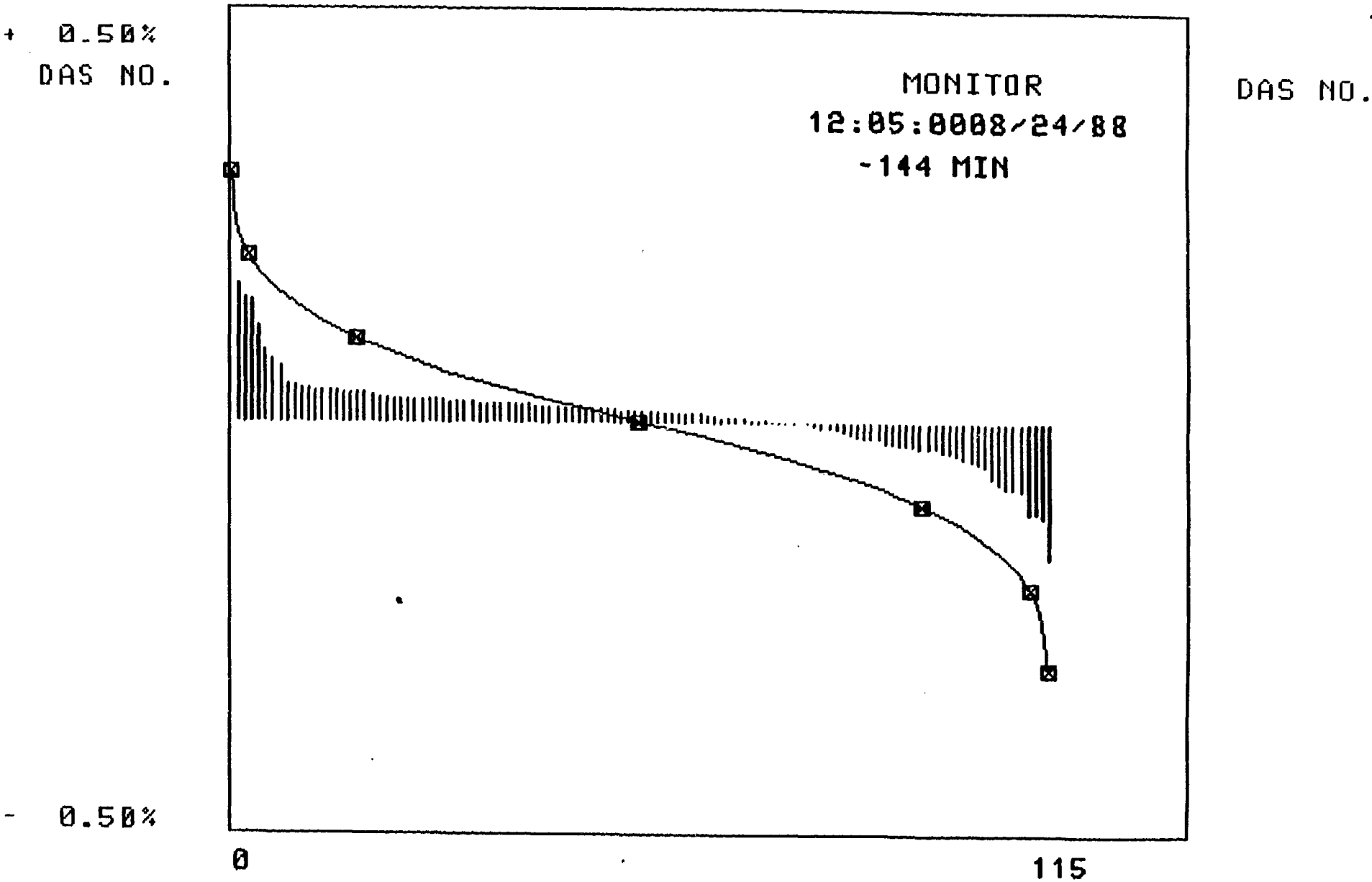
6. A. Ray, J. A. Bernard, and D. D. Lanning, "On-line Signal Validation and Feedback Control in a Nuclear Reactor," Fourth Power Plant Dynamics, Control & Testing Symposium, Knoxville, Tennessee, 1983.

7. R. W. Lindsay and J. D. Staffon, "Experience With Model-Based Display for Advanced Diagnostics and Control," Seventh Power Plant Dynamics, Control & Testing Symposium, Knoxville, Tennesse, May 15-17, 1989.

