Technical Specification - Cell Selection Integrity Verification (CSIV)

Version 1.0

Michael (Mike) Curnow
Defiant Networks, Inc.
June 21, 2022

Contents

Important Notice

Notice of Disclaimer & Limitation of Liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations. No recommendation as to products and services or vendors is made or should be implied. No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights. In no event shall authors of this document be held liable for loss of profits or any other incidental or consequential damages. Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and authors of this document shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

© 2022 Michael (Mike) Curnow, C6. Personal use of this material is permitted, along with republishing, reprinting this material for advertising or promotional purposes, creating new collective works, provided that this document and it's authors are cited in any redistributed pieces where this document or any portions of this document and any copyrighted and/or trademarked components are present.

1 Scope

This document specifies the Cell Selection Integrity Verification protocol, which is directed at bolstering the Cell Selection procedures defined in the Radio Resource Control (RRC)[1][3] protocol for 4G LTE and 5G NR.

The scope of this document also includes:

- The components of CSIV.
- The processes of each CSIV component.

2 References

[1] 3GPP TS 36.331 Release 15 - "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification"

[2] 3GPP TS 36.304 Release 16 - "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode"

[3] 3GPP TS 38.331 Release 17 - "5G; NR; Radio Resource Control (RRC); Protocol specification"

[4] 3GPP TS 38.304 Release 17 - "5G; NR; User Equipment (UE) procedures in idle mode and in RRC Inactive state"

3 Terminology

3.1 Cell Selection Concepts and Terminology

To understand the subject matter of the cell selection process, it is recommended that readers of this technical specification read at a minimum the following, as terminology and methodologies stated herein are drawn from these documents:

1. 3GPP TS 36.331 Release 15 - "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification"
2. 3GPP TS 36.304 Release 16 - "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode"
3. 3GPP TS 38.331 Release 17 - "5G; NR; Radio Resource Control (RRC); Protocol specification"
4. 3GPP TS 38.304 Release 17 - "5G; NR; User Equipment (UE) procedures in idle mode and in RRC Inactive state"

3.2 CSIV Terminology

This section includes terminology contextually relevant specifically to the this document. CSIV terminology is as follows:

- **CSIV** - Cell Selection Integrity Verification
- **LTE** - Long-Term Evolution, referring to the 4th generation of mobile network communications
- **NR** - New Radio, referring to the 5th generation of mobile network communications
- **OCS** - Onboard Cell-Selection Storage
- **PLMN** - Public Land Mobile Network
- **UE** - User Equipment, equipment utilizing cellular network to communicate (i.e. cellular telephone, cellular modem, IoT devices, etc)
- **VA** - Verification Algorithm
- **VC** - Verification Condition

4 Introduction

This document introduces Cell Selection Integrity Verification (CSIV) , a process for drastically increasing the integrity of mobile connectivity and increases the fidelity between User Equipment (UE) (also known as a “Mobile Station” or MS for short) and the Cellular Base Station (BS/BTS), to include the Cell in which service is provided. This process capitalizes on information a BS sends to UE in Master Information Blocks (MIBs) and System Information Blocks (SIBs) to correspond with the mathematically provable underpinnings of BS and Cell parameters signaled to UEs in their vicinity of coverage.

4.1 Current Cell Selection

Cell Selection & Re-selection procedures follow the order of:

- **PLMN Selection** - Ensuring the PLMN of detected cell corresponds with the UE’s subscription information. (i.e. my device uses Verizon network, so the cell’s PLMN information must display identifying information for Verizon service). Defined in 3GPP TS 36.304 & 38.304 section 5.1.
- **Cell Selection** - Ensuring the cell meets minimum service reception power and service quality measurements defined in 3GPP TS 36.304 & 38.304 section 5.2.3.2.

Figure 5.2.2-1 [2][4] graphically illustrates this procedure.

4.2 Rationale and Intent

CSIV is expected to be enacted on the firmware of baseband processor chipsets, and integrated into the “Cell Selection” and "Cell Re-Selection" processes of manufacturers’ implementation of LTE E-UTRA UE Procedures in Idle Mode[2] and 5G NR UE Procedures in Idle Mode and in RRC Inactive State[4], i.e. building onto the Radio Resource Control (RRC) protocol used in 4G LTE and 5G NR.

During the initial conception of this criterion, research discovered that certain 4G LTE capable networking devices had an ability referred to as “Cell Lock” where the UE/MS can make use of a specific cell (based on PCI) to facilitate connectivity. This discovery validated the feasibility of implementing additional functionality to the base RRC standard implementation in the firmware of baseband processors in networking devices, thus implying possibilities to implement further hardening functionality to UE behavior at Layer 3 of the 4G LTE and 5G NR protocol stacks.

The current method of cell selection criteria has existed since the release of 3G Universal Mobile Telecommunications Service (UMTS) in 1999. Over the time spanning the origination of the currently used cell selection process which originated in 3G UMTS release and the release of this document, ways to leverage susceptible features in the RRC protocol have been devised and deployed already. Hence the need to harden the current cell selection mechanisms to include an account for cells which are detrimental to overall cell connectivity and communications.

4.3 Expected Use of CSIV

CSIV utilizes a set of VCs, which will supplement the standard cell selection mechanisms of the Radio Resource Control protocol as implemented in the firmware of UE/MS baseband processors. i.e. Expected use is for CSIV and it's generated VC to exist in the firmware code which dictates initial and stored-info cell selection re-selection for RRC implementation of UE/MS.

4.4 Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119], which is defined below:

• **MUST** - This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

• **MUST NOT** - This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

• **SHOULD** - This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

• **SHOULD NOT** - This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

• **MAY** - This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate

with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

5 Components

Various components are required for this mechanism to operate. The overall components for CSIV include:

- **Onboard Cell-Selection Storage (OCS)** - An area of storage on the UE which stores data collected from a cell that has passed Public Land Mobile Network (PLMN) and Cell Selection Criteria. This storage includes data from the Synchronization Signal Block (SSB) and Cell information gathered from System Information Blocks (SIB) types 1-5 for 4G LTE and types 1-4 for 5G NR, and static data such as that enumerated in 3GPP standards (scheduling info, timing info, etc)
- **Verification Conditions (VC)** - Are computational checks which make use of information in OCS that serve to provide boolean value output indicating a Cell's ability to pass certain conditions pertaining to scheduling, location, identity, timing, neighbor, and signal power. These conditions include static checks to ensure parameter values adhere to 3GPP enumerated set of values, and dynamic checks to contrast a Cell's parameters to that of other suitable candidate cells (i.e. those that already passed previous selection criteria) to discern deviations indicative of malicious Cell configuration pathologies.
- **Verification Process** - The formula which determines whether a Cell should be added to the UE's barred cell list based on outcomes of various VC's. It performs computations of static and dynamic VC's to determine cell legitimacy after previous selection processes have succeeded (i.e. PLMN Selection, Cell Selection, Service Selection).

