DTN-based Formula Student Rule Enforcement

Sebastian Schildt, Wolf-Bastian Pöttner, Johannes Morgenroth, Bennet Sartori, Lars Wolf
Institute of Operating Systems and Computer Networks
Technische Universität Braunschweig, Braunschweig, Germany
Email: schildt | poettner | morgenroth | sartori | wolf @ibr.cs.tu-bs.de

Willem Almstedt, Hendrik Heine, Sandra Hesse, Eduardo Jiminez, Tim Lüdtke, Vinh Tran
Institute of Operating Systems and Computer Networks - Android Lab
Technische Universität Braunschweig, Braunschweig, Germany
Email: android-lab@ibr.cs.tu-bs.de

Daniel Mazur, Tobias Michaels, Christoph Stamprath, Nicolas Steinwand
Formula Student Germany
Email: mazur | michaels | stamprath | steinwand @formulastudent.de

***Abstract*—In Formula Student (FS) / Formula SAE (FSAE) competitions students build single seat formula race-cars with which they compete against teams from all over the world. Despite static disciplines such as cost reports, teams compete in multiple dynamic disciplines driving the car. An important set of rules deals with the necessary prerequisites for a driver to enter a discipline and the maximum amount of runs each registered driver is allowed to drive. So far these rules have not been enforced adequately by most international events.**

In this paper we present the design and implementation of a prototype system using Radio-Frequency Identification (RFID) and Delay Tolerant Network (DTN) technology to document and check compliance with the rules. We share experience gained during a prototype trial during the Formula Student Germany 2013 event.

I. Introduction

In Formula Student (FS)[1] and Formula SAE (FSAE)[2] competitions students build single seat formula race-cars with which they can compete against teams from all over the world. Teams compete in multiple dynamic disciplines driving the car. However, the competition is not won solely by the team with the fastest car, but rather by the team with the best overall package of construction, performance, and business planning.

Since the competition is primarily focused on the design of the race cars, influence of the driver shall be kept as low as possible to avoid teams hiring professional race drivers to score more points. Therefore, individual drivers may only compete in a subset of the dynamic disciplines and further in a subset of the runs (heats) in each discipline [11]. Safety is a prime concern during events. On every day with dynamic disciplines there are mandatory driver-briefings. Only after attending these briefings drivers are allowed to compete on that particular day. To enforce and check adherence to this rules, the legacy system requires drivers to wear multiple one-time wristbands. Every driver wears a personal wristband with a number and receives a colored wristband for each driver briefing (see Figure 1). At past Formula Student Germany (FSG) event, paper-based lists have been used to document the runs of each driver.

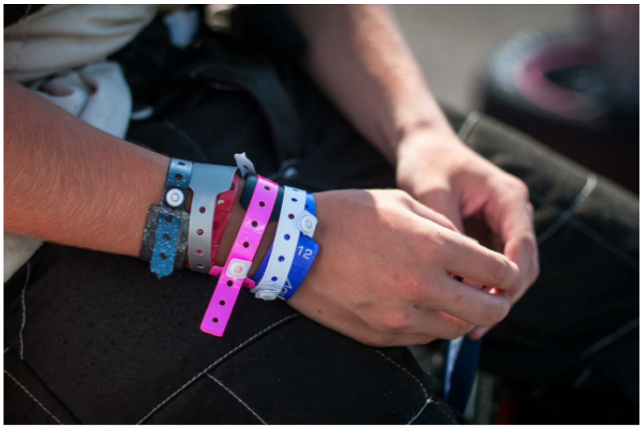


Figure 1: Legacy System requires one wristband per day

Especially for the yearly FSG competition this approach does not scale so well anymore. With 115 teams and more than 300 registered drivers distributing and checking wristband efficiently *and* accurately has become infeasible. Therefore, in the middle of 2012 a decision has been made to consider technical solutions for the problem. In cooperation between the FSG and TU Braunschweig the development of a system to improve driver management has been started. Finally, in 2013 the system was ready to be tested alongside the old pen & paper approach during the FSG 2013 event, which took place from July 30th to August 4th on the Hockenheim racetrack[3] in Germany.

The contributions of this paper are as follows: We present a complex cyber-physical communication-centric system integrating various technologies that are a hot topic in industry such as Radio-Frequency Identification (RFID) technology

[1] http://www.formulastudent.de/

[2] http://students.sae.org/competitions/formulaseries/

[3] http://www.hockenheimring.net/en

and mobile applications as well as Delay Tolerant Networks (DTNs), a technology straight from research. As of today, this is one of the few examples where DTN technology has been used in a “real” application and not just some research prototype. In this paper we will describe the implemented system and the experience gained from the FSG 2013 event.

II. Requirements

There are some constraints and requirements the system has to deal with. An important part are the rules the system is designed to enforce. Another set of challenges stems from the fact that the system needs to be deployed ad-hoc without any guarantees regarding the availability of infrastructure.

