Project Title: *UFTR DIGITAL CONTROL SYSTEM UPGRADE*

UFTR-QA1-14, Safety System Design Basis

Prepared by,

Prof. Alireza Haghighat

.... (Signature)

Date: 7/7/10

Reviewed by,

Dr. Gabriel Ghita

.... (Signature)

Date: 7/7/10

Approved by,

Prof. Glenn Sjoden

.... (Signature)

Date: 7/6/2010

THE DISTRIBUTION LIST:

No.	Name	Affiliation	Signature	Date
1.				
2.				
3.				
4.				
5.				
6.				

THE LIST OF THE REVISED PAGES OF THE DOCUMENT

Revision no.	*Reviewed by*	*Approved by*	*The Modified Pages*	*Date*

TABLE OF CONTENTS

1. Purpose

The purpose of the Safety System Design Basis is to establish the proposed UFTR protection system design under regulatory bases and specify the general qualities that the resulting design will satisfy. The upgrade includes installation of the TELEPERM XS (TXS) system, which consists of both hardware and software that monitors and automatically initiate protective action for the UFTR. This design basis shall also introduce the need for diversity and defense-in-depth (D3) within the proposed protection system. This document adheres to requirements given in item 4 of IEEE Std. 603-1991, /10/.

2. References

2.1 UFTR Documents

/1/ UFTR-QA1-103, "Diversity and Defense-in-depth (D3) Analysis," 2009

/2/ UFTR Supplemental Safety Analysis Report (SSAR) 2009.

/3/ UFTR Technical Specifications (TS) 2006

2.2 Regulation and Guidance

/5/ ANSI/ANS 15.1, "Development of Technical Specifications for Research Reactors," 1982.

/6/ BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Controls Systems," March 2007

/7/ DI&C-ISG-02, "Task Working Group #2: Diversity and Defense-in-Depth Issues," September 26, 2007

/8/ DI&C-ISG-04, "Task Working Group Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc)," September 28, 2007

/9/ DI&C-ISG-05, "Task Working Group #5: Highly-Integrated Control Rooms—Human Factors Issues (HICR—HF)," September 28, 2007

/10/ IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," 1998

/11/ NUREG/CR 6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994

3. Definitions, Acronyms, and Abbreviations

3.1 Definitions

Defense-in-Depth: The practice of having multiple, redundant, and independent layers of safety systems to reduce the risk that a single failure of a component or system will cause the catastrophic failure of the reactor.

Design Basis Event: Postulate events used in the design to establish the acceptable performance requirements for the structures, systems, and components.

Diversity: In fault tolerance, realization of the same function by different means. For example, use of different signals, processors, storage media, programming languages, algorithms, or development teams.

Nuclear Instrumentation (NI): The portion of a train that directly senses and responds to changes in neutron and/or gamma ray levels in the reactor core and converts the measured interaction into an electric, optic, or pneumatic signal.

Operating Bypass: The inhibition of the capability to accomplish a safety function that could otherwise occur in response to a particular set of generating conditions.

Protective Action: The initiation of a signal within the sense and command features or the operation of equipment within the execute features for the purpose of accomplishing a safety function.

Redundant Equipment or System: A piece of equipment or a system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function, regardless of the state of operation or failure of the other.

Safety Function: One of the processes or conditions (for example, emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, post-accident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a design basis event.

Sensor: The portion of a train, other than nuclear instrumentation, that responds to changes in a plant variable or condition and converts the measured process variable into an electric, optic, or pneumatic signal.

Sensing Equipment: This expression includes both nuclear instrumentation (NI) and sensors.

Train: An arrangement of components and modules required to generate a single protective action signal when required by a generating station condition. A train loses its identity where single protective action signals are combined.