5.1 Onboard Cell-Selection Storage (OCS)

OCS storage is categorized into 3 types: Dynamic Cell List; Static Cell Lists; Dynamic Sets Lists. All of which are stored in UE's baseband processor for further computation.

5.1.1 Dynamic Cell List

A list of cell entries, where each entry contains information elements of a particular cell, which is utilized for further computation.

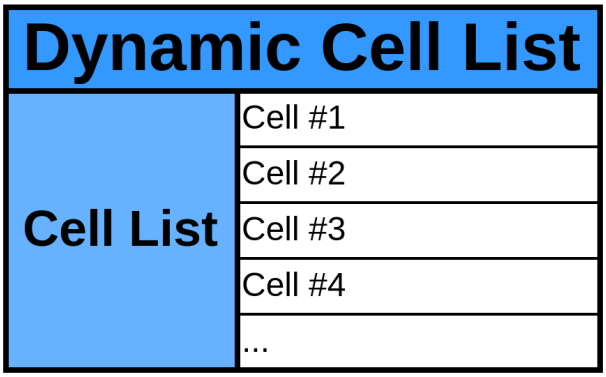


Figure 5.1.1-a. Dynamic Cell List

Dynamic Cell List Entry				
Cell List Entry	Cell #		1	
	Identity	Cell Identifier	199462415	
		Physical Cell Identity	404	
		Tracking Area Code	9801	
	Scheduling	si-WindowLength	ms40	
		SIB List	SIB-Type	sibType3
			Periodicity	rf8
			SIB-Type	sibType3
			Periodicity	rf16
			SIB-Type	sibType5
			Periodicity	rf32
	Scheduling	connEstFailCount	n4	
		T300	ms2000	
	Priority	cellReselectionPriority	6	
	Neighborhood	Intrafrequency	Cell #	1
			PCI	54
			Cell #	2
			Cell #1	117
		Interfrequency	Cell #	1
			PCI	69
			Cell #	2
			PCI	420

Figure 5.1.1-b. Dynamic Cell List Entry

- **Cell Number/#** - Numeric identifier of a Dynamic Cell List Entry.
- **Identity** - Contains identity information for cell list entry.
  - Cell Identifier - Used to identify a cell uniquely within a Public Land Mobile Network (PLMN). In 4G LTE this is referred to as the E-UTRAN Cell Identifier (ECI), has a length of 28 bits and contains the eNodeB-Identifier (eNB-ID). In 5G NR this is referred to as the NR Cell Identity (NCI), has a length of 36 bits and contains the gNodeB-Identifier (gNB-ID).
    Example:
    cellIdentity 0000000000000000000100000000
  - Physical Cell Identity (PCI) - The Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS) from the cell's Synchronization Signal Block (SSB), of which the UE is able to calculate the Physical Cell Identity (PCI). Formula: *PCI* = 3(*PSS*) + *SSS*
  - Tracking Area Code (TAC) - The BTS broadcasts its (TAC), which is a bit string (16 bits in 4G and 24 bits in 5G) used to indicate which Tracking Area the BTS belongs to, and the TAC is unique within a PLMN.
    Example:
    trackingAreaCode 0000000000000001
- **Scheduling** - Contains information relevant to scheduling of SIB messages from a cell to receiving UE within vicinity of cell's coverage.
  - si-WindowLength - The length of the SI scheduling window. In 4G this unit is in milliseconds, where ms1 denotes 1 millisecond, ms2 denotes 2 milliseconds and so on. In 5G this unit is measured in slots, where the value s5 corresponds to 5 slots, value s10 corresponds to 10 slots and so on. The network always configures si-WindowLength to be shorter than or equal to the si-Periodicity.
    Examples:
    4G LTE
    ```
    si-WindowLength                 ENUMERATED {
                                        ms1, ms2, ms5, ms10, ms15, ms20,
                                        ms40},
    ```
    5G NR
    ```
    si-WindowLength                 ENUMERATED {s5, s10, s20, s40, s80, s160, s320, s640, s1280},
    ```
  - SIB List - Contains the SIB-Type and si-Periodicity for each SIB the cell is broadcasting to UE's withing vicinity of coverage.

    * SIB-Type - This value represents the mapping to a SIB type which information such as *si-periodicity* would apply to.
      Example:

```
SIB-Type ::=                    ENUMERATED {
                                    sibType3, sibType4, sibType5, sibType6,
                                    sibType7, sibType8, sibType9, sibType10,
                                    sibType11, sibType12-v920, sibType13-v920,
                                    sibType14-v1130, sibType15-v1130,
                                    sibType16-v1130, sibType17-v1250, sibType18-v1250,
                                    ..., sibType19-v1250, sibType20-v1310, sibType21-v1430,
                                    sibType24-v1530, sibType25-v1530, sibType26-v1530}
```

    * si-Periodicity - Periodicity of the System Information (SI) message in radio frames, such that rf8 denotes 8 radio frames, rf16 denotes 16 radio frames, and so on.
      Example:

```
si-Periodicity                  ENUMERATED {rf8, rf16, rf32, rf64, rf128, rf256, rf512},
```

- **Timing** - Contains information relevant to timing operations of the cell and connection timeout configurations.
  - connEstFailCount - This is used to configure parameters for connection establishment failure control.
    Example:

```
connEstFailCount                        ENUMERATED {n1, n2, n3, n4},
```

  - T300 - A timing value from IE "UE-TimersAndConstants" used to establish limit for connection timeouts.
    Example:

```
UE-TimersAndConstants ::=       SEQUENCE {
    t300                            ENUMERATED {
                                        ms100, ms200, ms300, ms400, ms600, ms1000, ms1500,
                                        ms2000},
```

- **Priority** - Denotes the degree of priority of other UE to camp on the cell.
  - connectionReselectionPriority - The absolute priority of the concerned carrier frequency, as used by the cell reselection procedure. Represented as integers between 0 (lowest) and 7 (highest).
    Example:

- **Neighborhood** - Contains information of a cell's intrafrequency and interfrequency cell neighbors.
  - Intrafrequency Neighbor PCI List - The intra-frequency neighbor list contains PCIs of all intra-frequency cells that are registered neighbors with the current cell who's integrity we're verifying.
    * Cell Number/# - Numeric identifier of an Intrafrequency Neighbor Cell List Entry.