A. Formula Student Rules

During an FS/FSAE event there are 4 dynamic disciplines in which a team can compete: *Acceleration*, where the goal is to finish a 75 m sprint in the shortest possible time, *Skidpad*, where cars drive on a figure-of-eight track, *Autocross*, which is one lap on a track of approximately 805 m where the result determines the starting position for the *Endurance* discipline, which goes for a total distance of 22 km on the Autocross track. *Endurance* is counted as two disciplines since the overall time as well as the fuel-efficiency of a car yield points. For *Acceleration*, *Skidpad* and *Autocross* each team has two heats. These disciplines are open for a predetermined time during the event, and a team can queue to compete in a discipline anytime.

For all disciplines a driver is only allowed to drive if he attended the associated driver briefing on that day. Furthermore, while a driver can compete in more than one discipline, he is only allowed to take one heat in a specific discipline and can compete in at most 3 of the 5 disciplines. This is to preclude teams from focusing their efforts on professional drivers, as FS is intended as design competition with a strong focus on engineering and to a lesser degree on driving skills. A prerequisite for all cars is to pass mechanical and electrical safety checks to ensure that cars adhere to FS regulations and specifications.

To be able to reliably check whether a driver attended the drivers briefing is especially important, as the drivers’ and track marshals’ safety depend on it. If there is doubt whether a driver attended the briefing, he will not be allowed to drive. If there are doubts whether the driver already exceeded his number of runs, he might be allowed to drive. If later cross checking reveals that he was indeed over his allowed number of heats that run will be nullified. At the digression of the scoring team there might be further penalties for breaking the rules. Therefore, it is desirable to be able to reliably check the number of runs before a driver enters a heat.

As the safety and fairness of the event depends on the data collected by the system presented in the following sections, it needs to be resilient against different attacks, such as modification of collected records, even if hardware gets stolen (for details see Section III-D). Also, the system should be robust enough to be able to gracefully deal with situations where the communication infrastructure breaks down.

B. Challenges

While there is a Wi-Fi network deployed during FSG events, this is not true for some of the other FS events, and even with Wi-Fi, connectivity can be intermittent and coverage incomplete. A typical FSG event has several hundreds of team members and volunteers and thousands of visitors. With such a high number of people, and thus possible attackers, the system should be hardened against all foreseeable attacks. Additionally, the system will be used by volunteers who have not been involved in the development of the system. This demands good usability, so that the system can be used by anyone after a short introduction.

III. Architecture and Design

This section will detail the overall architecture of the system. We motivate the choice of RFID technology, describe the use cases and provide an analysis of potential attack vectors and measures taken to defend the system. We then continue to present the developed software modules and applications.

A. Smart Card Technology

The goal of this project is to replace the variety of wristbands with a single RFID based wristband. Because the Time Keeping (TK) system uses Ultra-High-Frequency (UHF) RFID technology to identify cars, the aim was to choose a technology that would not interfere with the essential TK system. The first basic design decision was, whether an RFID tag should only identify a driver or should carry actual information. In the first case a tag only needs to store a permanent ID and all book keeping must be done at a backend. We opted for the second option: Storing all required information on the bands themselves, effectively making them self-contained. The goal was to make the system resilient against failures in the backend or communication infrastructure: In case of problems the system should be able to continue functioning locally using just the information available on the RFID wrist band to prevent any interruption of the dynamic disciplines. Basically this requirement demanded the use of proximity card technologies (ISO/IEC 14443 [3]). This RFID technology only works across a few centimeters, but its various implementations can store up to a few kBits of data. The alternative, vicinity cards (ISO/IEC 15693 [2]), have an effective range of 1 - 2 m, but a very low data-rate, and can usually only store a few bytes of data. Different vendors offer cards implementing either of those standards.

Due to the high availability and market penetration we considered NXP’s MIFARE family of proximity tags. The MIFARE Ultralight [5], [6] family is not an option as it only support 64 bytes to 192 bytes of usable storage. Most Ultralight variants do not support any kind of security mechanism despite write protection. The most widespread RFID card is the MIFARE Classic system [8] offering storage capacities of 1 kiB to 4 kiB. MIFARE Classic supports authentication and block based access rights depending on crypto keys. However, the proprietary crypto system has been thoroughly broken [1], which today makes the MIFARE Classic security features basically worthless. The MIFARE Plus S [9] was introduced as a successor. While remaining backwards-compatible with the widely deployed MIFARE Classic system, it supports upgraded security mechanisms based on the AES standard. The last option is the MIFARE DESfire EV1 [7] system available in capacities ranging from 1 kiB to 8 kiB. This smart card includes abstractions to support several applications on a single chip.

In the end we decided to use a system based on MIFARE Classic RFIDs. We do not need the additional features of the DESfire variant, and the MIFARE Classic is the most widespread and cheapest solution offered by most suppliers. With regard to the broken security, we opted to implement our own security, which should make the system rather independent from the actual RFID system used. As we will see in section III-D our security concept depends on only two features, which are provided by the MIFARE Classic system: A unique immutable serial number for each RFID and the ability to permanently and irrevocably write protect sectors.