3.2 Acronyms

AQP	Acquisition and Processing
ARM	Ariel Radiation Monitor

BDT	Blade-Drop Trip
BF3	Boron Tri-fluoride detector
BTP	Branch Technical Position
D3	Diversity and Defense-in-Depth
DI&C	Digital Instrumentation and Control
FC	Fission Chamber
FM	Fan Monitor
FRM	Flow Rate Monitor
FT	Full Trip
GW	Gateway
GDC	General Design Criteria
HW	Hardware
IC	Ionization Chamber
IEEE	Institute of Electrical and Electronics Engineers
ISG	Interim Staff Guidance
LOCA	Loss of Coolant Accident
LEU	Low Enriched Uranium
LSSS	Limiting Safety System Setting
MCR	Main Control Room
MRS	Manual Reactor Scram
MSI	Monitoring Service Interface
NI	Nuclear Instrumentation
NRC	Nuclear Regulatory Commission
NUREG	Nuclear Regulatory Commission Regulation
QDS	Qualified Display System
RTD	Resistive Temperature Detector
RTS	Reactor Trip System
SAR	Safety Analysis Report
SU	Service Unit
SW	Software
TXS	TELEPERM XS
UFTR	University of Florida Training Reactor
WLM	Water Level Monitor

4. Safety System Design Basis

The UFTR protection system has been designed in accordance to ANSI/ANS 15.1, /5/. The following documents have been considered in preparation of licensing documentation:

- DI&C-ISG-02, /7/, DI&C-ISG-04, /8/, DI&C-ISG-05, /9/
- NUREG/CR 6303, /11/
- BTP 7-19, /6/

As discussed in the D3 document, /1/, the proposed protection system is comprised of three blocks. System blocks are shown in Figure 4-1 below, where arrows depict intended functional interface.

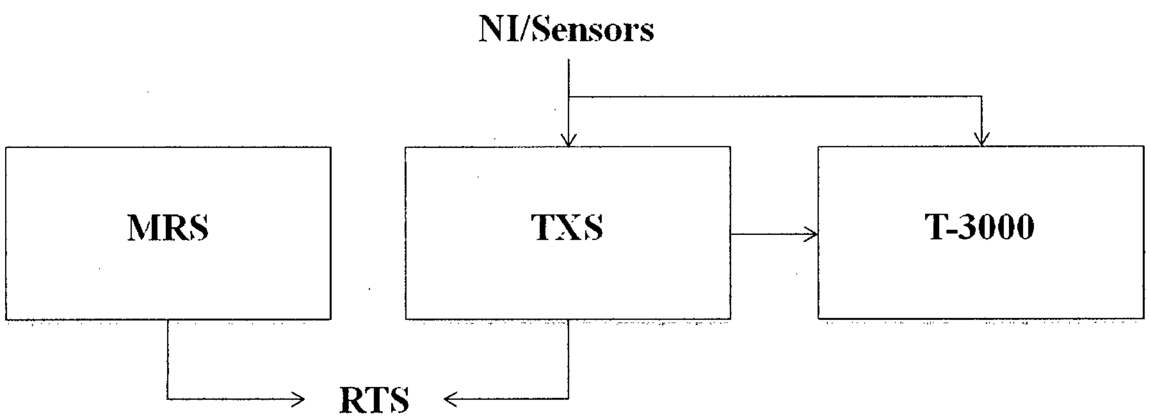

Figure 4-1: The Proposed UFTR Protection System

The above system includes the TXS as the primary protection system, providing Monitoring and Indicator System (MIS) and Reactor Trip System (RTS), the T-3000 system (with a diverse hardware and software) providing reactor control and a diverse MIS, and a hardwired Manual Reactor Scram (MRS) providing a diverse RTS as compared to TXS. Further, because of the unidirectional communication between the TXS and T-3000, and no communication between the TXS and MRS, the failure of the MRS or T3000 blocks will not impact the operation of the TXS. Analysis of diversity and defense-in-depth (D3) issues is given in UFTR-QA1-103, /1/. The following section is organized in accordance to Item 4 of IEEE Std. 603-1991, /10/.

4.1 Clause 4.1 of IEEE Std. 603-1991

The proposed protection system has two modes of operation; there are automatic and manual. The design basis events for the automatic mode, along with initial conditions and allowable limits of plant parameters for each event, are discussed in the following subsections:

4.1.1 Loss-of-Coolant Accident (LOCA)

This design basis event shall be analyzed during full-power operation. The loss-of-coolant accident (LOCA) shall cause reactor trip once the flow rate signal in the primary loop has become invalid. Lack of coolant within the core is allowed during this event due to the negative void and temperature coefficients for the UFTR core. Analysis of this feature is given in UF SSAR, /2/.