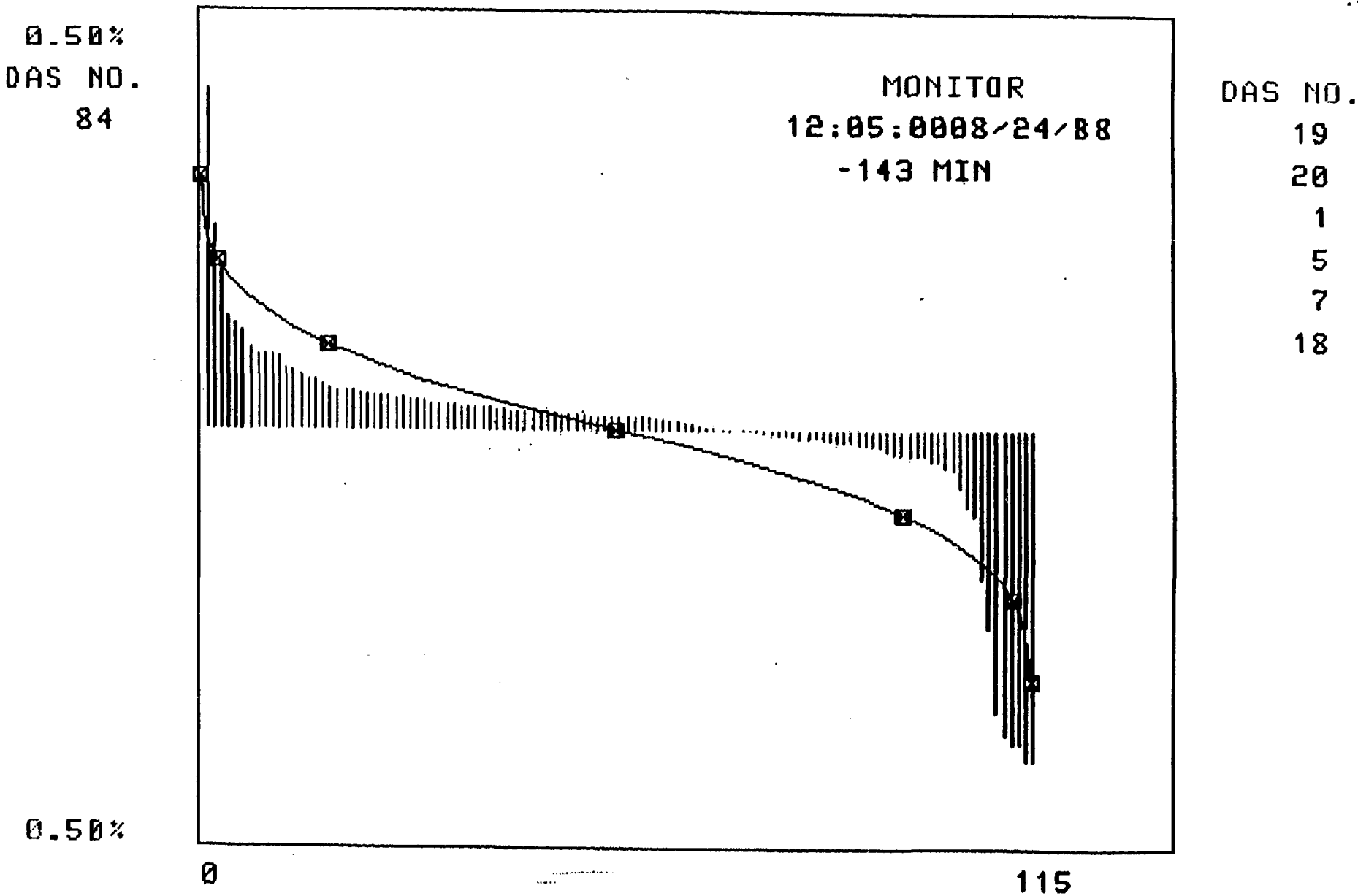
8. R. E. Uhrig, "Use of Neural Networks in Nuclear Power Plants," Seventh Power Plant Dynamics, Control & Testing Symposium, Knoxville, Tennesse, May 15-17, 1989.

9. R. W. King, W. H. Radtke, J. E. Mott, "Pattern-Recognition System Application to EBR-II Plant-Life Extension," Proceedings of the ANS Topical Meeting on Nuclear Power Plant Life Extension, Vol. II, Snowbird, Utah, July 31-August 3, 1988, pp. 512-518.