B. Use Cases

Based on the FSAE rules [11] and hands-on experiences during past FSG event we have identified the following use cases for the system:

Driver Registration: When a driver arrives at the event grounds to register as driver he gets his wristband identifying him as driver. The band needs to be initialized. This should be done using a laptop computer running Linux or Windows operating systems. Drivers can be selected from a list fetched from the FSG website backend. The driver wristband must be held to an USB RFID device connected to the computer which will write the registration record to the RFID chip. The wristband is initialized with personal information, such as name or team affiliation, obtained from the central FSG database. This process is similar to the legacy process of registering drivers, with the only exception that the wristband needs to be held against the RFID writer before it is put on the driver's wrist. Since the driver registration is located in an office environment, we can assume a permanent and rather stable network connection.

Safety Briefing: Every morning drivers need to arrive in time for the briefing. With the legacy system the drivers get individually colored wristbands for each meeting which are distributed and put on by volunteers. With the RFID based system there are a couple of laptop computers running Linux or Windows (see figure 2). The application should not require any user interaction except placing an wristband onto the USB RFID device. When a wristband is detected, a briefing record is written and a screen indicating success (green) or failure (red) is shown to the driver. For capacity reasons in the RFID as well as in the legacy system, drivers get their wristband or their record upon entering the meeting, because all drivers arrive over the course of a couple of minutes while everybody is leaving at the same time. In the seldom occurring case that a driver needs to leave during the meeting there is only one exit available. Volunteers will either cut the meeting wristband (legacy system), or in case of the new system, write information about the canceled briefing to the wristband.

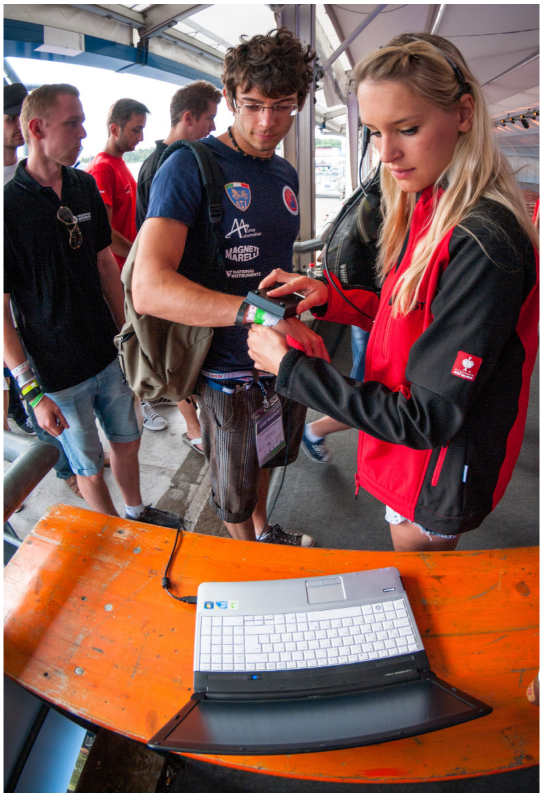
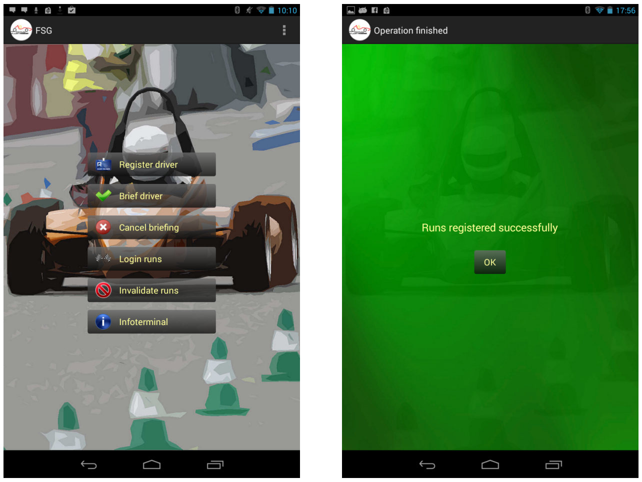


Figure 2: Driver safety briefing (Photographer: Grams)



Operation finished

Runs registered successfully

OK

(a) Start Screen

(b) RFID Action succeeded

Figure 3: Mobile Application

Dynamic Disciplines: When a driver wants to compete in a dynamic discipline there is a volunteer with an Android device at the top of the queue. The application (see Figure 3) is preconfigured with the correct type of discipline (*Acceleration*, *Skidpad*, *Autocross* or *Endurance*). Whenever a wristband is brought close to the RFID device, compliance with rules is checked. If successful, a run record is written to the wrist band. Any failure to comply with the rules is indicated, and the volunteer or other dynamics personnel need to decide what to do. If they choose to override the system, and let the driver have its heat anyway, this incident will also be stored on the wristband.