4.1.2 Slow Insertion of 0.06% Δk/k/second

The UFTR Technical Specifications (TS), /3/, require that the reactivity addition from control blade withdrawal must be less than 0.06% Δk/k/second when averaged over any 10 second interval. In this hypothetical accident, a reactivity insertion at this maximum rate initiates the transient and continues until the reactor is tripped at the overpower trip setting.

4.1.3 Sudden Insertion of the Maximum Allowed Excess Reactivity

The UFTR TS, /3/, allow a maximum excess reactivity of 1.4% Δk/k. This reactivity insertion may continue until the reactor is tripped at the overpower trip setting.

4.1.4 Control Blade System Malfunction

Control blade system malfunction is an anticipated operational occurrence that can be expected to occur during the lifetime of the UFTR. The only way in which the blades could fail to fall into the reactor during a reactor scram would be through either failure of the circuits to de-energize the electromagnetic coupling, or a mechanical failure of the blade drives or jamming in the shroud. This may occur at any time during reactor operation.

4.1.5 Loss of Power

Loss of power is an anticipated operational occurrence that may occur multiple times during the lifetime of the UFTR. Loss of the power source to UFTR during reactor operation will cause control blades to demagnetize and drop into the core due to gravity. This type of event is allowed during any plant conditions since it directly causes safe shutdown of the reactor.

4.2 Clause 4.2 of IEEE Std. 603-1991

Protective action for the UFTR is performed by the reactor trip system (RTS). Protective action is automatically initiated via the proposed TXS system. Manual reactor scram (MRS) is used to initiate protective action for the UFTR if the TXS fails. It is important to note that failure of protective action during a design basis event will not result in an uncontrolled release of radiation. The UFTR two trip types as follows:

- *Full trip (FT):* Nuclear instrumentation (NI) induced trips which involve the dumping of the primary water plus the drop of control blades; and
- *Blade-drop trip (BDT):* Sensor induced trips which involve the drop of the control blades without dumping the primary water.

The control blades are "fail-safe" in the sense that they will drop into the core by gravity in the event of a loss of power. In case of a manual scram or any scram signal from the instrumentation system, the electromagnets are de-energized and the blades drop into the core. Emergency core cooling capability is not required for the UFTR. Loss of coolant does not lead to an uncontrolled release of radiation, since the UFTR shuts itself down due to the loss of moderator. Explanation of this feature is described in UF SSAR, /2/. The corresponding protective actions of the execute features for each design basis event is given in the following subsections:

4.2.1 Loss-of-Coolant Accident (LOCA)

LOCA will cause the loss of the valid flow rate meter (FRM) signal in the primary coolant loop, which will cause automatic initiation of BDT via TXS. Loss of coolant in the core due to the LOCA will also contribute to the safe shutdown of the UFTR as a result of the negative void coefficient of reactivity.

4.2.2 Slow insertion of 0.06% Δk/k/second without scram

This design basis event shall cause automatic initiation of FT via the TXS when any NI signal becomes invalid due to high reactor power.

4.2.3 Sudden Insertion of the Maximum Allowed Excess Reactivity

This design basis event shall cause automatic initiation of FT via the TXS when any NI signal becomes invalid due to high reactor power.

4.2.4 Control Blade System Malfunction

This anticipated operational occurrence shall be mitigated by FT initiated by the MRS.

4.2.5 Loss of Power

Loss of Power directly causes BDT, thus no execute feature must be initiated during this event.

4.3 Clause 4.3 of IEEE Std. 603-1991

There is no need for an operating bypass for the UFTR, thus there are no permissive conditions for this type of bypass.

4.4 Clause 4.4 of IEEE Std. 603-1991

The existing analog protection system has four levels of protection for the design basis events. These four levels are pre-operation check, monitoring of ex-core parameters, interlocks, and trip system. For the new digital protection system, besides the aforementioned levels, we are considering diversity signals. Sub-sections below elaborate on all levels of protection for the proposed digital system.

4.4.1 Pre-operation checks

Prior to the reactor start-up, operator has to check several components as listed in Table 4-1.