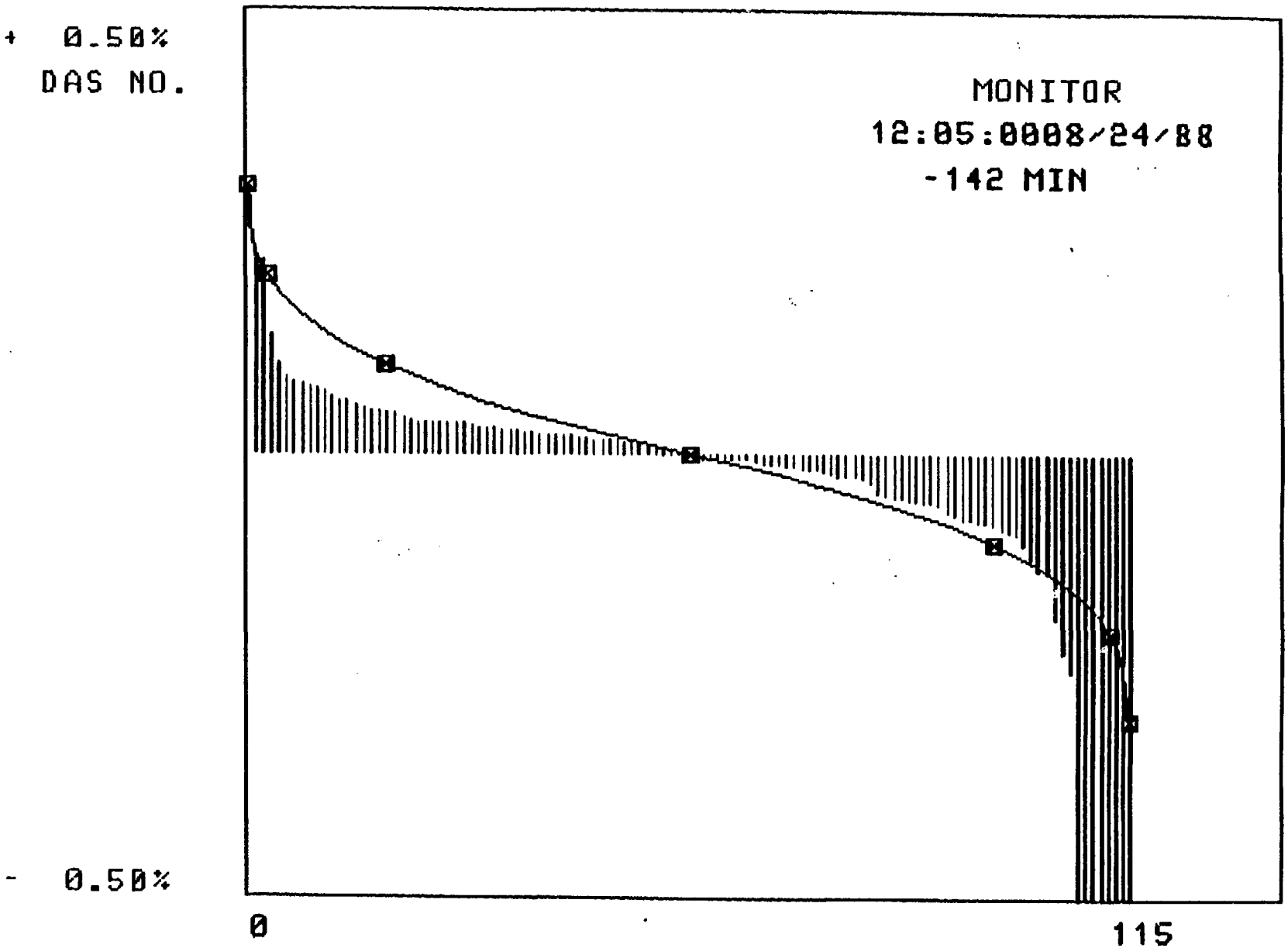
AVE DEV = 0.03 PER CENT



AVE DEV = 0.06 PER CENT

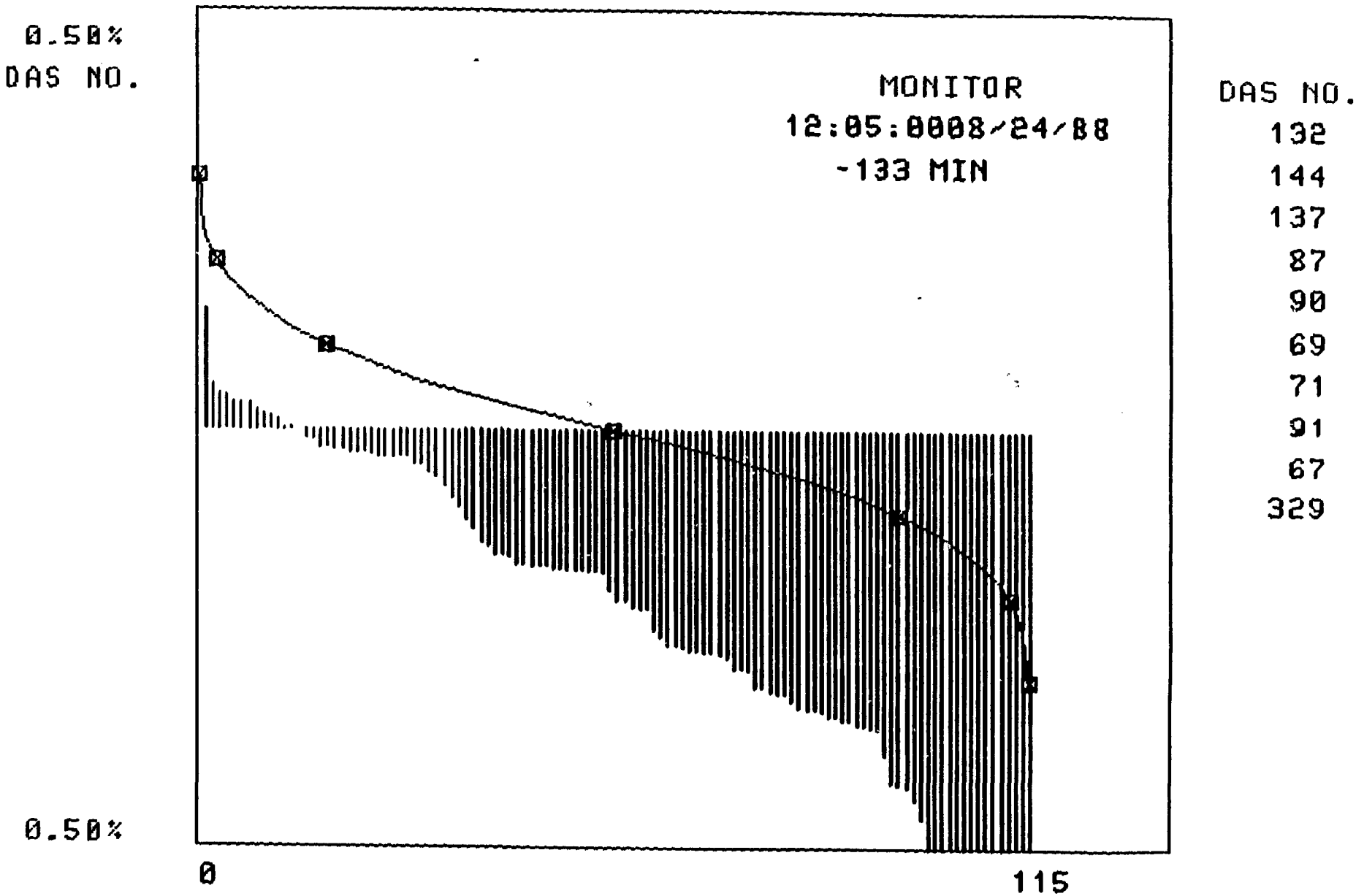