C. System Overview

The developed system consists of a backend server that can provision the mobile devices and collect information sent by them. Android Devices are used in the field to interact with the RFID tags. All devices have access to the local Wi-Fi network. However, continuous Wi-Fi connectivity cannot be ensured everywhere on a typical Formula Student event site. To cope with transient connectivity, we base all communication on DTN technology. More specifically we use IBR-DTN [12], [4], a Bundle Protocol (BP) implementation for Linux and Android. Delay Tolerant Networking approaches replace the end-to-end semantics of common protocols such as IP with a hop-by-hop store and forward architecture. Originally devised for interplanetary networks where nodes might see each other only occasionally, this approach has also been widely applied for opportunistic ad-hoc networks with high mobility such as vehicular networks. The BP is a standardized and widely used DTN protocol. It supports optional end-to-end acknowledgements on top of the hop-by-hop approach. In fact, the BP can be seen as a superset of IP (and TCP, as it includes elements from both the networking and the transport layer): In continuously connected networks it works much like the former, while in addition it is able to deal with disruptions of the network. This leads to the use of the BP in networks with mobile devices such as smart-phones, which are regularly but intermittently connected to the Internet. These characteristics make a BP-based network a good fit for this application

A shadow copy of the state of all wristbands is held in the backend in order to detect manipulation. A wristband is a block-based storage of up to 4 kiB of data that we organize in various records. Each record represents one briefing/run/etc. that the driver has performed (see Section III-D). Whenever a wristband is read by one of the devices, all records are checked and verified. Data from the backend is only necessary for initializing the wristband.

After changing information in the backend (such as the personal information of a driver), updates are send out to all devices via the DTN network. Devices that receive such an update merge it into their local database. Furthermore, since wristbands are self-contained, only the driver registration process is required to have access to the complete database. Thus, rule enforcement is done in a fully distributed fashion by each individual hand-held device. Each time one of the involved devices reads a wristband, the complete state of the band is sent to the backend for advanced security checks. This allows detecting manipulations of the wristbands that are not covered by the manufacturers specifications.

D. Security Measures

To design the security architecture we analyzed different attack vectors the system should be resilient against. The goal was to ensure that drivers who break the rules can be reliably detected. Also the specific requirements towards the underlying hardware (especially the RFID tags) should be kept at a minimum to make the system as future-proof as possible.

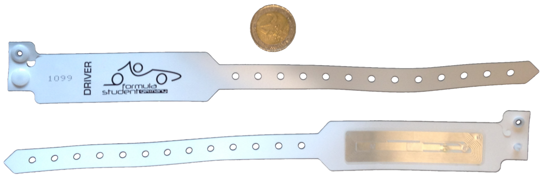


Figure 4: One-time wristband with embedded RFID chip and 2 € coin for size comparison.

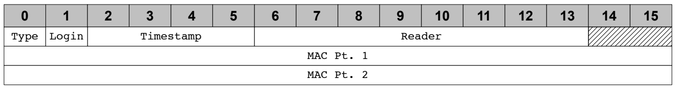
Physical Attacks: Swapping of wristbands to gain more runs should not be possible. Also a driver should gain no advantage from destroying a wristband. Of course, since bands might be inadvertently destroyed, there should also be no permanent disadvantages. This is achieved by using one-time wristbands (see Figure 4): After the band is closed, opening or removing it will destroy the wristband. Should a wristband get unintentionally damaged or destroyed, a driver can go to the service desk and request a new wristband that will be restored from backend data, while the old wristband will be blacklisted. It is not possible to cheat the system by destroying the wristband after a run: A driver is only logged into a run with a working wristband, and *eventually* that record will be transmitted to the backend. Even if a driver can gain a temporary extra run through good timing, this will be detected eventually.

Manipulation of data: The basic types of possible manipulation are: Adding records to the band, removing records or modifying existing records. Removing or modifying records is not possible because the used RFID chip has the ability to permanently set sectors as read only. This setting is irreversible and not dependent on any cryptography. Adding records is prevented by securing each record with a Keyed-Hash Message Authentication Code (HMAC), with a key stored on the RFID readers.

Cloning of data: Copying valid entries from one wristband to another is precluded by the fact that the data secured by the HMAC also includes the immutable serial number of the RFID chip, which is distinct for each wristband. Should any of the outlined mechanisms to prevent manipulation of data fail, there is second layer of protection due to the fact that on each transaction the content of the *whole* band is sent to the backend. This allows catching manipulations such as deletion of records (which should be impossible) by comparing the wristband state stored in the backend with a new scan coming in from one of the mobile devices.

Theft: A tablet running the software might get stolen and used to manipulate wristbands. While we consider this a rather low risk, there are some mechanisms to mitigate the effects: The device and app can be protected with a password, and the individual reader IDs can be blacklisted in the backend. Therefore, all records from a rogue reader can be identified by the backend.

Tampering with backend communication: If the wristbands themselves can not be hacked, an attacker might turn its attention to the backend, submitting false data. However, this is as difficult as tampering with the bands directly, as the backend always expects data bundles representing complete



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Type	Login	Timestamp				Reader								▨	▨
MAC Pt. 1															
MAC Pt. 2															

Figure 5: Wristband Data Format: Briefing Record

valid bands. A denial of service attack is however always possible. Due to the DTN design principles of the system, it will continue working with just the mobile devices and no available backend, giving the operators time to sort out a DoS attack.

Open Source: None of the implemented security measures depend on the secrecy of the source code. Access to the source code or, for instance, reading this paper, should not make it possible to compromise the system. Only keys need to be secret, and only standard cryptographic functions such as SHA-1 are used.