Table 4-1: List of components checked prior to reactor startup

Item	Component	Item	Component
1	Core Vent	14	Primary Coolant Resistivity Determinations
2	Diluting Fan System	15	Blade Withdrawal Time Measurement
3	Blade Gear Box	16	Primary Coolant
4	Manometers and Magnehelic Gage	17	Magnet Power Key
5	Portal Monitor	18	Log/linear recorder
6	Core Vent and Diluting Fan Systems	19	Equipment Pit Checkout and Gamma Radiation Levels
7	Shield Water	20	Water Sample Analysis
8	Demineralized Pump	21	Air Particulate Detectors
9	Magnet Power Key	22	Radiation Monitor Console
10	Exterior lights	23	Secondary Water and Strainer
11	Neutron recorder	24	Security System Monitors
12	Primary Coolant Pump	25	Complete Records
13	Source Alarm		

4.4.2 Monitoring of ex-core parameters

During reactor operations, in addition to monitoring the reactor core, several external parameters are continuously monitored. These parameters are listed in Table 4-2.

Table 4-2: Monitoring ex-core parameters during operations

Item	Parameter
1	Main AC power line
2	Primary and secondary coolant pump power
3	Console power
4	Core ventilation fan power
5	Stack dilution fan
6	Area radiation monitor
7	Air particulate

4.4.3 Interlocks

UFTR includes a number of interlocks to prevent design basis events. Table 4-3 lists these interlocks.

Table 4-3: List of the UFTR Interlocks

ID	Description
1	Inhibits withdrawal of blades if the source count rate is < 2 cps (mode 1*)
2	Inhibits withdrawal of blades if period (T) <10 s (mode 1*)
3	Inhibits reactor operation if detection (or safety) channels 1 & 2 (NIs) are not operable (mode 1*)
4	Inhibits attempt of simultaneous withdrawal of 2 or more safety blades (mode 2**)
5	Inhibits attempt of withdrawal of regulating blade with a period (T) < 30 s (mode 2**)

*Mode 1: Manual Protection and Control
**Mode 2: Automatic control

4.4.4 Reactor Trip system (RTS)

To maintain LSSS and prevent design basis events, UFTR has a reactor trip system (RTS). Table 4-4 lists the conditions, which initiate the RTS.

Table 4-4: List of Trips, their types and specifications

Trips and their Specifications	Type of Trip
Automatic	
Period ≤ 3 sec	Full*
Power ≥ 119% of full power	Full*
Loss of NI high voltage (<90%) Loss of electrical power to control console	Full* Full*
Primary cooling system Loss of primary pump power Low water level in core (≤ 42.5") No outlet flow Low inlet water flow (≤ 41 gpm)	Blade-drop
Secondary cooling system (≥ 1 kW) Loss of flow (well water ≤ 60 gpm) Loss of secondary well pump power	Blade-drop
High primary coolant inlet temperature (≥ 99°F)	Blade-drop
High primary coolant outlet temperature (≥ 155°F)	Blade-drop
Shield tank low water level (6" below established normal level)	Blade-drop
Ventilation system Loss of power to stack dilution fan Loss of power to core vent fan	Blade-drop
Manual	
Manual scram bar	Full*
Console key-switch OFF	Full*

*Full: Blade-drop & water dump

4.4.5 Signal diversity considered for the digital system

The existing UFTR analog protection system includes one train, which is comprised of only two safety channels of NI's. Both safety channels have to be operational, because only one of the channels monitors the low power range, while both cover the high power range in a diverse manner.

The new UFTR digital protection system also has one safety train; however, this train not only includes two NI channels, but also contains other sensor channels. Further, it is important to note that the two NI channels monitor the whole power range in a diverse manner. Table 4-5 lists the signals monitored within the proposed safety train.

Table 4-5: List of devices sending signals to the TXS within the single train

Monitored Parameter	Monitoring Device	Monitored Region
Whole power range	Fission chamber (FC), Ion chamber (IC)	Core
Whole power range, Reactor period	Boron Tri-fluoride detector (BF3), IC	Core
Temperature	Resistive Temperature Detector (RTD)	Core, primary & secondary loops
Flow rate	Flow Rate Monitor (FRM)	Primary & secondary loops
Water level	Water Level Monitor (WLM)	Core, Storage tank, shield tank
Area radiation level	Area Radiation Monitor (ARM)	East, north, south & west
Fan air flow	Fan Monitor (FM)	Core ventilation: stack dilution

The diverse set of signals within the new safety train shall improve defense-in-depth within the TXS block by causing TXS to use diverse signals to monitor the same region of the UFTR. Table 4-6 summarizes how different segments of the reactor are monitored by a diverse set of sensors.