    * Physical Cell Identity (PCI) - The Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS) from the cell's Synchronization Signal Block (SSB), of which the UE is able to calculate the Physical Cell Identity (PCI). Formula: $PCI = 3(PSS) + SSS$

- Interfrequency Neighbor PCI List - The inter-frequency neighbor list contains PCIs of all inter-frequency cells that are registered neighbors with the current cell who's integrity we're verifying.
    * Cell Number/# - Numeric identifier of an Interfrequency Neighbor Cell List Entry.
    * Physical Cell Identity (PCI) - The Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS) from the cell's Synchronization Signal Block (SSB), of which the UE is able to calculate the Physical Cell Identity (PCI). Formula: $PCI = 3(PSS) + SSS$

5.1.2 Static Cells Lists

Multiple sets of static values corresponding to store enumerated values from the 3GPP standards.

Static Cell Lists	
si-Periodicity	8
	16
	32
	64
	128
	256
	512
si-WindowLength	ms1
	ms2
	ms5
	ms10
	ms15
	ms20
	ms40
connEstFailCount	n1
	n2
	n3
	n4
UE-TimersAndContants -> T300	ms100
	ms200
	ms300
	ms400
	ms600
	ms1000
	ms1500
	ms2000

Figure 5.1.2-a. Static Cell Lists

- **si-Periodicity List** - Valid enumerated values from the 3GPP 4G LTE & 5G NR Standards.
- **si-WindowLength List** - Valid enumerated values from the 3GPP 4G LTE & 5G NR Standards.
- **connEstFailCount List** - Valid enumerated values from the 3GPP 4G LTE & 5G NR Standards.
- **UE-TimersAndConstants/T300** - Valid enumerated values from the 3GPP 4G LTE & 5G NR Standards.

5.1.3 Dynamic Set Lists

Dynamic Set Lists reflect the current neighboring cells, priority parameters, and cell signal power for each cell that is currently a suitable candidate. Data within these lists are obtained through entries in the *Dynamic Cell List*, and will change according to the information and amount of Cells stored as entries. As suitable candidate cells are no longer feasible, the entry is removed from the *Dynamic Cell List Entries* and subsequently relevant information is removed from the varying Dynamic Set Lists correspondent to their respective PCIs, with the exception of the *Priority List*, as it's merely a collection of the various *cellReselectionPriority* values present throughout all *Dynamic Cell List* entries.

Dynamic Set Lists			
Neighbor Cell List	Intrafrequency Neighbor Cell PCI List	Cell #	1
		PCI	69
		Cell #	2
		Cell #1	420
		Cell #	3
		PCI	117
		Cell #	4
		PCI	86
	Interfrequency Neighbor Cell PCI List	Cell #	5
		PCI	12
		Cell #	6
		PCI	50
		Cell #	7
		Cell #1	47
		Cell #	8
		PCI	23
CID List		75155471	
		74641935	
		49001966	
		196837391	
		197107726	
TAC List		9984	
		9984	
		9983	
		9983	
		9991	
Priority List		0	
		5	
		4	
		3	
		6	
		7	
Cell Power List		Cell #	1
		PCI	10
		Srxlev	2
		Cell #	2
		PCI	22
		Srxlev	10
		Cell #	3
		PCI	26
		Srxlev	25
		Cell #	4
		PCI	118
		Srxlev	16

Figure 5.1.3-a. Dynamic Set Lists

- **Neighbor Cell List** - Contains the PCIs current intrafrequency and interfrequency neighbor cells.
  - Intrafrequency Neighbor Cell PCI List - Intrafrequency Neighbor Cell PCI's.
    * Cell Number/# - Numeric identifier of list entry.
    * Physical Cell Identity (PCI) - PCI For cell entry.
  - Interfrequency Neighbor Cell PCI List - Interfrequency Neighbor Cell PCI's.
    * Cell Number# - Numeric identifier of list entry.
    * Physical Cell Identity (PCI) - PCI For cell entry.
- **CID List** - A list of Cell Identifiers (ECI/NCI) for all current suitable candidate cells.
- **TAC List** - A list of Tracking Area Codes for all current suitable candidate cells.
- **Priority List** - A list of current *Dynamic Cell List Entries*' *cellReselectionPriority* values.
- **Cell Power List** - List of current and active suitable candidate cells and their post cell-selection S_{rxlev} measurements.
- UE Power - This list stores the configuration setting of the UE's P_{CMAX}. As of this version of this document, the only value to populate this list is the UE's P_{CMAX}.
  - P_{CMAX} - The configured maximum UE output power. Unit measured in dBm.

5.2 Verification Conditions (VC)

These represent various conditions of computations in regards to the state of a cell as it is proceeding through the selection processes.

5.2.1 Scheduling Verification

Ensuring that SIB scheduling IEs correspond with known enumerated values.

5.2.2 Timing Verification

Ensuring timing values correspond with known enumerated values.

5.2.3 Duplication Verification

Ensures a duplicate of cell doesn't exist.

5.2.4 Location Verification

Ensures the TAC of current cell matches already known TACs present in the *Dynamic Set Lists*' TAC List.

5.2.5 Priority Verification

Determines if the cell's reselection priority is high compared to those in the *Dynamic Set Lists*' Priority List.

5.2.6 Neighborhood Verification

Ensuring the cell's neighboring cells correspond with neighbor cells from current suitable candidate cells.

5.2.7 Signal Power Verification

Ensure a cell's signal power isn't abnormally high when compared to those of other suitable candidate cell's.

5.3 Verification Algorithm (VA)

This computation utilizes the 7 *Verification Conditions* to make a determination on whether a cell should be added to the UE's *barred_cell* list.