E. Data format

The system is designed around the drivers' wristbands. All relevant data to check rule compliance and log certain events resides on the wristbands to cope with outages of the network. Records are stored on the wristband are permanently write-protected. Furthermore, each record contains an HMAC that covers all information of the record as well as the unique wristband ID and a secret system key. Wristbands that do not contain any records are not accepted by the system and must be initialized first. Whenever a wrist band is read by one of the devices, all records are checked and verified. If at least one record has an invalid HMAC, the whole wristband is considered to be invalid.

The memory on a 4 kiB MIFARE Classic chip is organized in 32 sectors of 4 blocks and 8 sectors of 16 blocks. A block is always 16 bytes. The first block of each sector is reserved to store MIFARE Classic specific access rights. By setting write protection for a block and disallowing any change of access rights regardless of key, a sector can be permanently write protected. Therefore, a 4 block sector can store 48 bytes of information. As the write protection works on sector level, the goal is to fit any record into a single sector. The following records can be stored:

Registration Record: The registration record is written during driver registration when an empty band is initialized. The registration record is always the first record on a wristband. It uses two sectors and is thus the only exception to the rule that each record should use one sector. The reason is that the 0'th sector has only 32 bytes of usable data. These are used for the HMAC. The actual data is in sector 1. All records start with a type ID, identifying the type of the sector. In addition the registration sector stores a driver ID, a team ID, a FS class ID (at the moment only electric or combustion) and a car ID. The remaining space is used for the driver's name.

Briefing Record: The briefing record (Figure 5) stores, whether a driver attended the drivers' briefing. The "login" field defines whether a driver attended or aborted a meeting. Keep in mind, that due to the write protection a sector cannot be modified after it has been written. Therefore another record needs to be written to invalidate a previous record (see also Section III-B). A time-stamp indicates the time of the briefing and the reader ID identifies the device that created the record.

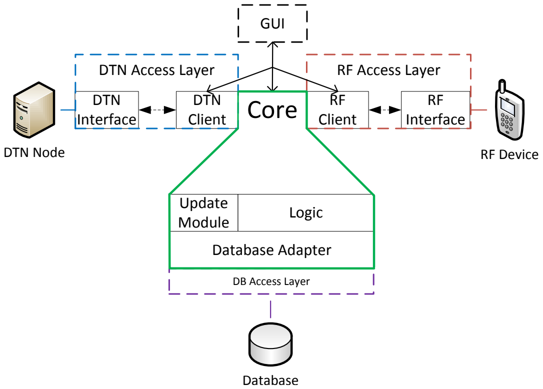


Figure 6: Software Design Overview

Run Record: A run record is written on track, when a driver passed the checks of the system and is allowed to compete in a dynamic discipline. The login fields works similar to the briefing sector. Logging out a run becomes necessary if the driver commences a heat, but can not finish it due to circumstances outside his control, such as people or broken down cars on track (when according to the rules he gets a "rerun"). For the *Skidpad* discipline a driver can decide to take his two heats at once, which will be marked in the count field. The "Dscpl" field identifies the discipline as introduced in section II.

Blacklist Record: The blacklist record (not pictured) can be used to invalidate a still working RFID chip. This can happen if a wristband is replaced due to physical damage or erratic behavior. No reader will accept a wristband which has a blacklist record on it. A blacklist record is composed of a type-field, the time-stamp, the reader ID and the HMAC.

F. Software Components

The system consists of four main software applications:

1) Backend server
2) Driver registration software
3) Briefing login software
4) Mobile Android application

Except the backend server, all software is designed to be used by any FSG volunteers after only a small introduction of a few minutes. As we made the decision to use Android as our mobile platform, most part of the software is written in Java. Actually, the core data structures and application logic are written in plain Java and shared across all platforms (see Figure 6).

The core logic includes a generic DTN communication interface, which is connected to the IBR-DTN [12] protocol stack when running on a PC platform and to the IBR-DTN's Android API [4] for the mobile applications. Similarly, the RF client interface abstracts the communication with an Near Field Communication (NFC) reading device. For the PC applications we interfaced an off-the-shelf USB desk reader, while on Android we wrapped the Android NFC API.

Backend Server: The backend server has been implemented as Java EE application using the Tapestry[4] framework. It will aggregate DTN messages it gets from mobile Android devices and put the received data in a PostgreSQL[5] database. As an Android device always sends the complete wristband content on any transaction, the history of a wristband can be followed in great detail. The backend will do consistency checks off all received data, and flag a warning in the web interface if some inconsistencies or violations are detected. The user can annotate those warnings and flag them as solved. Furthermore, the backend is used to provision the Android devices: New driver databases or blacklists can be created and distributed to the devices in the field using DTN.

Driver Registration Software: The Driver registration software is used by volunteers to initialize wristbands upon driver registration. The software runs on a laptop with a desk NFC reader. The GUI supports searching for a registered driver by his name or team. The driver database used by the application is downloaded from the official Formula Student Germany web-server using an encrypted and authenticated web-service. All participating teams are required to register on the FSG homepage.