Table 4- 6: Proposed Diverse Monitoring of different regions of the UFTR

Sensor/Monitor	Core	Primary	Secondary	Reactor Cell	Confinement
FC+BF3	✓				
IC	✓				
RTD	✓	✓	✓		
FRM	✓	✓	✓		
WLM	✓	✓			
ARM				✓	✓
FM				✓	✓

The above table indicates that each segment of the reactor is monitored at least by two diverse sensors.

In Table 4-7, we list combination of different devices which monitor the same parameter in a diverse manner.

Table 4- 7: Each row contains the combination of NI/sensors that can be used to determine the parameter to the left, along with their respective location in UFTR. Only parameters that have multiple modes of detection are included in this table.

Parameter	*	Core	Primary	Secondary	Reactor Cell	Confinement
Reactor Power Level	P	IC				
	1	BF3+FC				
	2		RTD(2)+FRM			
	3		RTD(2)	RTD(2)+FRM		
	4		FRM	RTD(2)+FRM		
Reactor Period	P	BF3+FC				
	1	IC				
Core Temperature	P	RTD(6)				
	1		RTD(2)+FRM			
	2		FRM	RTD(2)+FRM		
	3		RTD(2)	RTD(2)+FRM		
	4	IC	RTD(2)			
	5	BF3+IC	RTD(2)			
Primary Temperature Change	P		RTD(2)			
	1	IC	FRM			
	2	BF3+FC	FRM			
	3		FRM	RTD(2)+FRM		
	4	IC		RTD(2)+FRM		
	5	BF3+FC		RTD(2)+FRM		
Secondary Temperature Change	P			RTD(2)		
	1		RTD(2)+FRM	FRM		
	2	IC	FRM	FRM		
	3	BF3+FC	FRM	FRM		
	4	IC	RTD(2)	FRM		
	5	BF3+FC	RTD(2)	FRM		
Primary Flow Rate	P		FRM			
	1	IC	RTD(2)			
	2	BF3+FC	RTD(2)			
	3		RTD(2)	FRM+RTD(2)		
	4	IC		RTD(2)+FRM		
	5	BF3+FC		RTD(2)+FRM		
Secondary Flow Rate	P			FRM		
	1		RTD(2)+FRM	RTD(2)		
	2	IC	RTD(2)+FRM	RTD(2)		
	3	BF3+FC	RTD(2)+FRM	RTD(2)		
	4	IC	FRM	RTD(2)		
	5	BF3+FC	FRM	RTD(2)		
Core Water Level	P	WLM				
	1		FRM			
	2	IC	RTD(2)			
	3	BF3+FC	RTD(2)			
	4		RTD(2)	FRM+RTD(2)		
	5	IC		RTD(2)+FRM		
	6	BF3+FC		RTD(2)+FRM		
Area Radiation Monitor	P				Any combinations of two ARMs at different locations	Core ventilation & Stack dilution
	1				Two other ARMs	

* P= Primary mode of detection, (1,2,3…)= groups of other NI/sensors used to determine the same parameter.

The analytical limit associated with each variable is given by specifications according to the UFTR TS, /2/.

The limiting safety system settings (LSSS) are given in Table 4-8.

Table 4-8: List of the UFTR Limiting System Safety Setting (LSSS) and their description

Item	LSSS Description
1	Power level shall be < 119 kW_{th}.
2	The primary coolant flow rate shall be > 41 gpm.
3	The primary coolant, a) Inlet temperature shall be < 99°F. b) Outlet temperature shall be < 155°F when measured at any fuel box outlet.
4	The reactor period shall be > 3 sec

The above LSSS are established from operating experience and safety considerations. They are established for the protection of the fuel, the fuel cladding, and the reactor core integrity. .