AVE DEV = 0.09 PER CENT

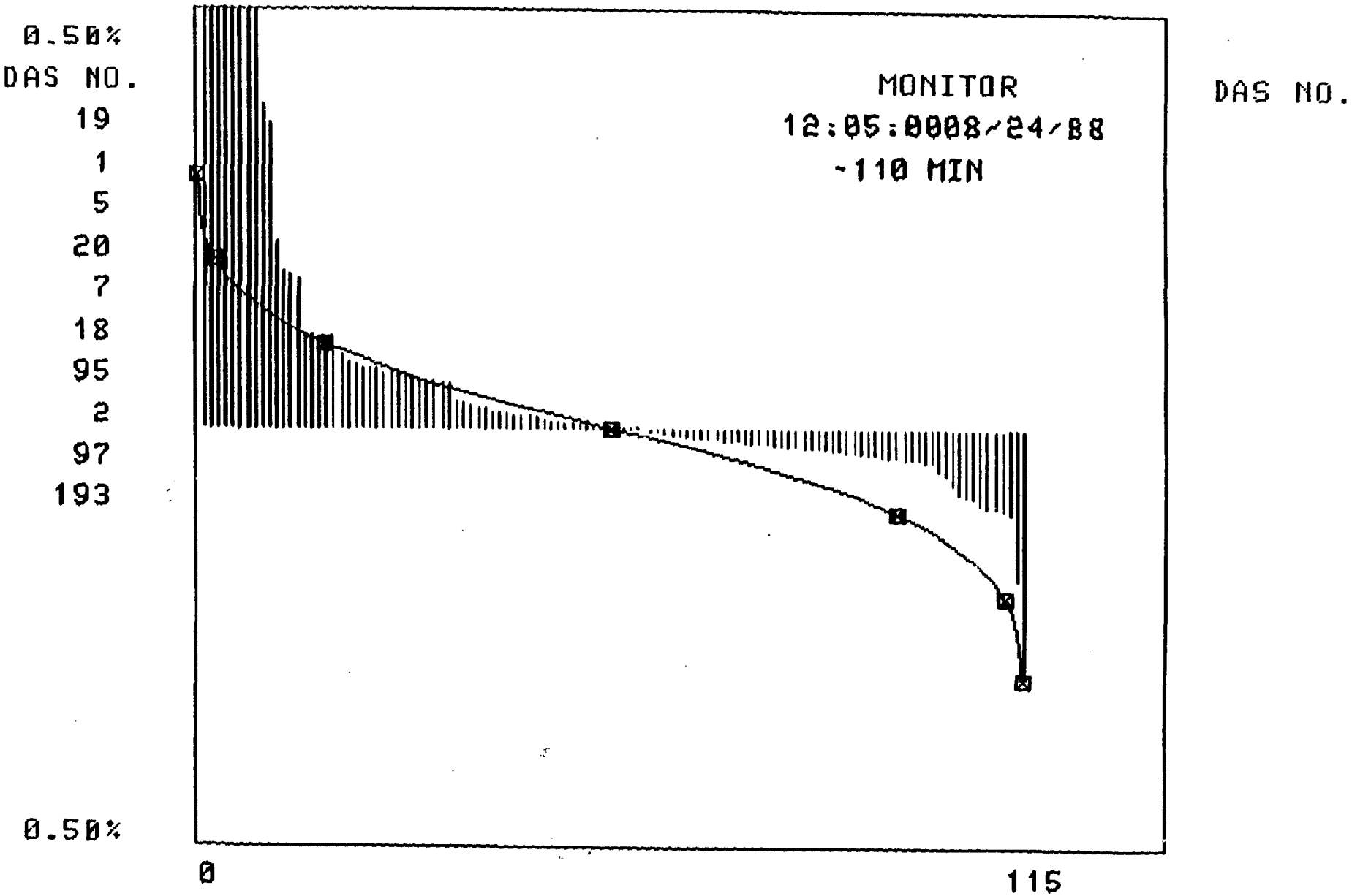


DAS NO.
19
20
5
1
95
18
7
2

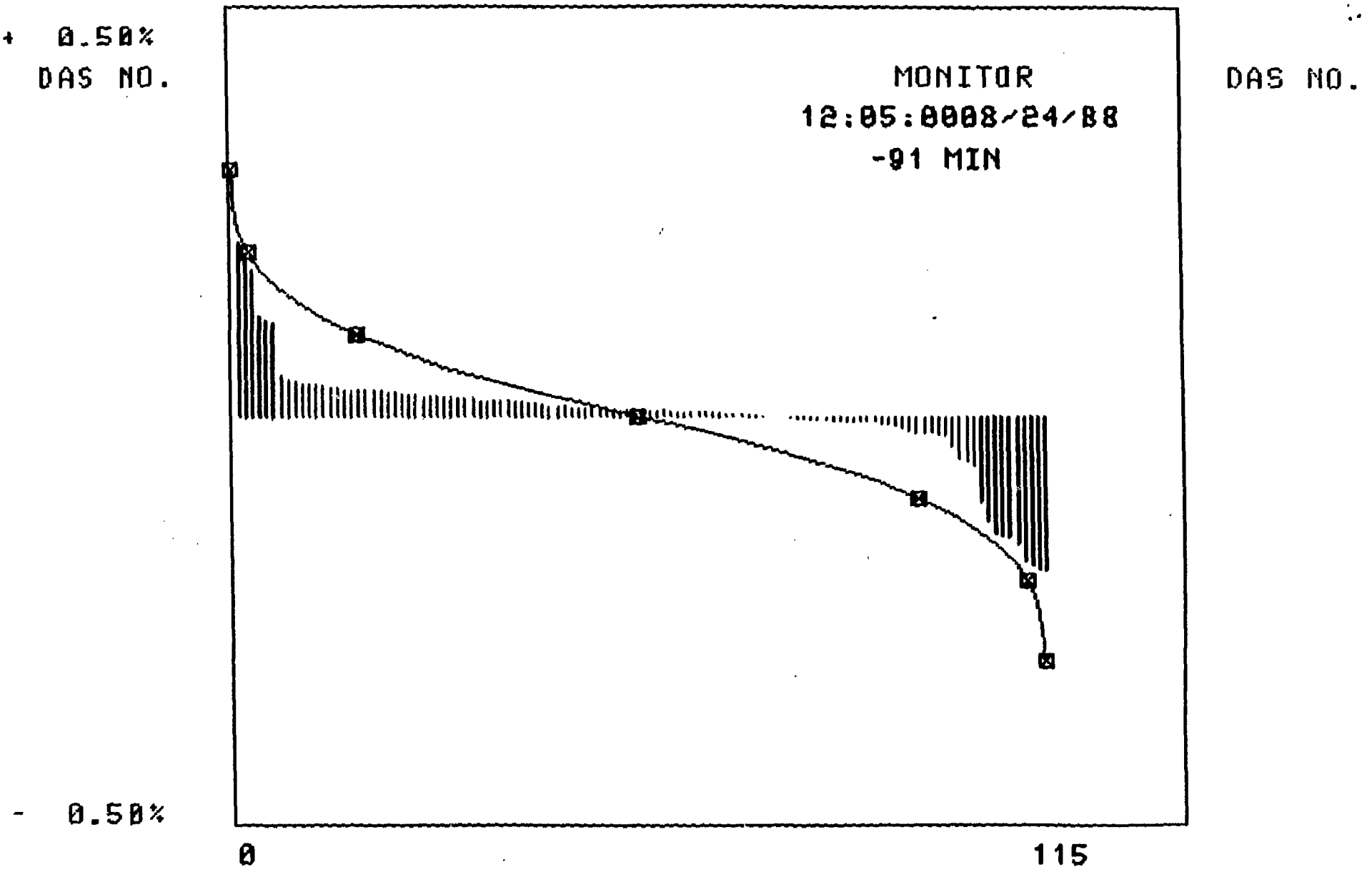