Briefing Login Software: While the Android application is capable of writing briefing information to the wristband, we developed a specialized solution that enables higher throughput while needing fewer volunteers. A laptop is equipped with up to two NFC readers situated left and right of the device. Drivers are required to put their wristband on the reader, and check whether the half of the screen for their queue lights up green. Thus one volunteer is enough to supervise two queues, and only needs to intervene, if there are technical problems with the system.

Android Software: The Android software wraps the complete functionality of the system, including the driver registration and briefing functionality. This allows a mobile person to perform any tasks within the system. Some of this functionality can be locked, so it can not be used without a password. The prime functionality of the Android software is logging in runs. A clear and simple UI design ensures that a stressed volunteer on track with bad visibility due to sunlight can use the application effectively. The complete screen will turn green or red depending on the result of the operation. That means during routine operation a user only needs to set-up his discipline once and hold the device to a driver's wristband until the screen turns green.

IV. FSG 2013 Trials

The system has been tested during the FSG 2013 event (July 30th to August 4th) in all use cases: Driver registration, driver briefing and checking in runs for all dynamic disciplines. Figure 7 shows an overview of the event grounds. The map shows the position of indoor Wi-Fi access points (AP X) and outdoor access points (OAP X). Generally, Wi-Fi availability at certain locations can be hard to predict and the setup shown in Figure 7 is the result of 3 years of experience and evolves every year. The primary goal of the Wi-Fi system is to provide teams and visitors with Internet access. There is quite a bit of contention in the spectrum, as apart from the depicted APs several dedicated Wi-Fi bridges are used to connect cameras and or extend the network to areas where no fiber or copper link is available. More directed and undirected Wi-Fi links are used for critical infrastructure such as the timing and display system. Some more hard to predict or control Wi-Fi interference is caused by people using 3G hot-spots or teams using wireless telemetry systems.

A. RFID Wristbands

As seen in Figure 4 the sourced wristbands have the RFID chip and antenna laminated between two sheets of plastic. A problem was the high failure rate of the RFID bands. We needed to replace almost 20% of all wristbands during the event. This number is clearly too high. As wristband failure was detected mostly during the driver's briefing (after the night), this problem could be dealt with on the spot. We assume mechanical problems or insufficient water resistance. While a postmortem did almost never show any problems with the antenna, there might in some case have been problems with the hair-thin bonding connections between RFID chip and antenna. Also we do not know how moisture would affect the RFID system if it gets captured between the plastic layers. We are positive the failure rate could be decreased in the future with a changed mechanical design of the wristbands.

B. Driver Registration

Driver registration was done at location 2 ("Sachs") in Figure 7. This was pretty straightforward as the Sachs building is used as main office during the event, and therefore has good network coverage and in case of unforeseen problems IT support is also located there. For the volunteers doing the registration, the new process was not a problem: Even in the old system, they need to look up the drivers details in the FSG backend database and issue a special wristband. Just as with the old system, wristbands will not just be given out, but also attached to the registered driver, to prevent fraud by giving the band to another person after registration.

C. Driver Briefing

The driver briefings took place in locations 4 and 5 ("Boxendach"). Laptop with USB desk RFID readers have been used to log briefings to the wristbands (see Figure 2). This procedure has been generally uneventful and just worked as intended, except a higher than expected number of broken wristbands. Replacing the bad bands at this point was a nuisance, but did not pose any problem.

D. Dynamic Discipline Login

As the Wi-Fi coverage is focused around the visitor and exhibition areas, Wi-Fi availability is not guaranteed on the racetrack. The *Acceleration* discipline takes place in region 14 at the bottom of the map. The nearest Wi-Fi APs are in areas 5 and 6 ("Boxendach"), which are heavily loaded during *Acceleration* as this area is accessible to visitors. The *Skidpad* discipline takes place in the middle of the dynamic area (to the