4.5 Clause 4.5 of IEEE Std. 603-1991

As discussed in the introduction of Section 4, the Manual reactor scram (MRS) is available in the event that the TXS fails to initiate the RTS. Depression of the MRS button causes the control blade drive (clutch current control) to shut off, which allows the blades to drop into the core due to gravity. The MRS button will also provide a HW and SW interrupt for the TXS system. This event is referred to as a blade-drop trip (BDT). If the control blades do not function properly and the core overheats, the negative void and temperature coefficients will cause the core to go subcritical and shut down even without insertion of the control blades. This is explained in UFTR SSAR, /2/. Therefore, instrumentation is not an absolute necessity for shutting the UFTR down because of its inherent safety features. A full trip (FT) may also be initiated by operator action by turning off the console magnet power switch. This will deactivate the control blade drive and dump the primary coolant. Following subsections will elaborate on how the MRS provides the necessary protective actions:

4.5.1 Clause 4.5.1 of IEEE Std. 603-1991

Protective action may be initiated by manual means at any time during reactor operation.

4.5.2 Clause 4.5.2 of IEEE Std. 603-1991

Justification for permitting initiation by manual means lies in the fact that no action or inaction of the operator during a design basis event can result in the uncontrolled release of radioactivity. This is described in more detail in UFTR SSAR, /2/.

4.5.3 Clause 4.5.3 of IEEE Std. 603-1991

Environmental conditions imposed upon the operator during normal, abnormal, and accident conditions shall not be of concern, since the worst-case accident scenario does not result in the release of radioactivity. It's also important to note that the main control room (MCR) is isolated from the reactor cell.

4.5.4 Clause 4.5.4 of IEEE Std. 603-1991

All variables listed in Table 4-1 shall be displayed for the operator via the T3000 control system when the operator manually initiates protective action.

4.6 Clause 4.6 of IEEE Std. 603-1991

The number and locations of sensors required for protective purposes is provided in Table 4-1. Loss of all valid signals from any one of the five segments of the UFTR listed in Table 4-3 shall result in the safe shutdown of the UFTR via BDT. Further detail of TXS software logic for reactor trip is provided in Appendix B of this document.

4.7 Clause 4.7 of IEEE Std. 603-1991

TXS system components are located in the MCR, which is isolated from the reactor cell. The MCR receives power and air-conditioning that is independent from the reactor cell. Prevention of electromagnetic interference is achieved by the shielding effect of metallic front plates in each TXS cabinet. Thus, conditions within the MCR are not subject to change due to UFTR transient or steady-state conditions.

4.8 Clause 4.8 of IEEE Std. 603-1991

Conditions having the potential for functional degradation of protection system performance are not of concern since the loss of the protection system does not result in the uncontrolled release of radiation. For further detail on this feature, refer to UFTR SSAR, /2/.

4.9 Clause 4.9 of IEEE Std. 603-1991

Reliability analysis is not required for safety assessments because of the inherent safety features of the UFTR found in UF SAR HEU-LEU Conversion, /4/.

4.10 Clause 4.10 of IEEE Std. 603-1991

The following four subsections list the critical plant conditions during a design basis event.

4.10.1 Clause 4.10.1 of IEEE Std. 603-1991

Tables 4-3 and 4-4 show the conditions for interlocks, and automatic and manual initiation of the reactor trips, respectively.

4.10.2 Clause 4.10.2 of IEEE Std. 603-1991

Protective action is complete when either BDT or FT has been initiated. It is important to note that physical failure of the RTS does not cause an uncontrolled release of radiation. Indication of initiation shall be provided in the main control room (MCR).

4.10.3 Clause 4.10.3 of IEEE Std. 603-1991

No automatic control past RTS initiation is required.

4.10.4 Clause 4.10.4 of IEEE Std. 603-1991

Plant conditions return to normal once enough valid signals are available to continue operation of the UFTR. Signals that their values are within the LSSS ranges are considered valid and are provided in Section 4.4 of this document.

4.11 Clause 4.11 of IEEE Std. 603-1991

No safety functions shall be disabled as a means for protective provisions.

4.12 Clause 4.12 of IEEE Std. 603-1991

Because the proposed system contains digital instrumentation and controls, D3 among system components is analyzed in UFTR-QA1-103, /1/.