6 Processes

6.1 Onboard Cell-Selection Storage (OCS)

As a new cell undergoes selection procedures on the UE, data from the cell is stored in an ephemeral portion in the OCS block. If the cell passes cell selection muster, then this ephemeral data persists as an entry to the *Dynamic Cell List*. If the cell fails selection, then the temporary data is dropped. This process is repeated for each newly detected cell undergoing selection.

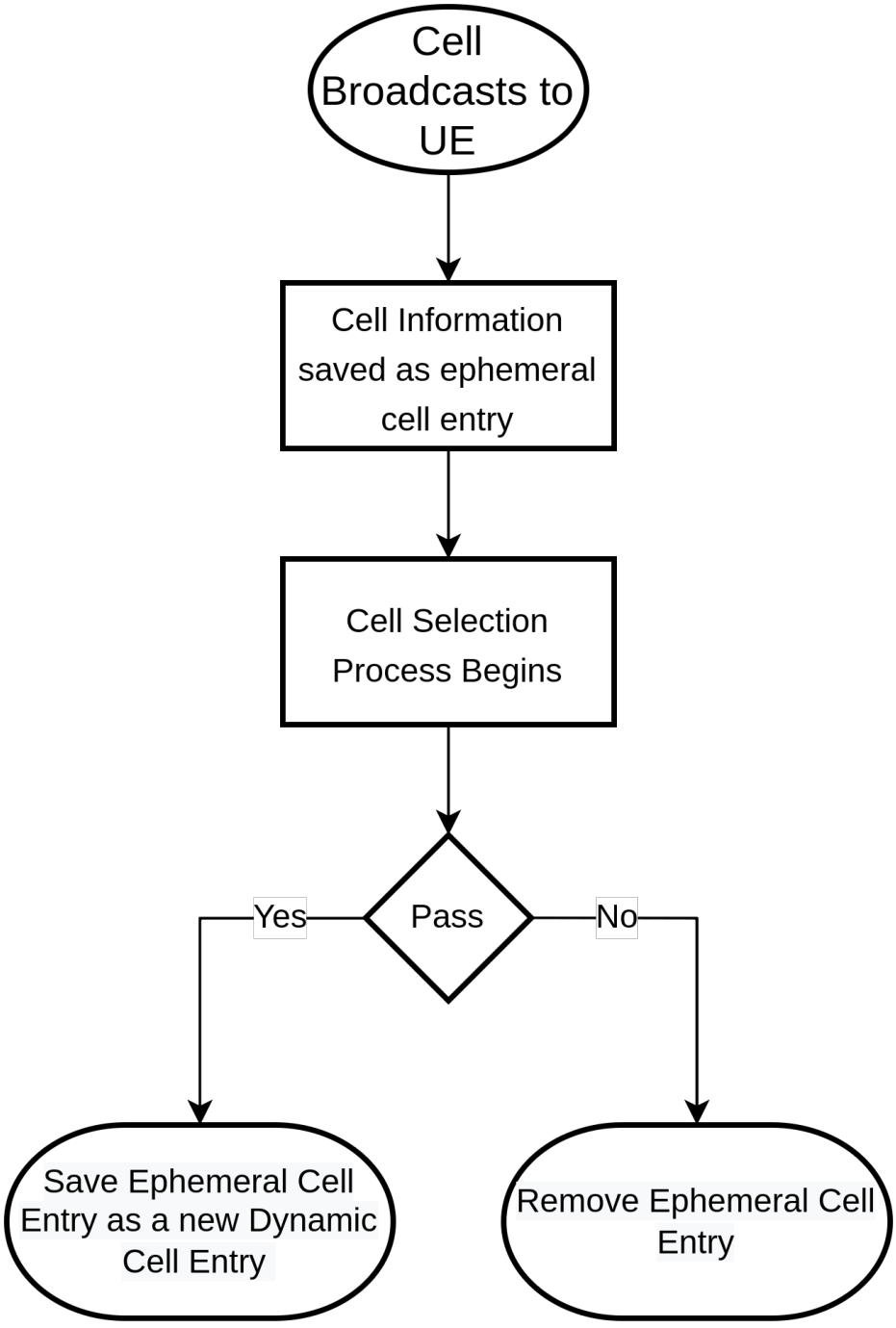


Figure 6.1-a. OCS Flow

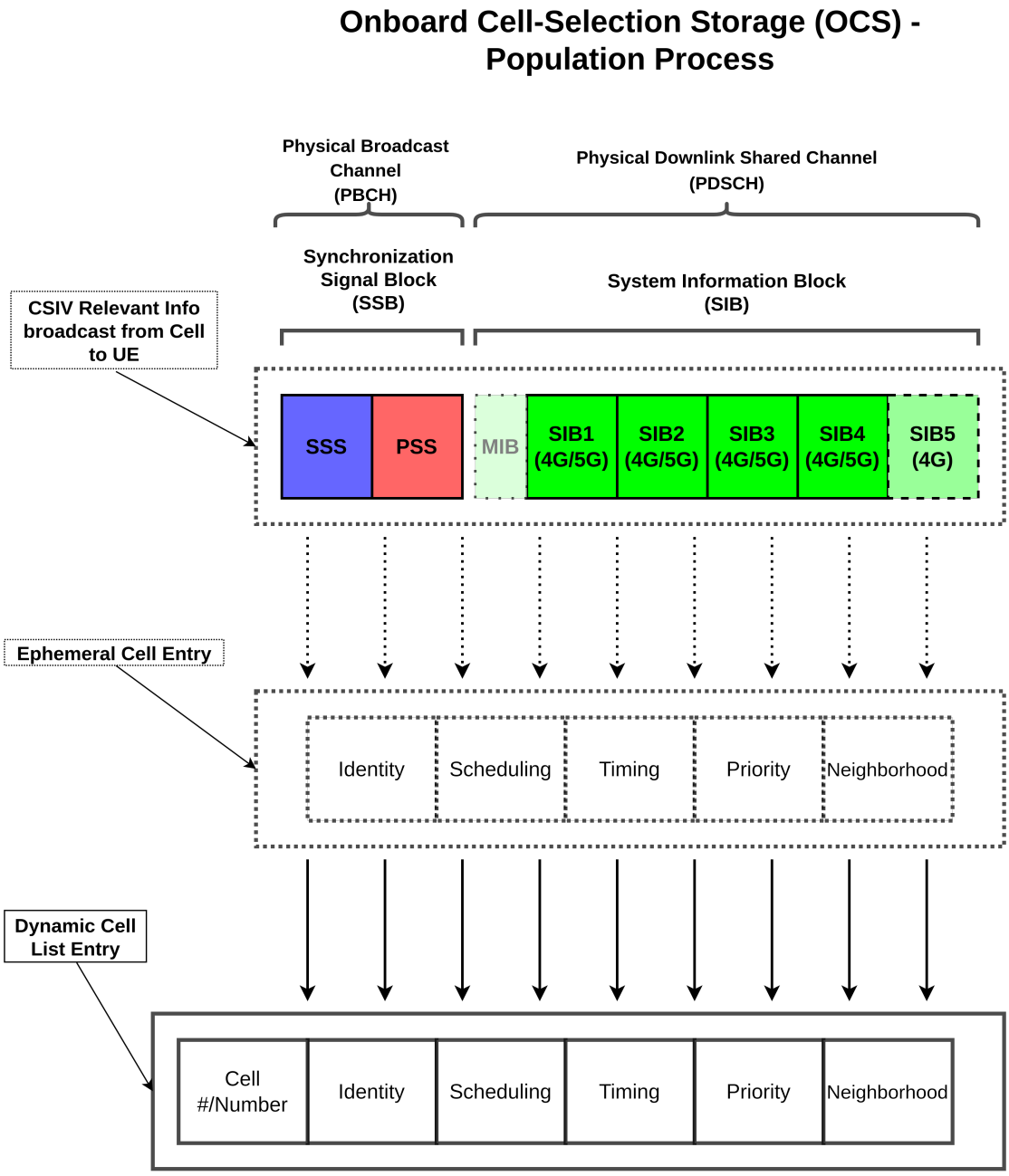


Figure 6.1-b. OCS Process (Cell Selection Succeeds)

6.2 Verification Conditions

6.2.1 Scheduling Verification (sVer)

Ensuring that SIB scheduling IEs correspond with known values.

Variables

Variable	Description	OBS Mapping
sip {...}	List of current *si-Periodicity* values in the cell entry's *SIB List*.	*Dynamic Cell List Entry->Scheduling->SIB List->si-Periodicity*
siw	The *si-WindowLength* of the cell's scheduling information.	*Dynamic Cell List Entry->Scheduling->si-WindowLength*
pe {...}	Enumerated proper values of *si-Periodicity*.	*Static Cell Lists->si-Periodicity*
we {...}	Enumerate proper values of *si-WindowLength*	*Static Cell Lists->si-WindowLength*

Verification Cases

- **sVc1** - Each entry's *si-Periodicity* in *SIB List* of the *Dynamic Cell List* is less than *si-WindowLength*.
  Operation:
  - If each **sip** is less than *siw*:
    - sVc1 = True.
  - Else:
    - sVc1 = False

  Formula:

  $$sVc1 = \begin{cases} 1 & \forall p \in sip : p < siw \\ 0 & else \end{cases}$$

- **sVc2** - Each entry's *si-Periodicity* in *SIB List* of the *Dynamic Cell List* matches one of the enumerated values as per 3GPP standards.
  Operation:
  - If each *sip* is in *pe*:
    - sVc2 = True
  - Else:

        * sVc2 = False

    Formula:

$$sVc2 = \begin{cases} 1 & sip \subset pe \\ 0 & else \end{cases}$$

- **sVc3** - Cell entry's *si-WindowLength* matches one of the enumerated values as per 3GPP standards.
  Operation:
  - If *siw* is on *we*:
    * sVc3 = True
  - Else:
    * sVc3 = True