[4] http://tapestry.apache.org

[5] http://www.postgresql.org

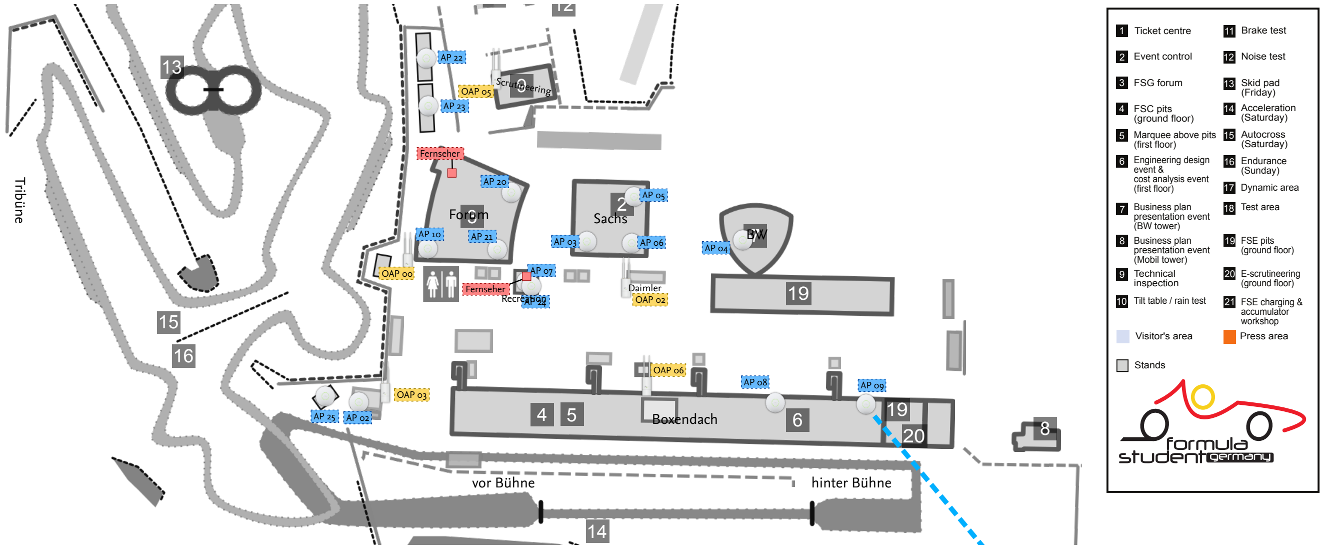


Figure 7: FSG 2013 part of the Event Grounds at Hockenheim Racetrack

left in Figure 7) at the figure of eight denoted by number 13 far away from any AP. The start of the *Autocross* and *Endurance* track is at location 15 and 16 and is thus well covered by OAP 01.

Low Wi-Fi signal strength combined with the fact that some teams use RF telemetry sometimes based on high powered Wi-Fi systems or technologies using the same band can make connectivity to the Wi-Fi in the dynamic areas spotty. It would be hard to deploy Wi-Fi infrastructure specifically to allow the mobile tablets predictable coverage. First, inside the dynamic area it is not always possible to get electricity and due to long queues in certain disciplines, sometimes the position where drivers are logged in can change. In order to make sure the racetrack gets maximum utilization, the volunteer doing the driver logins might move back along the queue, to login drivers before they are at the top of the queue. Even though some of the drivers might need to get logged out again, if the discipline closes, or if due to technical problems they will not be able to start once at the top of the queue, this approach still saves some time.

The actual scanning of the RFID band has not been faster than checking of the correctly color-coded wristband in the old system. The volunteer sometimes needs to fiddle with the drivers racing overall, to either see the color of a band or in the new system, position the tablet, so it can read the RFID tag. Reading the tag through the overall is not always possible and depends on the location of the band. While the new system does not save any time here, it should be noted that the manual system only checks whether a driver has a briefing, and documents that he took this run. Whether this particular driver or team is still eligible for a run, was usually not checked on track.

Even though scanning could have been faster, the new system did not introduce any additional delay as other parallel processes took more time. The most demanding discipline in this case is *Acceleration*: A run just consists of a 75 m sprint. After a car ran and clears the track, the next car is allowed to go. Statistics show that in 2013 we managed to get up to a frequency of 22 cars per 10 minutes (27 s/car), which is in line with the achieved performance in previous year's FSG 2012 event and one of the highest throughputs of all FS/FSAE events.

There have been no problems with the DTN: Basically, the person using the tablet to scan just did not care, whether his device was connected or not. In the backend we could see the records coming in, sometimes at intervals, without the person in the field noticing any different behavior in the application. After a discipline or during a longer break, we adopted the habit of searching a spot with Wi-Fi and let the device resend its complete database. While we did not spot any lost bundles, in hindsight this approach is very foolproof, as the backend filters out duplicates. It does not hurt to let the mobile devices reexport their whole database in a controlled environment "just to be sure" at the end of the day.

E. Rule Enforcement

While there was no deliberate attempt to break the rules, the system flagged a warning for a presumably not briefed driver. That driver was allowed to drive using the system's override because he had the appropriate briefing wristband from the legacy system. Shortly after that driver was scanned on track, the backend flagged a warning. Investigation showed that this driver in fact was not able to attend the driver's briefing in the morning, but instead got a private briefing at a later time. At this time he was only issued the compulsory wristband of the old system, but his RFID wristband has not been updated. This has proved that the system is capable of detecting rule violations on the spot.

F. Lessons Learned

For future events the RFID tags definitely need to be replaced with more robust ones. Even in the current prototype state, where the system was used alongside the legacy system, it did not introduce additional delays in the dynamic disciplines, which was a core requirement. Some extra time was required during the briefing to replace the broken bands. The additional time was not a problem and can be easily alleviated by sourcing better wristbands next time.

In 2013 we collected more precise and reliable data about the runs done by each driver, and could assure adherence to the rules. While we covered most of the technical challenges quite well for a new system, interestingly we ran into some unexpected policy hurdles: It was unclear, who is responsible for the data. In the events before, the only thing that has really been checked was, whether a driver attended a briefing. If not, the dynamics personal would simply refuse him to drive. It seems, despite the records, nobody *ever* checked proactively if the rules regarding the number of run have really been followed. Only in case of disputes somebody would dig into the records. This absence of processes or a responsible person was not caught before because everybody agreed, that generally the system is a good idea, and that somebody should improve the quality and efficiency of rule enforcement. It turned out that nobody identified himself with "somebody". This was not a problem this year, but will be rectified in the future because if there would be any disputes on track regarding the correctness of the system, somebody should be responsible.