AVE DEV = 0.35 PER CENT



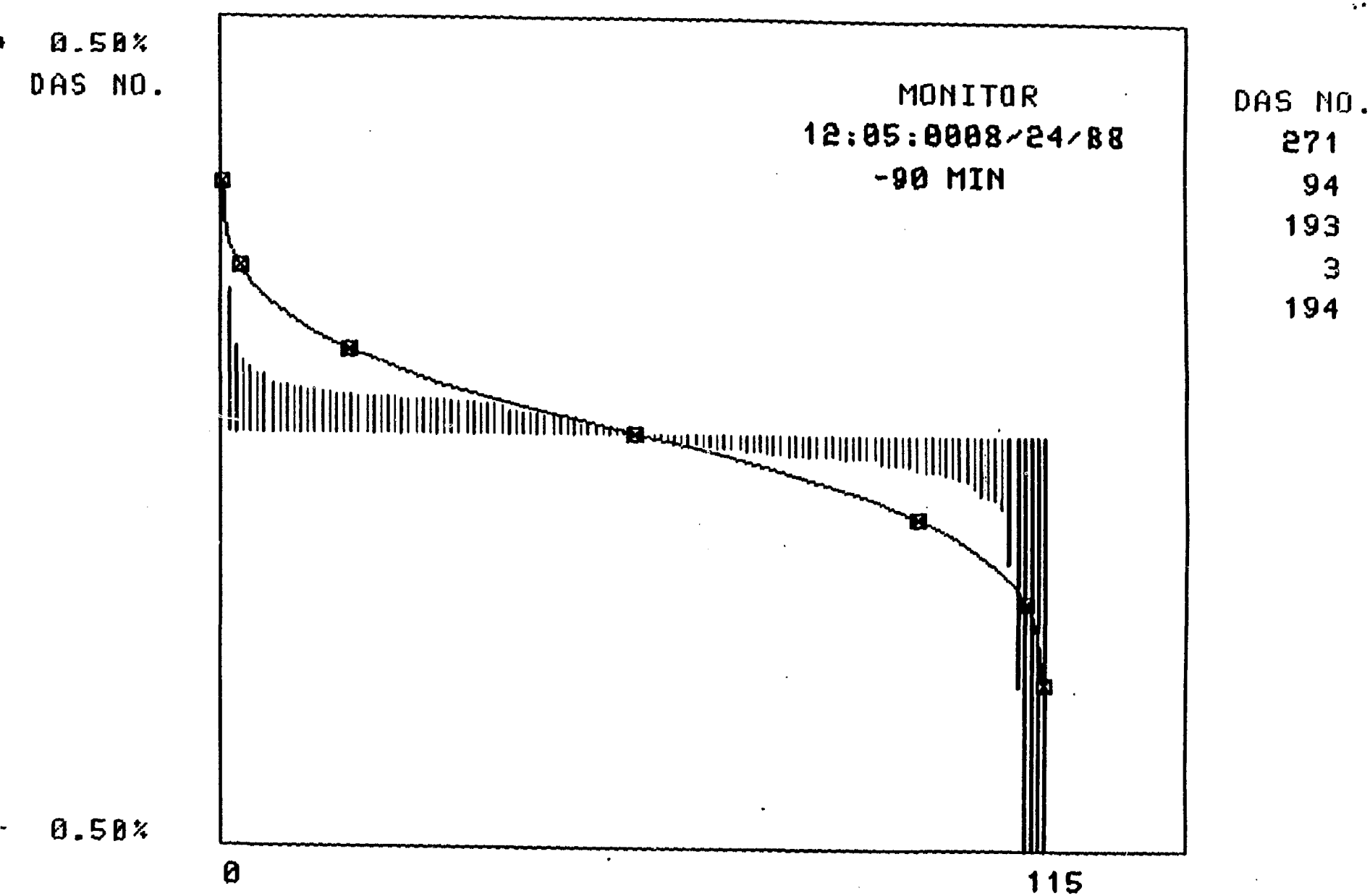
AVE DEV = 0.09 PER CENT



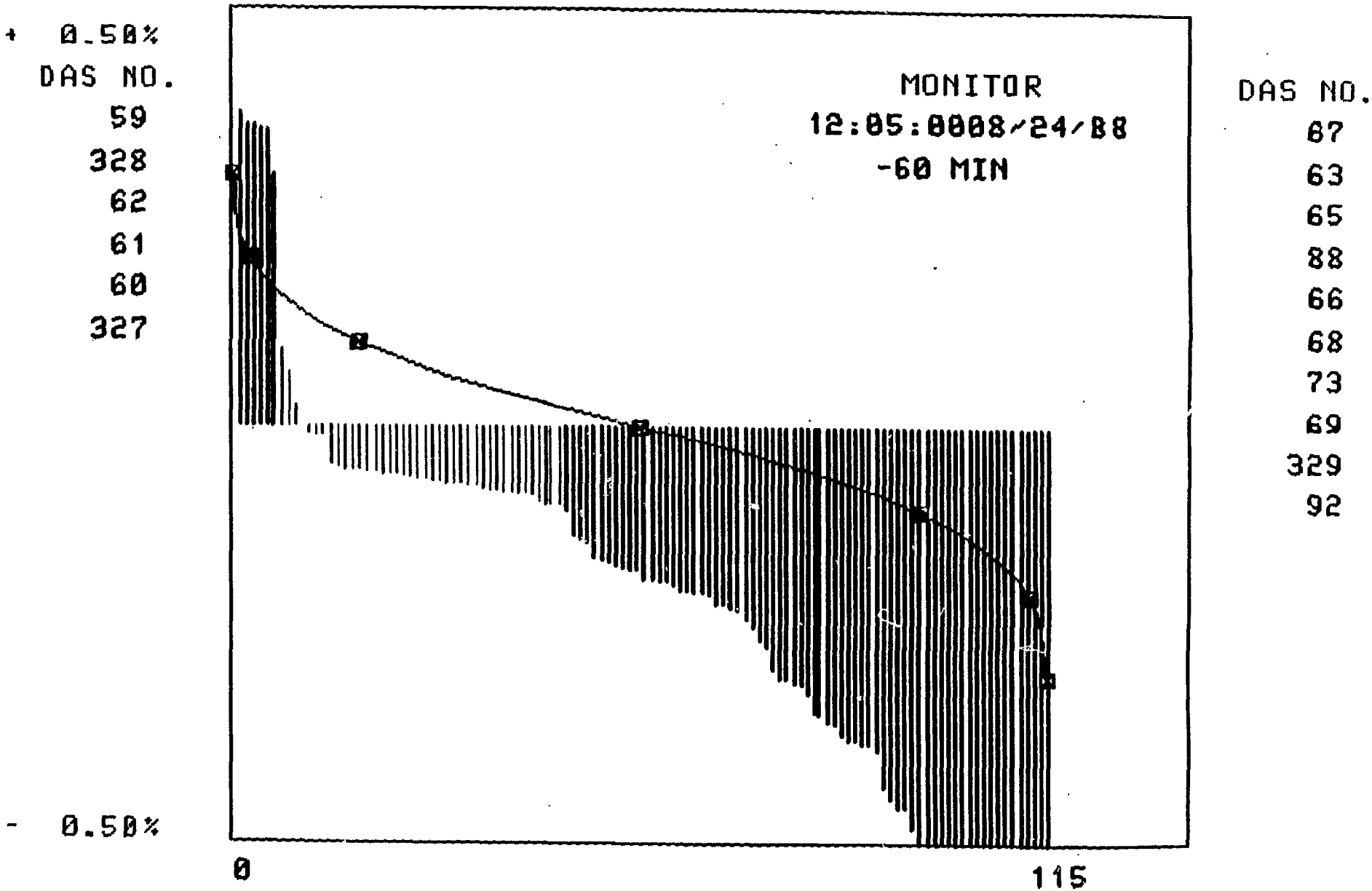