  Formula:

$$sVc3 = \begin{cases} 1 & siw \subset we \\ 0 & else \end{cases}$$

sVer Formula:

$$sVer = \begin{cases} 1 & sVc1 = True \ \& \ sVc2 = True \ \& \ sVc3 = True \\ 0 & else \end{cases}$$

6.2.2 Timing Verification (tVer)

Ensuring timing values correspond with known values.

Variables

Variable	Description	OBS Mapping
cfc	Value of *connEstFailCount*.	*Dynamic Cell List Entry->Timing->connEstFailCount*
cft	Value of *UE-TimersAndConstants->T300*.	*Dynamic Cell List Entry->Timing->T300*
ce {...}	Enumerated proper values of *connEstFailCount*.	*Static Cell Lists->connEstFailCount*
te {...}	Enumerate proper values of *UE-TimersAndConstants->T300*	*Static Cell Lists->UE-TimersAndConstants->T300*

Verification Cases

- **tVc1** - Cell entry's *connEstFailCount* matches one of the enumerated values as per 3GPP standards.
  Operation:
  - If **cfc** is in *ce*:
    * tVc1 = True.
  - Else:
    * tVc1 = False

  Formula:

$$sVc2 = \begin{cases} 1 & cfc \subset ce \\ 0 & else \end{cases}$$

- **tVc2** - Cell entry's *UE-TimersAndConstants->T300* value matches one of the enumerated values as per 3GPP standards.
  Operation:

  - If *cft* is in *te*:
    * tVc2 = True
  - Else:
    * tVc2 = False

  Formula:

$$sVc2 = \begin{cases} 1 & cft \subset te \\ 0 & else \end{cases}$$

- **tVc3** - Cell entry's *connEstFailCount* is not the highest value enumerated in *CE*.
  Operation:
  - If *cfc* is not max value of *ce*:
    * tVc3 = True
  - Else:
    * tVc3 = False

  Formula:

$$tVc3 = \begin{cases} 1 & cfc \neq max(ce) \\ 0 & else \end{cases}$$

- **tVc4** - Cell entry's *UE-TimersAndConstants->T300* value is not the highest enumerated value in *te*.
  Operation:
  - If *cft* is max value of *te*:
    * tVc4 = True
  - Else:
    * tVc4 = False

  Formula:

$$tVc3 = \begin{cases} 1 & cfc \neq max(ce) \\ 0 & else \end{cases}$$

tVer Formula:

$$tVer = \begin{cases} 1 & tVc1 = True \ \& \ tVc2 = True \ \& \ tVc3 = True \ \& \ tVc4 = True \\ 0 & else \end{cases}$$

6.2.3 Duplication Verification (dVer)

Ensures a duplicate of cell doesn't exist.