The DTN architecture worked flawlessly and let volunteers use the mobile Android devices without needing to worry about Wi-Fi coverage and availability. This is a testament to the applicability of DTN in such scenarios as well as the stability of the IBR-DTN implementation. In light of the rudimentary qualities of the old pen & paper system with the colored wristbands, it has been pointed out to the authors, that the new system might be over-engineered for the purpose and that a simpler systems might have been good enough: Less security that probably nobody will attack anyway, a centralized database without self contained RFID tags, as this will also detect inconsistency eventually. We understand this as a compliment, as from the end-user perspective the advanced capabilities of the presented system did not make interacting with it more complex.

V. Conclusions

We presented an RFID based system for managing drivers during an FS/FSAE event. The presented system is the culmination of work done during a university lecture, a master's thesis and the work of FSG volunteers. The work presented here is a good example how research predominantly done in university such as DTN networks, can be applied in the real world if enough engineering resources are invested. While the system and experiences presented here do not include thousands of data points or simulations, we feel in some cases experiences gathered by implementing something for real can be at least as worthwhile and a good addition to loads of rather artificial numbers.

The developed system can be used to enforce FS/FSAE rules and safety regulations regarding the drivers. It transforms a previously manual process into a fully digital and highly automated process. We use state-of-the-art RFID technology to allow for self-contained driver wristbands with no need for backend connectivity while on the race track. Since we do not rely on the security of the RFID system, security breaches of the underlying RFID system do not harm the security of our system. The RFID chips in the wristbands only have to support a permanent write protection on a per-block basis and have an immutable ID. For communication with the backend we use delay tolerant networks coming straight out of research to cope with intermittent connectivity. While this may not yet be the holy grail of a DTN killer-application [10] it is another proof that there are applications where DTN can make a difference.

We performed a full trail roll-out during the FSG 2013 event, which is one of the largest FS events worldwide. The system worked as intended and we collected valuable input to improve performance in the coming years.

Acknowledgements

We would like to thank the Formula Student Germany e.V. for providing us with the opportunity and funds to deploy the system on the FSG 2013 event. We thank all the FSG volunteers which helped to create and operate this new system. Your commitment and devotion makes the FSG an amazing event every year.

References

[1] G. de Koning Gans und Jaap-Henk Hoepman und Flavio D. Garcia. A Practical Attack on the MIFARE Classic. In *Proceedings of the 8th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications*, CARDIS '08, pages 267–282, 2008.

[2] International Organization for Standardization. ISO-IEC 15693-1:2010 Identification cards - Contactless integrated circuit cards - Vicinity cards - Part 1: Physical characteristics, 2008.

[3] International Organization for Standardization. ISO/IEC 14443-1:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics, 2008.

[4] J. Morgenroth, S. Schildt, and L. Wolf. A Bundle Protocol Implementation for Android Devices. In *Proceedings of the 18th annual international conference on Mobile computing and networking - Mobicom '12*, page 443, New York, New York, USA, Aug. 2012. ACM Press.

[5] NXP Semiconductors. MF0ICU2 - MIFARE Ultralight C. http://www.nxp.com/documents/short_data_sheet/MF0ICU2_SDS.pdf, Mai 2009. Version 3.2.

[6] NXP Semiconductors. MF0ICU1 - MIFARE Ultralight contactless single-trip ticket IC. http://www.mifare.net/files/3012/8379/9513/MIFARE_Ultralight_datasheet.pdf, April 2010. Version 3.7.

[7] NXP Semiconductors. MF3ICDx21_41_81 - MIFARE DESFire EV1 contactless multi-application IC. http://www.nxp.com/documents/short_data_sheet/MF3ICDX21_41_81_SDS.pdf, Dezember 2010. Version 3.1.

[8] NXP Semiconductors. MF1S70yyX - MIFARE Classic 4K - Mainstream contactless smart card IC for fast and easy solution development. http://www.nxp.com/documents/data_sheet/MF1S70YYX.pdf, Mai 2011. Version 3.0.

[9] NXP Semiconductors. MF1SPLUSx0y1 - Mainstream contactless smart card IC for fast and easy solution development. http://www.nxp.com/documents/short_data_sheet/MF1SPLUSX0Y1_SDS.pdf, Februar 2011. Version 3.2.

[10] J. Ott. 404 Not Found? – A Quest For DTN Applications. In *Proceedings of the third ACM international workshop on Mobile Opportunistic Networks - MobiOpp '12*, page 3, New York, New York, USA, Mar. 2012. ACM Press.

[11] SAE International. 2013 Formula SAE Rules. http://students.sae.org/cds/formulaseries/rules/2013fsaerules.pdf, 2013.

[12] S. Schildt, J. Morgenroth, W.-B. Pöttner, and L. Wolf. IBR-DTN: A lightweight, modular and highly portable Bundle Protocol implementation. *Electronic Communications of the EASST*, 37:1–11, Jan. 2011.