AVE DEV = 0.04 PER CENT



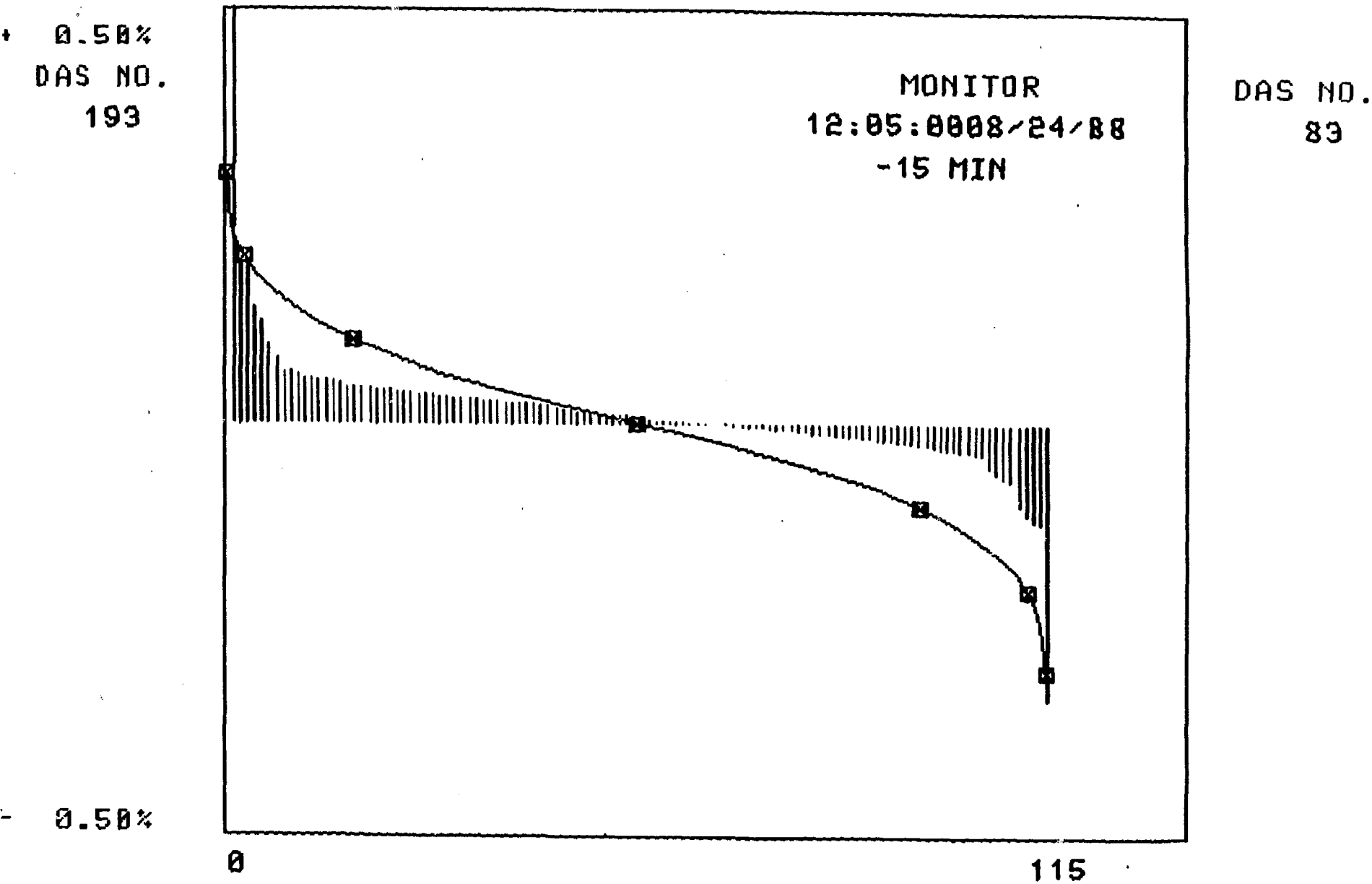
AVE DEV = 0.06 PER CENT

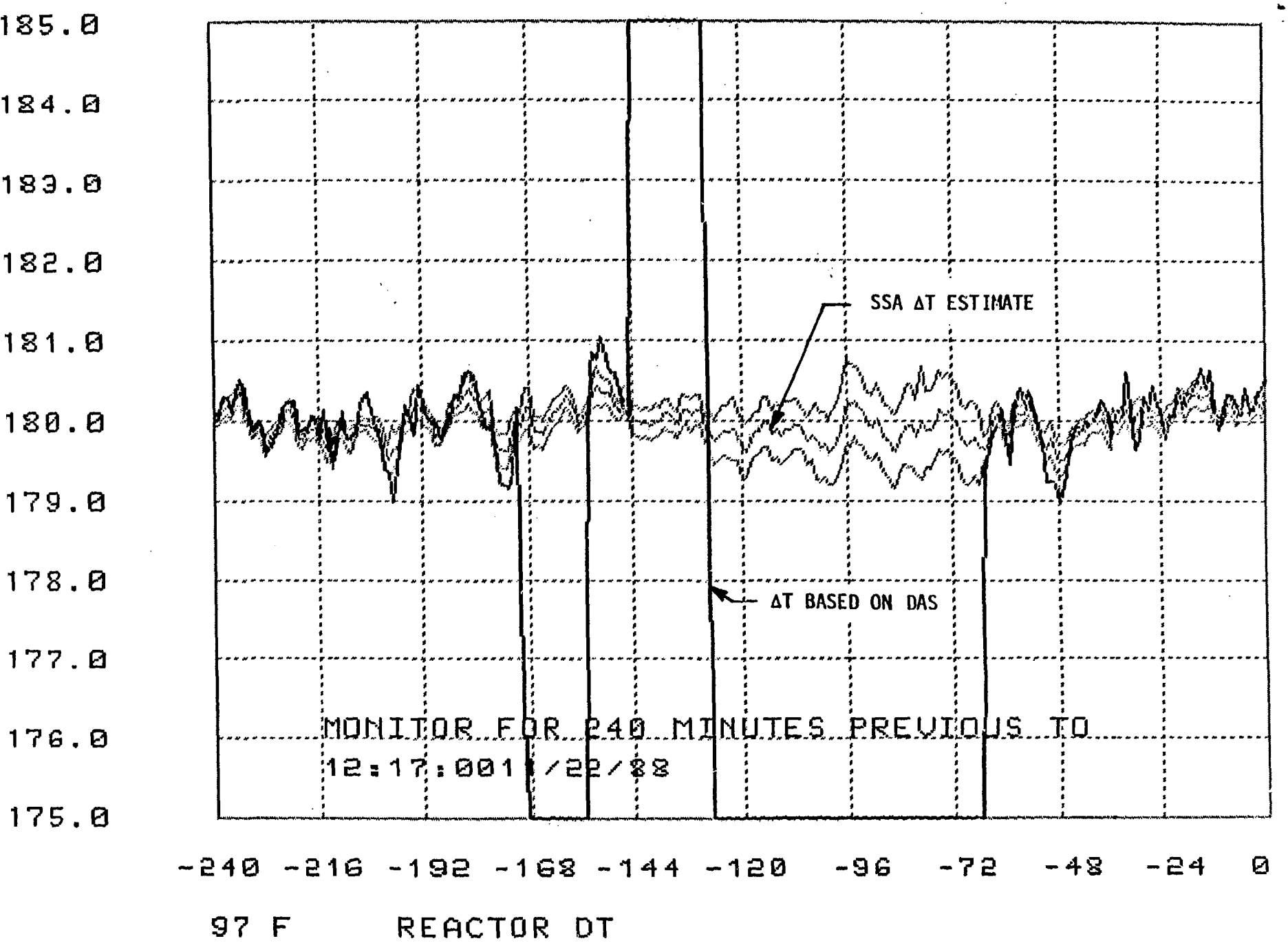


AVE DEV = 0.58 PER CENT



AVE DEV = 0.04 PER CENT




185.0
184.0
183.0
182.0
181.0
180.0
179.0
178.0
177.0
176.0
175.0
SSA ΔT ESTIMATE
ΔT BASED ON DAS
MONITOR FOR 240 MINUTES PREVIOUS TO
12:17:001 /22/88
-240 -216 -192 -168 -144 -120 -96 -72 -48 -24 0
97 F REACTOR DT