Variables

Variable	Description	*OBS Mapping*
cid	The cell's Cell Identifier (ECI or NCI)	*Dynamic Cell List Entry->Identity->Cell Identifier*
pci	The cell's Physical Cell Identity	*Dynamic Cell List Entry->Identity->Physical Cell Identifier*
npl {...}	List of neighboring cells' PCIs.	*Dynamic Set Lists->Neighbor Cell List->Intrafrequency Neighbor Cell PCI List*; *Dynamic Set Lists->Neighbor Cell PCI List->Interfrequency Neighbor Cell PCI List*
cl {...}	List of neighboring cells' CIDs.	*Dynamic Set Lists->Neighbor Cell List->CID List*

Verification Cases

- **dVc1** - Ensuring the Cell Identifier isn't already present in current list of Cell Identifiers.
  Operation:
  - If cid is not in cl:

        * dVc1 = True.
    - Else:
        * dVc1 = False

    Formula:

$$dVc1 = \begin{cases} 1 & cid \notin cl \\ 0 & else \end{cases}$$

- **dVc2** - Ensuring the Physical Cell Identity isn't already present in current list of Physical Cell Identities.
  Operation:
    - If pci is not in npl:
        * dVc2 = True.
    - Else:
        * dVc2 = False

  Formula:

$$dVc2 = \begin{cases} 1 & pci \notin npl \\ 0 & else \end{cases}$$

dVer Formula:

$$dVer = \begin{cases} 1 & dVc1 = True \ \& \ dVc2 = True \\ 0 & else \end{cases}$$

6.2.4 Location Verification (lVer)

Ensures the TAC of current cell matches already known TACs in the *Dynamic Set Lists*' TAC List.

Variables

Variable	Description	*OBS Mapping*
tac	A Cell's Tracking Area Code	*Dynamic Cell List Entry->Identity->Tracking Area Code*
tl {...}	List of TACs for current suitable candidate cells.	*Dynamic Set Lists->TAC List*

Verification Cases

- **lVc1** - TAC is present in known TAC List at least twice..
  Operation:
  - If tac is in tl 2 or more times:
    * lVc1 = True.
  - Else:
    * lVc1 = False

  Formula:

$$lVc1 = \begin{cases} 1 & \sum_{t \in tl} 1_{(t=tac)} \geq 2 \\ 0 & else \end{cases}$$

lVer Formula:

$$lVer = \begin{cases} 1 & lVc1 = True \\ 0 & else \end{cases}$$

6.2.5 Priority Verification (pVer)

Determines if the cell's reselection priority is high compared to those in the *Dynamic Set Lists*' Priority List.

Variables

Variable	Description	OBS Mapping
crp	The cell's *cellReselectionPriority* value.	*Dynamic Cell List Entry->Priority->cellRelesectionPriority*
cl {...}	List of *cellReselectionPriority* values for current suitable candidate cells.	*Dynamic Set Lists->Priority List*

Verification Cases

- **pVc1** - The cell's *cellReselectionPriority* value is not highest in set {1,...,7}.
  Operation:
  - If crp is not 7:
    * pVc1 = True.
  - Else:
    * pVc1 = False

  Formula:
  $$pVc1 = \begin{cases} 1 & cft \neq 7 \\ 0 & else \end{cases}$$
- **pVc2** - The cell's *cellReselectionPriority* is not among the highest or the actual highest in the *Dynamic Static List*'s Priority List.
  Operation:
  - If crp is lower than the max value of cl:

        * pVc2 = True.
    - Else:
        * pVc2 = False

Formula:

$$pVc2 = \begin{cases} 1 & crp < max(cl) \\ 0 & else \end{cases}$$

pVer Formula:

$$pVer = \begin{cases} 1 & pVc1 = True \\ 0 & else \end{cases}$$

6.2.6 Neighborhood Verification (nVer)

Ensuring the cell's neighboring cells correspond with neighbor cells from current suitable candidate cells.

Variables

Variable	Description	OBS Mapping
cipl {...}	The list of Intrafrequency Cell PCIs for current cell.	*Dynamic Cell List Entry->Neighborhood->Intrafrequency*
copl {...}	The list of Interfrequency Cell PCIs for current cell.	*Dynamic Cell List Entry->Neighborhood->Intrafrequency*
dipl {...}	Current list of PCIs of Intrafrequency Neighbor Cells.	*Dynamic set Lists->Neighbor Cell List->Intrafrequency Neighbor Cell PCI List*
dopl {...}	Current list of PCIs of Interfrequency Neighbor Cells.	*Dynamic set Lists->Neighbor Cell List->Interfrequency Neighbor Cell PCI List*
cpci	Current cell's PCI.	*Dynamic Cell List Entry->Identity->Physical Cell ID*

Verification Cases

- **nVc1** - The cell's Intrafrequency Neighbor list isn't empty.
  Operation:

  - If cipl is not empty:
    * nVc1 = True.
  - Else:
    * nVc1 = False

Formula:

$$nVc1 = \begin{cases} 1 & cipl \neq \emptyset \\ 0 & else \end{cases}$$

- **nVc2** - The cell's Interfrequency Neighbor list isn't empty.
Operation:
  - If copl is not empty:
    * nVc2 = True.
  - Else:
    * nVc2 = False

Formula:

$$nVc2 = \begin{cases} 1 & copl \neq \emptyset \\ 0 & else \end{cases}$$

- **nVc3** - The cell's PCI is present in the *Dynamic Set Lists->Neighbor Cell List->Intrafrequency Neighbor Cell PCI List*.
Operation:
  - If cpci is in dipl:
    * nVc3 = True
  - Else:
    * nVc3 = True

Formula:

$$nVc3 = \begin{cases} 1 & cpci \in dipl \\ 0 & else \end{cases}$$

- **nVc4** - The cell's PCI is present in the *Dynamic Set Lists->Neighbor Cell List->Interfrequency Neighbor Cell PCI List*.
  Operation:
  - Condition:
    * nVc4 = True.
  - Else:
    * nVc4 = False

  Formula:

$$nVc4 = \begin{cases} 1 & cpci \in dopl \\ 0 & else \end{cases}$$

- **nVc5** - One or more PCIs in Cell's *Dynamic Cell List Entry->Neighborhood->Intrafrequency* are present in *Dynamic Set Lists->Neighbor Cell List->Intrafrequency Neigh Cell PCI List*.
  Operation:
  - If more than 1 PCI in cipl is present in dipl:
    * nVc5 = True.
  - Else:
    * nVc5 = False

  Formula:

$$nVc5 = \begin{cases} 1 & iX > 1 \\ 0 & else \end{cases}$$

  where

Variable	Description
iX	Intersection of *cipl* and *dipl* defined as: $cipl \cap dipl$

- **nVc6** - One or more PCIs in Cell's *Dynamic Cell List Entry->Neighborhood->Interfrequency* are present in *Dynamic Set*

Lists->Neighbor Cell List->Interfrequency Neigh Cell PCI List.
Operation:

- If more than 1 PCI in cipl is present in dipl:
  - nVc6 = True
- Else:
  - nVc6 = True

Formula:

$$nVc6 = \begin{cases} 1 & oX > 1 \\ 0 & else \end{cases}$$

where

Variable	Description
oX	Intersection of *copl* and *dopl* defined as: $copl \cap dopl$

nVer Formula:

$$nVer = \begin{cases} 1 & nVc1 = True \ \& \ nVc3 = True \ \& \ nVc5 = True \\ 1 & nVc2 = True \ \& \ nVc4 = True \ \& \ nVc4 = True \\ 0 & else \end{cases}$$

6.2.7 Signal Power Verification (spVer)

Ensure a cell's signal power isn't abnormally high when compared to those of other suitable candidate cell's.

Variables

Variable	Description	OBS Mapping
pci	The current cell's PCI.	*Dynamic Cell List Entry->Identity->Physical Cell Identity*
dspl {...}	List of entries in *Dynamic Set Lists->Cell Power List*.	*Dynamic Set Lists->Cell Power List*
zs	Z-Score of current cell's S_{rxlev}.	*No Mapping*
zt	Z-Score threshold, currently assigned as value **2** for this version of this standard.	*No Mapping*

Prerequisite Formulas

- Standard Deviation Formula

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i\mu)^2}$$

where

Variable	Description
σ	Standard Deviation value.
N	Population count of S_{rxlev} values in *Dynamic Set Lists->Cell Power List*.
μ	Population mean.

- Z-Score Formula

$$z = \frac{x - \mu}{\sigma}$$

where

Variable	Description
z	Z-Score.
x	Raw Score.
μ	Population Mean.
σ	Standard Deviation value.

Verification Cases

- **spVc1** - The current cell's S_{rxlev} *Z-Score* is below threshold.
  Operation:
  - Condition:
    * spVc1 = True.
  - Else:
    * spVc1 = False

  Formula:

$$XVc1 = \begin{cases} 1 & za < zt \\ 0 & else \end{cases}$$

spVer Formula:

$$spVer = \begin{cases} 1 & spVc1 = True \\ 0 & else \end{cases}$$

6.3 Verification Algorithm

This computation executes when a newly detected cell passes PLMN and Cell Selection procedures. The *Signal Power* VC (spVer) is ran first, to determine if newly detected cell possesses an abnormally high signal strength compared to those measured from current suitable candidates stored in the UE. If UE switches on and there are no current cells to base a measurement on then this is considered an automatic "pass", where the remaining 6 VCs are computed in order illustrated in Figure 6.3.1-a and described in 6.3.1. Since spVer alone isn't a sufficient bases of integrity failure, subsequent VC must be calculated in order to prove the ineligibility of a cell. In the case of an spVer failure, the VCs computed are considered as egregious offenders (VCs defined further in this section) and the failure of one of these is subject to fail the CSIV process.

6.3.1 VA Process

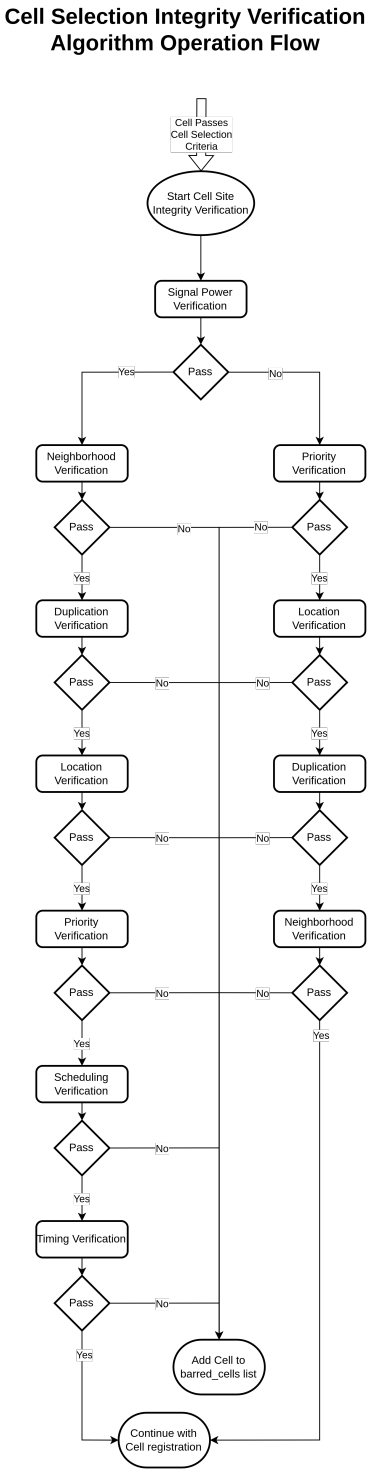


Figure 6.3.1-a. CSIV Algorithm Operation Flow

- When a new cell passes selection criteria:
  - Run Signal Power Verification
    * If Pass:
      · Run Neighborhood Verification.
        - If Pass - Continue.
        - If Fail - Move cell to barred_cell list.
      · Run Duplication Verification.
        - If Pass - Continue.
        - If Fail - Move cell to barred_cell list.
      · Run Location Verification.
        - If Pass - Continue.
        - If Fail - Move cell to barred_cell list.
      · Run Priority Verification.
        - If Pass - Continue.
        - If Fail - Move cell to barred_cell list.
      · Run Scheduling Verification.
        - If Pass - Continue.
        - If Fail - Move cell to barred_cell list.
      · Run Timing Verification.
        - If Pass - Continue.
        - If Fail - Move cell to barred_cell list.
      · Register with new Cell.
    * If Fail:
      · Run Priority Verification.
        - If Pass - Continue.
        - If Fail - Move cell to barred_cell list.
      · Run Location Verification.
        - If Pass - Continue.
        - If Fail - Move cell to barred_cell list.
      · Run Duplication Verification.
        - If Pass - Continue.
        - If Fail - Move cell to barred_cell list.

- Run Neighborhood Verification.
  - If Pass - Continue.
  - If Fail - Move cell to barred_cell list.
- Register with new Cell.

6.3.2 Formula

$$V(C) = \begin{cases} 1 & (spVer = 1 \,\&\, pVer = 1 \,\&\, lVer = 1 \,\&\, dVer = 1 \,\&\, nVer = 1) \mid \\ & (spVer = 0 \,\&\, nVer = 1 \,\&\, dVer = 1 \,\&\, lVer = 1 \,\& \\ & pVer = 1 \,\&\, sVer = 0 \,\&\, tVer = 0) \\ 0 & spVer = 0 \,\&\, (\, nVer \mid dVer \mid lVer \mid pVer \mid sVer \mid tVer) = 0 \end{cases}$$

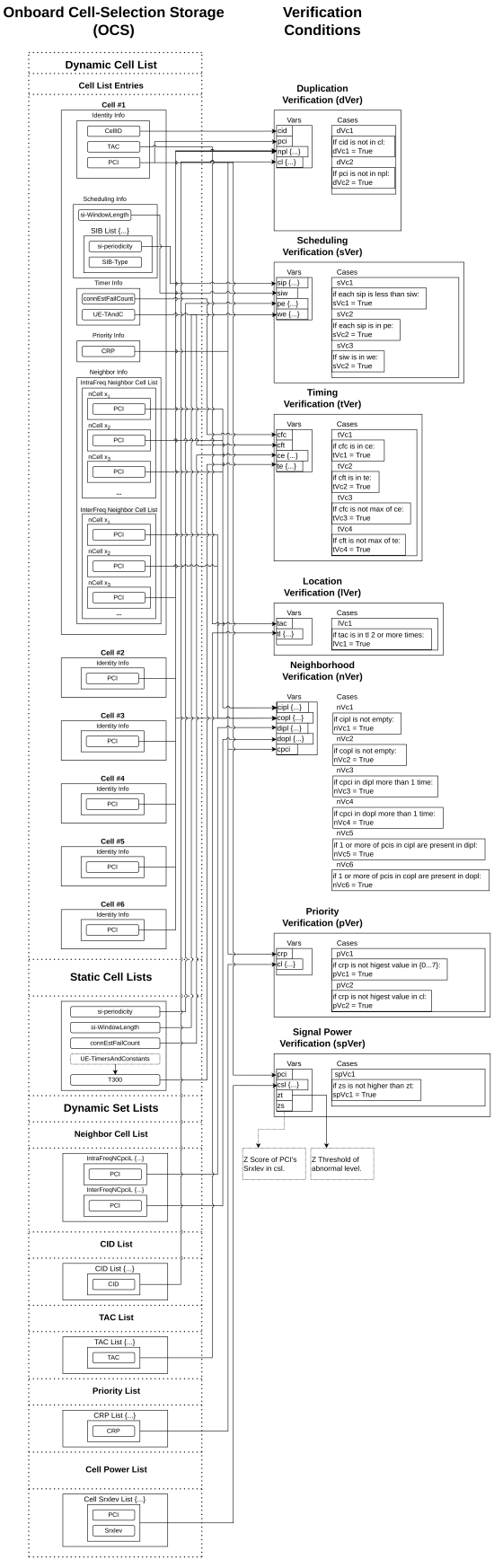
6.3.3 Initial Stored-Info Cell Selection

Initial Cell Selection is defined in 3GPP TS 36.304 & 3GPP TS 36.304 as having "no prior knowledge of which RF channels are NR frequencies", whereas *Stored-Info Selection* is defined as requiring "stored information of frequencies and optionally also information on cell parameters from previously received measurement control information elements or from previously detected cells".

CSIV is primarily meant for processing the integrity of *detected cells*, meaning those who have directly made itself known to the UE and performs measurements thusly. While it is not meant for measuring integrity of cells with limited stored parameters via *Stored-Info Cell Selection*, implementers of this specification **MAY** adapt the Verification Algorithm to account for whatever Verification Conditions apply to information available as part of *Stored-Info Cell Selection*.

7 Appendices

7.1 Appendix A - OCS + VC Mapping



7.2 Appendix B - Changelog

Date	Change/Comments	New Version
6/7/2022	Version 0.1 drafted.	Version 0.1
6/17/2022	Correcting figure numbers for figures: • Figure 5.1.1-a. Dynamic Cell List • Figure 5.1.1-b. Dynamic Cell List Entry • Figure 5.1.2-a. Static Cell Lists • Figure 5.1.3-a. Dynamic Set Lists • Figure 6.1-a. OCS Flow • Figure 6.1-b. OCS Process (Cell Selection Succeeds)	Version 0.2

6/17/2022	Modified case 1 of piecewise notation case to include proper parentheses in Section 6.3.2.	Version 0.2
6/18/2022	Correct variable name "za" to "zs" in section 6.2.7.	Version 0.2
6/17/2022	Text edits to Sections: • 5.2.1 • 5.2.2 • 5.2.4 • 6.1	Version 0.2
6/18/2022	New figure images: • Figure 5.1.1-a. Dynamic Cell List • Figure 5.1.1-b. Dynamic Cell List Entry • Figure 5.1.2-a. Static Cell Lists • Figure 5.1.3-a. Dynamic Set Lists	Version 0.2

6/18/2022	Fixed Variables table in Section 6.2.5.	Version 0.2
6/18/2022	Modified width of Example images in Section 5.1.1.	Version 0.2
6/18/2022	Formatting modifications throughout document.	Version 0.2
6/21/2022	Publish Version 1.0.	Version 1.0

8 Acknowledgements

The following individuals provided contributory significance to the current state of this document described herein:

- **Rodney LaLonde**
  Document review & spVer VC formula input.
- **Anthony Candarini**
  Document review.